Nadie está a salvo de los ataques de los ciberdelincuentes

ANTONIO SALAS

LOS HOMBRES QUE SUSURRAN A LAS MÁQUINAS

Hackers, espías e intrusos en tu ordenador

Lectulandia

Descubre las luces y sombras de tu nueva vida en esta inquietante investigación de Antonio Salas en la que aprenderás cómo defenderte en la red. Una red en la que todos estamos atrapados. Una red llena de mentiras. El satélite que estábamos a punto de *hackear* pasaría sobre nosotros a las 5:17 a.m. Forcé la vista intentando localizarlo entre las estrellas. El *hacker* había comenzado su investigación fabricándose un palo de escoba y unos radios de bicicleta. Después perfeccionó el sistema con una antena direccional y un conector específico. «Esto nos calcula el efecto doppler, Falta 1 minuto y 30 segundos. Pasará a 875 kilómetros de altitud y a 7.430 kilómetros por hora. Va a aparecer justo por allí», me dijo mientras señalaba con el dedo algún punto en el horizonte, sin dejar de teclear comandos para mí indescifrables, y susurraba a la máquina como el amante que intenta seducir a su amada. Conecté la cámara de vídeo para grabar el instante en el que rompía la seguridad del satélite e interceptaba sus comunicaciones. «Ya estamos dentro». Mientras te sientes seguro en la intimidad de tu cuarto, o con tu teléfono móvil en el bolsillo, se producen un millón y medio de ataques informáticos al día. La mayoría de nuestros teléfonos y ordenadores ya están infectados. Los ladrones de vidas buscan suplantar tu identidad en redes sociales…

Lectulandia

Antonio Salas

Los hombres que susurran a las máquinas

Hackers, espías e intrusos en tu ordenador

ePub r1.0
Titivillus 01.12.15

Título original: *Los hombres que susurran a las máquinas*
Antonio Salas, 2015

Editor digital: Titivillus
ePub base r1.2

«Internet es una gigantesca máquina de espionaje al servicio del poder. Debemos luchar contra esta tendencia y convertirla en un motor de transparencia para el público, no solo para los poderosos.»

Julian Assange, Wikileaks

«Aunque no esté haciendo usted nada malo, le están vigilando y le están grabando. Y la capacidad de almacenamiento de estos sistemas se incrementa año tras año y añade ceros a la derecha a un ritmo constante, hasta el punto en que, sin haber hecho necesariamente nada malo, bastará con que le resulte sospechoso a alguien, incluso por error, y podrán utilizar este sistema para retroceder en el tiempo y escrutar todas y cada una de las decisiones que hayamos tomado, a todos y cada uno de los amigos con los que hayamos comentado algo, y atacarnos valiéndose de ello con tal de levantar suspicacias a partir de una vida inocente y pintar a cualquiera dentro del contexto de un malhechor.»

Edward Snowden

«Dale a un hombre un arma y puede robar un banco. Dale a un hombre un banco y puede robar el mundo.»

Tyrell Wellick, *Mr. Robot*, cap. 1x02

Prefacio
Ladrones de vidas

El último vídeo de gatitos en YouTube, que tu mejor amiga ha subido a su Facebook, te arranca una sonrisa. Pinchas en «Me gusta», y después lo compartes en tu muro añadiendo algún comentario ingenioso: «Ahora entiendo por qué mi perro cree que están para comérselos». Lo publicas también en tu perfil de Tuenti y tuiteas el enlace.

Ves que te han llegado seis nuevas solicitudes de amistad. Casi todo tíos. Ni siquiera te molestas en comprobar si realmente los conoces fuera de la red, o si tenéis amigos en común: los aceptas a todos. Con estos nuevos seis amigos, ya pasas de cien en Facebook y le ganas por tres a la presumida de tu amiga. Bien por ti. No serás la chica más popular del instituto, pero al menos en la red tendrás más «amigos» que ella…

Sospechas que probablemente alguno será un tío mayor, haciéndose pasar por alguien de tu edad. Recuerdas el incidente de aquella compañera. Descubrió que uno de los chicos que había agregado era en realidad un viejo verde que intentó quedar con ella. Pero ¿qué más da? Tú eres más lista y te sientes segura en la intimidad de tu cuarto, frente a la pantalla del ordenador. Incluso aunque algunos de esos perfiles fuesen falsos, ¿qué daño podrían hacerte desde el otro lado de la red? Terrible error.

A ti no te va a ocurrir lo que le pasó a tu hermano. Uno de los incautos que se bajaron la app The Adult Player, y que acabaron chantajeados con fotos comprometidas hechas desde su propia cámara. Lo has leído en las noticias: varios deportistas, actores y galanes famosos picaron el anzuelo. Pero crees que eso solo puede pasarle a un chico.

En casa estás a salvo, ¿verdad? Y la paranoia que te contagió aquella vecina que sufrió acoso hace unos meses ya está superada. Definitivamente, el ordenador te va mucho mejor desde que eliminaste el antivirus, que te ralentizaba unos incómodos segundos el equipo con tanta actualización de software y tanta tontería. ¿Quién va a querer crackearte a ti? ¿Qué podrías tener tú que le interesase a un pirata informático? Nuevo error.

Chateas un rato con tu amiga, comentando el último disco que os habéis bajado del eMule; lo horrible que sale una de clase en las últimas fotos que subió a Instagram o lo interesante que está el libro que te has descargado en PDF, de una página pirata. Ella te pide el enlace para bajárselo también, y tú se lo das, porque no sabes que el PDF es el vector de ataque preferido por los piratas informáticos.

Si tuvieses que comprar el libro físicamente para regalárselo, te lo pensarías dos veces, pero es fácil ser generoso con lo que no te cuesta nada. Y todavía crees, ingenua, que todo en la red es gratis. Aún no sabes que cuando algo es gratis en la red, el producto eres tú.

Suena un wasap. Es el grupo de las amigas del barrio. Te desnudas para meterte en la cama con el móvil mientras wasapeas con ellas, y durante un rato ríes despreocupada con sus ocurrencias. Tumbada sobre la cama, solo con una camiseta y las braguitas, pasas los siguientes minutos charlando con ellas a través del móvil, como si estuvieseis tomando cañas en el bar de la esquina. Solo que ahora puedes hacerlo en la intimidad y seguridad de tu habitación… ¿Intimidad?

Desde hace rato alguien te observa a través de la webcam del portátil que tienes sobre la mesa de tu escritorio. Justo frente a la cama. La activa por control remoto con un programa llamado Cammy, uno de los cientos de formas de *creepware* que existen para activar la cam o el micrófono de un contacto a distancia. Conoce tus rutinas, y lleva varios días grabándote mientras te desnudas en tu habitación. Tiene la esperanza de pillarte haciendo algo más fuerte, pero los vídeos de una joven de tu edad, desnudándose en su cuarto, ya valen dinero para algunas páginas de porno amateur. De hecho, todo vale dinero en la red.

También ha saqueado tus álbumes de fotos. Jamás sospecharías que tus fotografías veraniegas en la playa o bailando en la disco con tus amigas podrían valer dinero; hasta esas inocentes fotos de pies en la piscina que te gusta hacerte serán bien recibidas entre los fetichistas o pedófilos de Oriente Medio o Asia. Porque muchas de tus fotografías están ya en webs porno, para gusto y deleite de pajilleros japoneses, árabes o turcos, que podrían ser tus abuelos.

Incluso es posible que tu webcam esté directamente enlazada a una web especializada, como Insecam, una página donde se ofrecen miles de webcam pirateadas en todo el mundo, para que los *voyeurs* puedan contemplar cómo te desnudas en la «intimidad» de tu cuarto en tiempo real. Solo desde Insecam, en noviembre de 2014 se podía acceder a 4.591 cámaras pirateadas en los Estados Unidos, 2.059 de Francia, 1.576 de Holanda o 378 en España. Quizá la tuya sea una de ellas… Del Reino Unido se encontraron 500 enlaces, entre ellos algunos que filman, por ejemplo, la habitación de un niño en Birmingham, un gimnasio en Manchester o un pub en Stratford.[1]

Pero tu imagen, vestida o desnuda, es lo que menos interesa al ciberdelincuente. Quiere mucho más. Lo quiere todo. Quiere robar tu vida.

Ha echado un vistazo a tu cuenta bancaria. ¡Bah!, no tienes mucho. Así que apenas te robará unos euros. Tan poco que jamás te darás cuenta. Como ocurre con los miles de ordenadores que ha infectado en su red zombi. Si fueses una empresaria de éxito, o una adinerada banquera, quizá habría caído en la tentación de vaciarte la cuenta, o de utilizar los códigos de tu tarjeta de crédito para hacer compras en eBay, Amazon o Alibaba. Pero robar un par de euros a miles de cuentas es tan rentable como robar miles de euros a una sola. Y mucho más seguro. Por eso tu ordenador pertenece a una *botnet*.

Sin embargo, que te roben dinero tampoco es el mayor de tus problemas. Lo que realmente quiere el pirata que infectó tu ordenador es utilizar tu identidad digital. Tu

vida en la red. No eres una pieza de caza mayor, cuya captura requiriese una operación sofisticada de *malware* —software malicioso para infectar ordenadores y teléfonos móviles como el tuyo— dirigido, *pentesting* o ingeniería social. No. Eres una simple sardinilla anónima, en un banco de miles de peces, a la que capturó en su red de arrastre mientras navegaba por el inmenso océano de internet.

Le bastó diseñar un buen troyano. Esconderlo en un archivo «gratuito» —por ejemplo en una peli, una canción o un libro de moda— y subirlo a la red. Quizá, en la edición pirata del último libro de Antonio Salas… Tú te lo descargaste y con él te llevaste el virus a tu ordenador. A tu casa. No, nada es gratis en la red.

Ahora el tuyo es uno de sus ordenadores zombi. Como miles de ordenadores que se descargaron el mismo virus. El ciberdelincuente controla tu ancho de banda, tu disco duro, tu wifi, tus cuentas de correo o redes sociales. Tiene el poder total para utilizarlos como mejor le convenga. Y puede hacerlo él, o vender esa *botnet* al mejor postor en el mercado negro. Por ejemplo, en uno de los miles de mercados de vidas robadas en la Deep Web, la internet profunda, que no aparece en los buscadores.

¿Quién puede comprar tu vida? Alguien que necesite miles de ordenadores conectados entre sí a través de un mismo *malware,* para trabajar juntos por un objetivo más ambicioso… Como la red mundial del programa SETI, pero con intenciones mucho menos altruistas.

Tú no lo sabes, pero en la actualidad el negocio del *malware* supera con creces el tráfico de cocaína.

Utilizarán tu vida digital para abrir cuentas en casinos *online* a través de las que blanquear dinero. Para distribuir pornografía infantil en la Deep Web. Para robar a tu banco a través de tu cuenta. Para atacar objetivos políticos o económicos con programas de DoS o para distribución de propaganda yihadista. No hay más límite que la imaginación del ciberdelincuente. Y su imaginación no tiene límite.

Dentro de unos días, quizá de unas semanas, recibirás la visita de la Policía o la Guardia Civil. Te detendrán por distribuir porno infantil, por blanqueo de capitales o por difusión de propaganda terrorista. Jurarás una y otra vez que eres inocente, que no sabes de qué te hablan, pero las pruebas serán irrefutables. La IP de tu ordenador o de tu teléfono móvil o de tu red wifi aparece asociada a esos delitos y solo tú, o eso creías, tenías acceso a ellas. Entonces pensarás que habría sido más barato haberte comprado el disco, la peli o el libro, que descargártelo «gratis» en la red…

La Policía está desbordada. De la misma forma en que la legislación contra nuevas drogas de diseño evoluciona al rebufo de la creatividad de los químicos, los cibercriminales crean nuevos delitos que aún no están definidos como tales.

A pesar de los ingentes esfuerzos, dedicación y recursos que las Fuerzas y Cuerpos de Seguridad del Estado están dedicando a la seguridad informática, los *blackhats* —hackers de sombrero negro o ciberdelincuentes— siempre van un paso por delante. Las nuevas leyes sobre seguridad informática tardan mucho en ser aprobadas, y para cuando se legisla sobre un nuevo tipo de ciberdelito, intrusión o

malware, los *blackhats* ya han inventado mil nuevos virus, gusanos, troyanos y han descubierto nuevas vulnerabilidades en la red. Es una carrera perdida. Sobre todo si, como desveló hace un par de años Edward Snowden, el invasor de nuestra intimidad, el ladrón de nuestra vida, no es un cracker, ni una mafia organizada, ni un grupo terrorista… sino las agencias de Inteligencia más poderosas del mundo.

La buena noticia es que existen formas de ponérselo difícil. Existen maneras de protegerte. De evitar ser una sardinilla anónima en un inmenso banco de peces. Aunque solo ellos pueden ayudarnos a recuperar nuestras vidas robadas o evitar que nos las roben. Los hackers.

OCTUBRE DE 2014
MATAR A ANTONIO SALAS

«Más que por la fuerza, nos dominan por el engaño.»

Simón Bolívar

Quedamos en un discreto restaurante madrileño del norte de Madrid, donde nos reuníamos de cuando en cuando. Una decena de policías nacionales, municipales, guardias civiles… y un periodista encubierto. Yo era solo un invitado. Jamás tomé la iniciativa para convocar ninguna de aquellas tertulias, pero esta vez era distinto. Mis compañeros notaron que mi comportamiento era extraño. Me mantenía distante, preocupado, ensimismado… Y ante la insistencia de Pepe, saqué de mi mochila un puñado de papeles y se los pasé.

—Dime si te parece que es para preocuparse… Yo no sé qué hacer. —Supongo que mi voz delataba mi nerviosismo—. Seguramente será todo una paranoia, y este tío será un chalado que va de farol, pero he hablado con los organizadores del congreso y me confirman que es verdad. Se matriculó con nombre y DNI falso para asistir a mi conferencia y es verdad que alguien armó un follón en la entrada cuando se llenó la sala. Y si eso es cierto, quizá lo demás también lo sea.

A mi alrededor, en aquella mesa redonda, un grupo de veteranos policías se pasaban las hojas donde había impreso el email que acababa de recibir, en el que un conocido cibernazi, con una activa presencia en la red, me confesaba que en la mañana del 5 de marzo de 2014 había intentado degollarme con una navaja en el salón de actos del campus de Vicálvaro, de la Universidad Rey Juan Carlos de Madrid.

David Madrid, Pepe, Álex, Rubén, Toni, Rafa, Manu… se alcanzaban las hojas unos a otros. Era fácil reconocer cuándo llegaban al párrafo en cuestión, porque abrían mucho los ojos y dejaban escapar algún comentario… «Joder, qué fuerte.»

Casi todos habían oído ya hablar de MarkoSS88. El webmaster de una conocida página nazi es un veterano activista en la red. Sus Facebook, Telegram, Twitter y demás redes sociales han sido el campo de batalla de enconados debates entre los neonazis y los antifascistas. Intelectual e ideólogo, especialmente dedicado a la formación de las nuevas generaciones de jóvenes skinheads NS, MarkoSS88 es autor de muchos textos doctrinales sobre el movimiento nazi, su historia, política, filosofía y espiritualidad. Y en páginas de venta *online*, como lulu.com o dropbox.com, podía comprarse por

23 euros el libro que él firmaba: *¿Qué es el Nacional Socialismo? Un trabajo de dedicación y entrega.*

Pero MarkoSS88 no es solo un ideólogo. Al menos según su dilatada presencia en la red, también es un hombre de acción y un objetivo para los grupos antifascistas, tras el asesinato de un joven latin king que tuvo cierta difusión en las redes y encabezó alguna plataforma en change.org. Según él, en defensa propia.

Mis compañeros de tertulia sabían también que MarkoSS88 llevaba un par de años absolutamente obsesionado conmigo. Era uno de mis acosadores más leales en la red. Cada vez que me entrevistaban en un medio y colgaban la entrevista, su nick aparecía entre los comentarios más agresivos. Sus insultos y amenazas de muerte llegaban con cierta frecuencia a mis cuentas de Twitter o email. No dejaba pasar la ocasión de difamarme, calumniarme y expresar su íntimo deseo de verme muerto. Como otros muchos nazis, antisistema, puteros, proxenetas o traficantes. Nada nuevo. No es la primera vez que me pasa. Poco antes de recibir ese email, me había encontrado con un mensaje de la Fiscalía de Protección de Testigos, al acudir a Intervención de Armas de la Guardia Civil para renovar mi licencia trianual. La fiscal quería reunirse conmigo para valorar la renovación de mi situación como testigo protegido.

Pilar y Gonza —dos agentes del Grupo VII de Información, que habían llevado la Operación Puñal contra Hammerskin en cuyo juicio declaré— me escoltaron de nuevo hasta la Fiscalía para mantener la reunión con la fiscal (María Antonia Sanz), y con la psicóloga responsable de los testigos protegidos (Marta de Prado). Uno de ellos fue quien me regaló el pasamontañas que utilizo en las entrevistas.

El día en que presté declaración en el juicio, y antes de bajarme del coche en el que me habían trasladado a la Audiencia Provincial, escondido en la parte de atrás, en un dispositivo que parecía salido de una película, me dijo que me pusiese el pasamontañas. «Por tu seguridad —exclamó mientras señalaba los edificios que rodeaban la Audiencia—. Podría haber alguien en alguna de esas ventanas.»

Sabíamos que las novias de algunos de los quince skins imputados habían hecho un fondo para contratar a un sicario que impidiese mi declaración ante el tribunal, y aquella era su última oportunidad de silenciarme antes de entrar en la sala. Ahora, cinco años después, ese mismo guardia me acompañaba a la reunión con la fiscal que debía tomar la decisión de cerrar mi expediente o mantenerme como testigo protegido a continuidad.

Cuando la fiscal me preguntó si continuaba recibiendo amenazas, sonreí con resignación: «Casi a diario, señora…, y no solo de los neonazis». Solo

tuve que dejar sobre su mesa un montón de hojas impresas, con el torrente de amenazas que recibo, y la fiscal lo vio claro. Continuaría manteniendo el estatus de testigo protegido indefinidamente. Varias de aquellas amenazas venían firmadas por MarkoSS88.

Después de *El año que trafiqué con mujeres, El Palestino* y *Operación Princesa,* la lista de «damnificados» por mis infiltraciones había crecido de manera exponencial. Pero una cosa es que un puñado de cobardes te insulte, difame o amenace en la red, y otra muy distinta lo que aseguraba el email que mis amigos tenían ahora en sus manos, MarkoSS88 iba más allá. Mucho más allá.

No solo hablaba de cómo el 5 de marzo pasado había ido a buscarme armado con un cuchillo al Congreso de Inteligencia que se celebraba en la Universidad Rey Juan Carlos. No solo contaba con pelos y señales cómo había llegado hasta allí con la firme intención de rajarme el cuello, fuesen cuales fuesen las consecuencias. Incluso me explicaba que el día anterior había acudido al campus para estudiar los accesos al auditorio, las entradas y salidas, las rutas de escape…[2]

Sí, es verdad, he recibido amenazas antes. Pero es muy distinto cuando alguien te confiesa el día, la hora y cómo ha intentado matarte:

—Joder, Toni —dijo Álex, otro de los policías nacionales, al leer el correo —, tienes que averiguar quién es este tío. Podría volver a intentarlo.

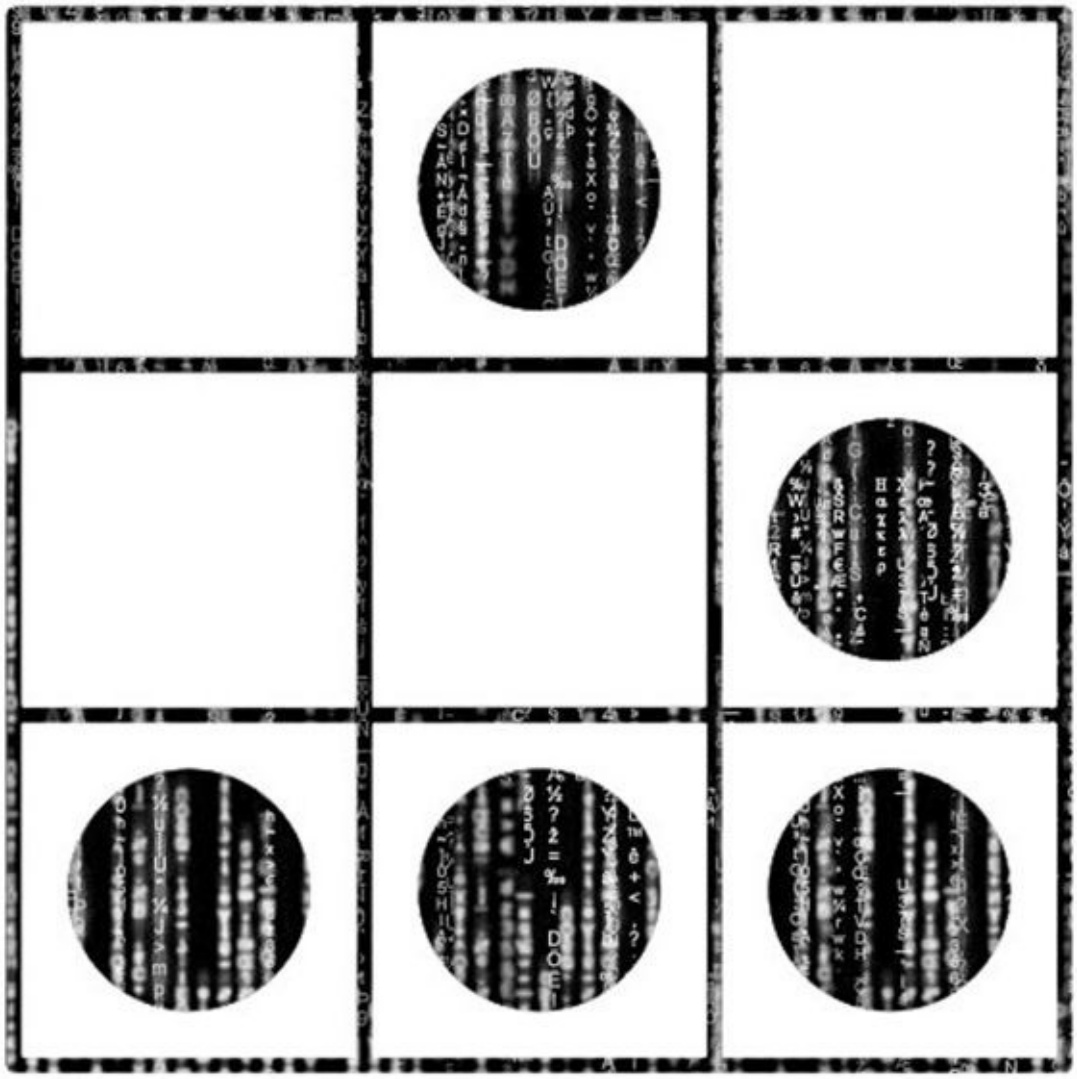
—Lo sé. En realidad, si un imprevisto no hubiese complicado los planes de MarkoSS88, probablemente él estaría muerto y yo en la cárcel. Pero no me hace ni puta gracia que pueda ocurrírsele intentarlo otra vez…

Para cuando recibí la confesión de MarkoSS88 yo ya llevaba meses sumergido en la investigación sobre el hacking y la (in)seguridad informática. Así que estaba preparado para iniciar la «caza». Pero subestimé a MarkoSS88. Tras esa identidad no se ocultaba un simple neonazi vinculado a UltraSSur. El skinhead que había confesado cómo el 5 de marzo de 2014 intentó ejecutar a Tiger88 resultó ser alguien muy distinto al del perfil que yo imaginaba. Más poderoso. Más peligroso.

Durante los últimos años he conocido a hackers de sombrero blanco, gris y negro, a ciberactivistas, ciberdelincuentes y ciberpolicías. He asistido a sus congresos, talleres y seminarios. He conocido a los espías que utilizan las redes informáticas para obtener información y a los ciberterroristas que distribuyen en ella su propaganda. He convivido con los ciberacosadores y con sus víctimas, e incluso me he convertido yo mismo en víctima de alguno de ellos. Y me he convencido de que, en el siglo XXI, no existe nada más urgente que conocer cómo funciona nuestra vida en la red. Porque todos estamos ya en ella. Héroes y villanos, criminales y policías, nazis, proxenetas, traficantes, terroristas… El ordenador, y más aún los teléfonos

móviles, son nuestro pasaporte al nuevo mundo. Si no usas internet y no tienes un teléfono móvil, no necesitas seguir leyendo. De lo contrario, prepárate para descubrir el lado oscuro, y también el más luminoso, de tu nueva vida. Una red en la que todos estamos atrapados. Una red llena de mentiras.

PARTE I



Glider. Símbolo hacker propuesto en octubre de 2003 por Eric S. Raymond como emblema de la cultura hacker: «El uso de este emblema expresa la solidaridad con los objetivos y valores de los hackers, y la forma de vivir de un hacker».El Glider tiene su origen en un juego matemático diseñado en 1970 por John Horton Conway, «el juego de la vida», que representa un autómata celular, equivalente a una máquina universal de Turing, es decir, todo lo que se puede computar algorítmicamente.

Capítulo 1
Los secretos están en el aire

«El honor ha de ser la principal divisa del Guardia Civil, debe por consiguiente conservarlo sin mancha. Una vez perdido no se recobra jamás.»

Duque de Ahumada, La Cartilla del Guardia Civil, artículo 1

Después de *Operación Princesa.* Octubre de 2013

Tiene algo de ritual. Cuando llega la caja con los primeros ejemplares de cada nuevo libro, el tiempo se detiene. Solemnemente la colocas sobre la mesa más cercana. Corres a por un cuchillo para rasgar el precinto. Abres las solapas de cartón y retiras el plástico protector de los libros. Y ahí está. Como un bebé recién llegado al mundo. Y así nació *Operación Princesa,*[3] mi anterior criatura.

Tras años de esfuerzo en la investigación, meses de trabajo en la redacción, y una gestación accidentada. Soportando las reticencias del gabinete jurídico, los sufridos correctores, y el departamento comercial de la editorial, el nacimiento de cada nuevo libro es como el de un nuevo hijo. Pero en mi caso, y en contraste con mis colegas, no implica que llegue el momento de disfrutar de dicha paternidad. No habrá ferias literarias, presentaciones en sociedad, ni promoción con los lectores. En mi caso, cada nuevo libro implica que empiezan los problemas.

A diferencia de otros formatos periodísticos, durante el trabajo de campo el periodista encubierto solo debe preocuparse de que el objetivo de su infiltración no lo descubra. Y si utiliza cámara oculta, prohibida en España en 2012, la principal preocupación es controlar los tiempos de duración de la batería, y de las cintas o tarjetas de grabación.

Durante los meses o años que dura la infiltración, estás concentrado en obtener el máximo de información sin que tu tapadera salte por los aires. Y en grabar y proteger el mayor número de horas de audio y vídeo…

Si todo sale bien, nadie sospechará de ti. Porque si alguien lo hiciese, y decidiera cachearte, no habría excusas. No existe una justificación convincente para el miembro de un grupo criminal a quien sorprenden grabando una reunión con sus compinches con una cámara oculta. O es un agente encubierto o es un periodista infiltrado.

Después llega el proceso de desaparición. Siempre es igual. Una vez concluida la investigación debes alejarte del colectivo investigado tan discretamente como llegaste a él. Sin prisas. Sin ruido. Sin llamar la atención. Como un fantasma.

Pero cuando se publica el libro, *ellos*, el objetivo, descubren que han tenido un infiltrado entre sus filas. E inevitablemente llega el odio, los insultos, las amenazas. Y el vehículo de ese odio es la red.

En cuanto saqué de la caja el primer ejemplar de *Operación Princesa*, fui consciente. Me sentía orgulloso por el estupendo aspecto que tenía mi nuevo bebé. Entre aquellas páginas había tres años de sudor, lágrimas y sangre. Pero también fui consciente de que los clubs de motoristas —especialmente los Ángeles del Infierno —, los narcos mexicanos y gallegos, y los políticos y agentes de Policía y Guardia Civil corruptos retratados en *Operación Princesa,* recibirían con poco sentido del humor la noticia. Ángel, aquel *free biker* oscuro y silencioso con el que habían

convivido, era un puto periodista infiltrado…

Los Ángeles del Infierno fueron los primeros en hacerme llegar, de forma elocuente, su ira. En un mundo cada vez más digital, el Facebook del *Ángel Oscuro* que había utilizado durante la investigación pronto empezó a recibir los mensajes predecibles tras toda infiltración: «hijo de puta», «traidor», «payaso». Siempre es igual.

Según supe gracias a los amigos que conservo vinculados al MC 1% más legendario de todos los tiempos, los Hell's Angels llegaron a consultar con sus distinguidos abogados las posibles fórmulas de demandarme por la información que publicaba en *Operación Princesa* sobre su organización. Según sus palabras literales: «Muchos somos demasiado reconocibles…». Sin embargo, con buen criterio, los abogados les recomendaron que se olvidasen del tema. Ventajas del formato «novela».

Aun así, *Operación Princesa* llegaría con otros panes bajo el brazo. Sorpresas tan gratas y reconfortantes como inesperadas.

Especialmente gratificante fue recibir, en mi Facebook legítimo, diferentes solicitudes de amistad de familiares, amigos y profesionales vinculados a Pilar de Lara, la implacable y valiente jueza que instruyó la investigación de la siniestra Operación Carioca, una de las tramas que articulan *Operación Princesa*.

Por mediación de una de aquellas nuevas ciberamigas —Amelia, una prestigiosa abogada lucense—, doña Pilar de Lara me hacía llegar su interés por las grabaciones que yo había hecho en el club Queens, uno de los burdeles donde se desarrolló la vergonzante Carioca.

Según la jueza, tras el descubrimiento de la posible fosa de una de las prostitutas presuntamente asesinadas y enterradas en el solar del Queens, mis grabaciones podían ser útiles para datar la fecha de la exhumación del cadáver… Como es natural, le facilité todos los vídeos y fotografías que había tomado durante mi investigación para *Operación Princesa* y quiero pensar, así me lo hizo saber Amelia, que fueron de alguna utilidad en el sumario.

A lo largo de esa investigación viajé a Lugo en tres ocasiones, y siempre sentí la tentación de contactar con doña Pilar de Lara. Nunca lo hice. Cuando un juez se enfrenta en solitario al poder político, empresarial y policial de su ciudad, destapando la mayor trama de corrupción de su historia, es inevitable convertirse en objetivo de las iras, descréditos y ataques de los corruptos. Y de sobra sabía que acudir a la jueza en busca de información para mi libro solo podía causarle problemas. Así que durante su instrucción del caso jamás contacté con ella. Lo prometo. Hasta hoy solo he coincidido en persona con Pilar de Lara en una ocasión… Fue en 2015, y ya en el transcurso de la actual investigación. Y doña Pilar ni siquiera fue consciente de que yo estaba allí, a unos centímetros de ella. Solo hoy sabrá que estuvimos tan cerca y por qué.

Cuando *Operación Princesa* salió a la luz, uno de mis temores era que despertase

enemistades para conmigo en la Guardia Civil, con quienes siempre había tenido una relación cordial. Por suerte ocurrió todo lo contrario.

Particularmente conmovedor fue el gesto de Roberto, un guardia civil de Lugo que, emocionado por el contenido de mi novela, que no dejaba en muy buen lugar a su Comandancia, me envió un obsequio que me dejó perplejo y que quizá pocos podrán valorar… Roberto me regaló su tricornio reglamentario. El mismo que utilizó en su jura de bandera en la Academia, y en el que escribió una inmerecida dedicatoria.

No fue la única reacción imprevisible de la Benemérita. En su número 828, de febrero 2014, la revista oficial del Instituto Armado, *Guardia Civil*, dedicaba tres páginas a mi novela. A pesar de que *Operación Princesa* desnudaba, sin ninguna compasión, las miserias de docenas de guardias civiles y policías corruptos implicados en el escándalo destapado por Pilar de Lara, otros guardias —guardias honrados, que todavía mantienen viva la fe en La Cartilla, y el espíritu que el Duque de Ahumada intentó plasmar en ella— acogieron mi libro con un cariño que no esperaba.

Sin duda, sin ninguna duda, la mayor sorpresa en ese sentido llegó, como nos llegan hoy las noticias, vía email. Un email que terminaría abriéndome las puertas del inabarcable mundo de unos y ceros.

Una nube de secretos en el aire

Me llegó una mañana, desde el Servicio de Asuntos Internos de la Guardia Civil, redireccionado a través de mi página web: el email de uno de los siete investigadores que habían llevado a cabo la Operación Carioca. Después de un amistoso saludo y de darme la enhorabuena, me preguntaba si habría alguna forma de poder conocernos:

> … dígame qué quiere que le facilite para contrastar que realmente soy quien digo y así, si usted lo ve conveniente, poder reunirnos y conocerle en persona y tener la satisfacción de que nos firmara sus libros. Muchas gracias de antemano.

Tardé unos días en responder. Los que necesité para contrastar el origen del email, y convencerme de que era legítimo. Aun así le pedí un teléfono de contacto oficial, que pudiese verificar como perteneciente al SAI de la Guardia Civil. Comprensivo con mi desconfianza, aceptó. Hecho esto, Omar y yo iniciamos un intercambio de correos y conversaciones telefónicas que terminaría con un encuentro personal. El primero de muchos…

Al mismo tiempo y por su cuenta, Luis, otro exmiembro del Servicio de Asuntos Internos que había liderado la investigación de los policías corruptos de la Carioca, también sintió el impulso de escribirme, ignorando que su compañero ya lo había hecho:

> … por cierto, en aquellos tiempos yo era el sargento que mandaba el pequeño grupo que estuvo mucho tiempo en Lugo investigando aquello, de manera clandestina, y casi casi tan solos como tu guardia Luca (investigar la corrupción es lo que tiene, y más la relacionada con la prostitución, que es un tema al que la gente no le da el mínimo interés si no es cuando lo hacen delante de sus casas). Y recuerdo que por entonces me leí tu libro *El año que trafiqué con mujeres*, que aunque muy bueno también, no daba ese protagonismo (creo) a los sentimientos de las mujeres. Sigue así.

Omar y Luis se ganaron mi confianza y mi simpatía al instante. Demostraron una sensibilidad hacia el problema de la prostitución que había visto en pocos policías. Y teníamos mucho en común.

Ellos como guardias civiles, y yo como periodista, nos habíamos acercado a las prostitutas inicialmente como fuentes. Pero Omar y Luis, y estoy seguro de que todos sus compañeros del SAI, sufrieron el brutal impacto emocional, la atroz tormenta mental que implica conocer las miserias más íntimas de una mujer traficada.

Durante el ingrato trabajo de Asuntos Internos —los policías que investigan a otros policías—, Omar y Luis vivieron en carne propia el vértigo que implica conocer esas historias. Los cómo, cuándo y por qué aquellas chicas habían llegado a los burdeles españoles. Y demostraron una sensibilidad, comprensión y caridad que a mí no puede menos que conmoverme. Mientras otros policías se aprovechan de su estatus para ganarse los favores sexuales de las mujeres prostituidas, escudados tras su placa, los agentes del SAI se convirtieron en los ángeles de la guarda de la

auténtica Álex Cardona[4] y de sus compañeras de infortunio. Incluso llegaron a pagarles comida y techo con sus parcos salarios de funcionario, cuando el Gobierno de España, como en tantas otras ocasiones, se olvidó del servicio que las testigos protegidas estaban haciendo a la retirada de mierda en el seno de nuestras Fuerzas y Cuerpos de Seguridad del Estado. Y en las concejalías, alcaldías y ayuntamientos de varias ciudades españolas.

Los policías probablemente ven el lado más oscuro de la humanidad a diario. Asesinos, violadores, estafadores, pederastas… Yo solo soy un turista que entra y sale de esos mundos para contarlo. Ellos se pasan allí la vida. Supongo que es lógico que en algunos casos algo se rompa en su interior, y más de uno sienta la tentación de cruzar la raya. Por eso existen policías que pueden pararse ante el espejo, y sentirse orgullosos del uniforme que visten. Otros solo pueden sentir vergüenza. Y si alguien sabe que esto es una realidad son los de Asuntos Internos. Su trato a las prostitutas de la Operación Carioca me demuestra que ellos todavía pueden mirarse al espejo con orgullo.

A pesar de que debería ser yo quien de alguna manera encontrase la forma de premiar la honestidad y la sensibilidad de aquellos policías, fueron ellos quienes volvieron a sorprenderme con un obsequio tan inesperado como desproporcionado. Una placa del Servicio de Asuntos Internos decorada con una inmerecida leyenda que hoy preside mi despacho de trabajo. No podré presumir de ella, ni mostrarla a nadie, pero me ayuda a recordar que a veces el miedo, la angustia y la soledad de este oficio tienen recompensa. Conocer a policías honestos que todavía creen en lo que hacen.

Durante una de nuestras reuniones me hicieron el mejor cumplido que he recibido.

Cuando tras varios encuentros Omar ya se sentía con la suficiente confianza como para soltármelo, se sinceró. Desde que leyeron *Operación Princesa*, una duda corroía al Servicio de Asuntos Internos de la Guardia Civil:

—Toni, no te ofendas, pero tengo que preguntártelo porque en el grupo tenemos un debate sobre esto. Cuando nosotros estábamos en Lugo, haciendo la investigación… ¿tú estuviste siguiéndonos?

Encajé la pregunta con sincera perplejidad.

—Joder, Omar. Claro que no. Pero ¿cómo se os ha ocurrido algo así?

—Coño, es que no lo entiendo. En tu libro describes con tantos detalles los lugares, los personajes, las matrículas… todo. Es como si hubieses estado detrás de nosotros durante la investigación.

No. Yo no estuve vigilando a los vigilantes mientras hacían su trabajo. La documentación que dio lugar a la novela se debe exclusivamente a mi propia investigación, pero mentiría si no reconociese que me llenó de satisfacción que los agentes del SAI llegasen a tener esa duda.

Sin embargo, el mayor regalo que me hicieron los agentes de Asuntos Internos, y que marcó el arranque de esta investigación, fue abrirme los ojos. Hasta aquella

mañana en la que compartimos desayuno en un centro comercial de la periferia de Madrid, jamás me había dado cuenta de una realidad tan evidente que me había pasado desapercibida durante toda mi carrera como periodista.

Los guardias del SAI y yo comentábamos con frecuencia detalles del caso, e intercambiábamos puntos de vista. Por otras fuentes, y mucho antes de conocerlos (doy mi palabra de honor de que fue así) yo había tenido acceso a todos los informes redactados por los agentes de Asuntos Internos durante la investigación de la Operación Carioca. En varios de ellos se transcribían las intervenciones telefónicas a los sospechosos, el registro forense de sus equipos informáticos, y el volcado de datos y sms de sus teléfonos móviles… Por supuesto, resultaron imprescindibles los continuos operativos de seguimiento, los incansables interrogatorios y todo el trabajo policial «convencional», pero en aquellos informes técnicos que sacaban petróleo de la vida digital de los sospechosos estaba casi todo. Porque en pleno siglo XXI, nuestra vida discurre alternativamente en dos mundos paralelos: el real y el digital.

—Nosotros teníamos orden judicial, pero cualquier hacker podría haberlo hecho por su cuenta —dijo uno de los agentes del SAI haciendo un gesto con la mano, como si quisiese agarrar algo invisible suspendido sobre nosotros—. La información está aquí, a nuestro alrededor, atravesando el aire. Pero hay que saber cómo recogerla…

Imposible una imagen más gráfica. Aquel sencillo gesto con la mano, intentando tomar algo en el aire, refleja una circunstancia tan turbadora como evidente. Los secretos más inconfesables, las cuentas bancarias de los corruptos, la correspondencia más comprometedora de los políticos, los proyectos militares más confidenciales… Toda esa información está aquí, a nuestro alrededor, suspendida en el aire, cifrada o no, en redes inalámbricas que nos atraviesan en todo momento y lugar. Vivimos envueltos, rodeados, sumergidos en esa nube de información invisible. Solo hace falta saber cómo abrir los ojos para descubrirla.

Y los hackers no solo tienen la capacidad de acceder a la información. También, cada vez más, pueden encontrar las vulnerabilidades de cualquier tecnología utilizada en nuestra vida diaria. Una vida diaria más y más influenciada por el «internet de las cosas». Aparatos de televisión, coches, implantes médicos, frigoríficos inteligentes… La tecnología electrónica ha llegado a nuestras vidas para quedarse, y toda tecnología tiene alguna vulnerabilidad. Menos de dos años después de aquella conversación con los agentes del Servicio de Asuntos Internos, yo mismo sentiría la adrenalina que experimenta un hacker al penetrar en el sistema de un organismo oficial en otro país, o abrir un acceso a todos los datos, contraseñas y cuentas de cientos de usuarios, tras atraerlos en un lugar público hacia una falsa wifi, o presenciaría cómo un joven hacktivista se embarcaba en el hackeo de un satélite utilizando una tecnología accesible a cualquiera… Pero antes de eso debería iniciar un largo viaje, y mi primera etapa se encontraba en un lugar muy familiar. La guarida de un espía.

Juan vs. David: un hacker en el CNI

«No toda la información hay que salir a buscarla por ahí afuera. Alguna ya está disponible y es bastante próxima, aunque resulta improductiva si desconocemos su existencia», dice David R. Vidal, el «agente Juan» en su *Diario de un espía*.[5]

Ese mes de octubre de 2013 mi mentor en *El año que trafiqué con mujeres* ultimaba el borrador de su primera obra. Él fue el segundo elemento que encauzaría la presente investigación: el comentario de los agentes del SAI había azuzado mi curiosidad periodística, y David era lo más parecido a un hacker que yo conocía.

En las mismas fechas, el programa de televisión *Equipo de investigación* había concertado con mi editorial grabar una entrevista conmigo. Los compañeros de La Sexta estaban realizando un reportaje sobre los Ángeles del Infierno y estaban interesados en recoger mi testimonio, y en grabar algunos de los «fetiches» del mundo de las bandas moteras que había recogido durante mi investigación.

Mi editora había cerrado una cita con mis colegas de La Sexta, pero todavía tenía tiempo de recorrer los 600 kilómetros que me separaban del «búnker» de trabajo de David, en un pequeño pueblo del norte de España, y regresar a tiempo para la entrevista. Así que arranqué la moto, la misma que utilicé durante la investigación de *Operación Princesa*, y puse proa al norte… Llovía mucho. Fue un error. Y lo pagaría en carne… en mi carne.

A pesar de la tromba de agua, disfrutaba de la carretera. Mientras limpiaba el casco con la mano y sentía cómo poco a poco la lluvia iba calando mi ropa recordé mi historia personal con el «agente Juan».

La primera vez que oí hablar de David R. Vidal fue en la Comisaría Central de la UCRIF en Madrid. Había iniciado mi investigación sobre el tráfico de niñas y mujeres para su explotación sexual dando palos de ciego. Como siempre. Acudí a congresos y cursos sobre prostitución, visité las asociaciones de empresarios del sexo, como ANELA, y a sus enemigos naturales, las asociaciones de apoyo a las prostitutas, como Alecrín, AMUNOD o APRAMP, y pedí ayuda a los responsables policiales de la lucha contra la trata. Y durante una de mis visitas a la sede de la UCRIF, en la calle General Pardiñas de Madrid, uno de los oficiales de Inteligencia de dicho servicio me puso sobre la pista:

—Pues, Toni —me dijo—, la persona que más sabe sobre este tema es David Vidal. Deberías conocerlo…

El oficial de Inteligencia de la UCRIF no demostraba ninguna simpatía por el tal Vidal, de ahí que valorase aún más su criterio. Habían coincidido durante una operación policial en el norte, y al oficial le había sorprendido encontrar a un civil que lucía una pistola Glock al cinto y manipulaba con impunidad los ordenadores de la comisaría. Me reconoció que probablemente era el mayor experto en España sobre la trata de seres humanos. ¿Quién era aquel tipo que se paseaba armado por las

comisarías de policía, manipulando sus ordenadores, sin pertenecer oficialmente al Cuerpo?

El oficial de Inteligencia tenía razón. David resultó ser el mejor maestro que cualquier periodista que aspirase a infiltrarse en la trata de blancas podría soñar. En mi segundo libro, *El año que trafiqué con mujeres*,[6] David se convirtió en mi padrino.

Doy mi palabra de honor de que nunca antes había visitado un burdel. De su mano conocí cientos, y aprendí, sin delicadeza, miramientos ni pérdidas de tiempo, cómo funciona el negocio de la información en la noche:

—Si quieres que una puta te dé información, jamás y digo jamás, te acuestes con ella. Y si lo haces, no lo hagas en el club, ni le pagues por follar. Si subes con una puta en un club y te la follas, para ella serás un cliente, no un amigo. Y a los clientes se les saca la pasta, no se les da información. Así que te guardas la chorra y te aguantas. Y si ves que te ponen muy cachondo, porque las condenadas saben ponerte cachondo, te vas al cuarto de baño y te haces una pajilla. Ya verás como después sales más calmadito y puedes seguir hablando con ellas sin pensar en tirártelas.

Así de brutal y directo era mi mentor. Implacable con mi inexperiencia en los prostíbulos, pero un acelerante impagable en mi investigación. Con él aprendí a mimetizarme entre los proxenetas, a localizar el mejor punto de observación en los clubs, a reclutar fuentes… Y pronto el «agente Juan» se convirtió en uno de los nombres recurrentes de mis libros. Durante sus incursiones en las trastiendas de la información, David utilizaba el nombre de «John Osaro»; yo solo me limité a castellanizarlo.

Por aquella época David trabajaba para el Ministerio del Interior, controlando una tupida red de informadores en diferentes países africanos. Pero entonces el presidente José María Aznar declaró la inmigración ilegal y el tráfico de seres humanos como un problema de seguridad nacional, así que me pareció buena idea hablarle de David a uno de mis contactos en el CESID, el servicio de Inteligencia precursor del actual CNI. Y mi sugerencia debió de resultarles interesante, porque pocas semanas después Ramiro, un entrañable coronel del Ejército español, que coordinaba el CESID en la región, mantuvo su primera entrevista con David R. Vidal.

Incómodo en el trato, y con un incisivo sentido del humor cuya ironía no todos saben apreciar, David era, por encima de todo, una autoridad en su área, y al parecer Ramiro juzgó que mi recomendación estaba justificada. Ese mismo año, David «fichaba» por el servicio de Inteligencia español, y pronto tejió una nueva red de informadores que ha proporcionado la materia prima para miles de informes de Inteligencia de temática diversa.

En el año 2010, David fue uno de los fundadores de GlobalChase,[7] pionera academia privada de Inteligencia en España que llevó por primera vez al entorno universitario las prácticas más operativas.

Ese mismo año, durante mi infiltración en el terrorismo internacional para

documentar mi libro *El Palestino,*[8] volví a encontrármelo. Continuaba manteniendo su irritante sentido de la ironía, su afición a la buena mesa, buenos coches y buenas mujeres, y su perspicaz inteligencia e implacable profesionalidad. Para entonces simultaneaba dos ambiciosas redes de información, tanto para el Ministerio del Interior como para el Centro Nacional de Inteligencia: llegó a tener bajo su responsabilidad hasta a veinticinco informadores en dieciséis países, fundamentalmente en el continente africano. Algo inaudito en la historia de los servicios de información.

Pero antes de todo ello, en sus orígenes, David R. Vidal era informático. Durante once años fue el responsable del área informática del departamento de Servicios Generales de una conocida entidad bancaria. Además, en los noventa y principios de los 2000 publicó más de setenta artículos sobre programación, domótica, comparativas de productos —especialmente nuevas tecnologías y autoedición—, etcétera, en revistas tan emblemáticas como *PC World,* donde fue articulista habitual durante diez años. Algunos todavía están disponibles en la web de la histórica publicación informática.[9]

Y precisamente esa, la del hacking, fue una de las habilidades del agente Juan que tanto el Ministerio del Interior como el CNI supieron explotar.

Yo viví todo el proceso muy de cerca. David reclutaba sus informadores en los países de origen, como Nigeria. Diseñó su propio sistema de cifrado de comunicaciones e instruyó a los informadores para enviar sus informes a través de páginas web ficticias que había creado, los cuales eran recibidos en un servidor que estaba en Rusia y de ahí pasaban a otro «blindado» en España, previamente diseñado para esta operación.

A David le pregunté por qué tenía el primer servidor en Rusia. Se sonrió y respondió algo que me produjo cierto desasosiego:

—Se supone que los hackers están en Rusia o en China, ¿no?

Ahora, mientras iba camino de su guarida, casi podía recordar aquello como una primera lección para mi nuevo proyecto.

Además, David creó su propio virus informático, destinado a obtener información en los países objetivo, infectando las comunicaciones en las que una serie de palabras clave —algo así como *visado* + *España* + *prostitución,* etcétera— disparaban la activación del programa, interceptando las comunicaciones a partir de ese momento. Una pequeña red Echelon a la española…

Y todo eso coordinado desde un local de aspecto inocuo, en el pequeño pueblo al que ahora me dirigía, bajo una lluvia y frío intensos. Más intensos cuando te desplazas sobre dos ruedas.

El local donde se guarece la base de operaciones del agente Juan tiene una apariencia totalmente inofensiva desde el exterior, aunque entre sus paredes se ha ocultado uno de los canales de información directa más importantes del Gobierno de España.

Aparqué la moto en la entrada, y tras franquear la verja metálica, crucé la primera puerta. A la izquierda, cajas con restos de componentes electrónicos, un cuarto de baño y un armario repleto con primeras marcas. A David siempre le ha gustado vestir bien. Sigo avanzando entre cajas de componentes eléctricos y llego a la segunda puerta, que conduce a otra sala repleta de ordenadores, impresoras y más piezas informáticas. La tercera puerta da acceso al despacho. Un poco más ordenado. Un ordenador conectado a dos inmensas pantallas preside la mesa de trabajo. Enfrente, cubriendo toda una pared, un enorme mapa del mundo de 3 metros de largo por 2 de alto ante el que posó para la foto publicada en *El Palestino,* cuando todavía trabajaba para el CNI y no podía dar la cara. Y a la derecha, el cuarto de los servidores y el generador eléctrico, que evitaría que una caída del fluido eléctrico impidiese a David continuar recibiendo la información de sus «agentes» sobre el terreno. Veinticuatro horas al día. Siete días a la semana.

—¿Así que ahora quieres conocer el mundo de los hackers? —me preguntó sentado tras las pantallas, sonriendo con la ironía y paternalismo al que ya me tiene acostumbrado—. ¿Y qué parte exactamente?

—¿Cómo que qué parte? Pues no sé… ¿hay más de una?

David negó con la cabeza, en un gesto que le he visto hacer en muchas ocasiones. Cada vez que le preguntaba una estupidez.

—*Phreaking*, ingeniería inversa, *hacking wifi*, ingeniería social, forense, *pentesting*, *exploits*, hacktivismo… Pero ¿tú qué crees que es un hacker?

—¿Un pirata informático? —respondí haciéndome eco de un prejuicio repetido en miles de películas, informativos y artículos periodísticos.

—Mal empiezas. Si pretendes acercarte a la comunidad hacker insultándolos, no te van a recibir bien. Un hacker es todo lo contrario a un ciberdelincuente. Un hacker es un sabio, un investigador tecnológico, un creador… un hombre que habla con las máquinas.

—Pero todas las noticias que salen cada día sobre hackers…

—Eso es culpa de vosotros, los periodistas, que necesitáis titulares llamativos y frases sencillas en artículos asequibles. Pero el mundo de la seguridad informática, en el siglo XXI, no es sencillo ni asequible. Es inmenso. Global. Afecta a todo y a todos, y no se puede resumir en un titular periodístico. Ni siquiera en un libro.

Desde el principio David se mostraba profundamente escéptico con mi capacidad para afrontar un tema de tales proporciones, y tenía motivos. Él estaba familiarizado con las infinitas ramificaciones e implicaciones del término *hacking*. Yo no. Todavía creía que la seguridad informática era un problema limitado a las grandes empresas y el espionaje industrial o militar. Nada más lejos de la realidad.

—Tu ordenador está infectado —me espetó sin la menor anestesia—, me apostaría el cuello. Y si tienes un smartphone, posiblemente también, como le ocurre a mucha gente.

—Vale, en mi caso es posible que alguien sintiese interés, pero ¿quién va a querer

espiar a mi madre, o a tu hija, o al vecino del tercero?

—La filosofía de internet es compartirlo todo gratis, y eso tiene sus riesgos. La falta de conocimientos de muchos usuarios la aprovechan los del «lado oscuro» para meter cosas maliciosas.

A medida que David desarrollaba su argumentación, empecé a sentir temor.

—La mayoría de la gente pulsa en el primer botón que le ponen delante en una web, lo que equivale a suicidarse. Los más torpes ni siquiera tienen antivirus, que sin ser una panacea es algo muy recomendable.

Yo asentí con la cabeza sin añadir nada.

—Y los que tienen antivirus se creen que con eso basta. Y se equivocan. Ahora los ataques llegan de todos lados. No solo de la creciente industria del cibercrimen, que ya mueve más pasta que el tráfico de armas o la prostitución. A ellos les interesa todo lo que hay en tu ordenador: datos bancarios, fotos, vídeos, cuentas de email… Todo vale dinero. Pero también interesa lo que hay alrededor. Tu conexión wifi, tu módem, también puede emplearse para cometer un delito que luego te vas a comer tú. Por no hablar de tu teléfono móvil. La industria del *malware* está creciendo más en el desarrollo de ataques a teléfonos móviles que a ordenadores, y eso es porque ahora llevas tu vida en el móvil. Cuentas de Facebook, Twitter, WhatsApp, facturas… todo convenientemente geolocalizado en cada momento. Y tu vida vale dinero. Por eso te la roban.

—Pero ¿quién te la roba?

—Uf, el mercado es muy amplio. Desde el que quiere apropiarse de las contraseñas de tu banco, a hacktivistas que quieran utilizar tu ordenador a distancia para un ciberataque de protesta contra una empresa. El vecino de abajo que piratea tu wifi para bajarse porno infantil, que te atribuirán a ti si la policía se planta en tu casa siguiendo el rastro de alguna imagen. Ciberdelincuentes rusos, ucranianos o chinos que utilicen tus cuentas de Facebook o mail para abrir líneas de blanqueo de dinero a través de casinos *online*… Y lo mejor es que no hay vacuna posible. La seguridad informática absoluta no existe.

—¿Cómo que no existe? Tiene que haber alguna forma de protegerte.

—No.

Se hizo un silencio incómodo. Parecía que la investigación había concluido antes de comenzar. David no dejaba un resquicio a la esperanza. Según su conocimiento en la materia, que no es poco, no había solución…

—Pero vamos a ver, David, existen montones de empresas de seguridad que viven de proteger a sus clientes. Hay una industria de antivirus y programas defensivos para proteger tu ordenador o tu teléfono… ¿Me estás diciendo que todo eso es mentira?

—Digamos que la protección es relativa.

—Joder, pero aclárate…

David se giró en su sillón enfrentándose a una de las pantallas y tecleó algo en el

navegador. Buscaba la sección de noticias de Google. David no es amigo de los diarios en papel. Pocas veces le he visto leer un periódico impreso. Sin embargo, sigue puntualmente la actualidad a través de los diarios *online*.

—Aquí está. Edward Snowden… ¿Has leído algo sobre él?

—Claro, está en todos los informativos desde hace unos meses.

En junio de 2013, el informático Edward Snowden revolucionó al mundo al filtrar cientos de miles de documentos en los que se demostraba que la NSA (la Agencia de Seguridad Nacional estadounidense) tenía la capacidad para espiar a todos los ciudadanos del mundo. Incluyendo jefes de Estado, presidentes y reyes. Nadie que tuviese un ordenador o un teléfono móvil estaba a salvo.

—Piénsalo, Toni. No hay antivirus que te proteja de esto. Una cosa es protegerte de un delincuente informático, y otra de los gobiernos. Si las grandes compañías como Google, Facebook, Yahoo, Hotmail, Twitter, WhatsApp, etcétera, pactan con un servicio de Inteligencia el acceso a la tecnología que controla tus mensajes, tus redes sociales o tus archivos de datos, dejando «puertas traseras», nadie puede protegerte. Y cuando no pactan, los servicios de Inteligencia van y les pinchan el cable directamente. El mérito de Snowden fue decírselo a la opinión pública, pero los que entienden de estas cosas lo saben desde hace… no sé, cuarenta años. La información es poder, y tener toda la información es tener todo el poder. Hoy casi nadie guarda una cartilla del banco bajo el colchón, ni escribe sus intimidades en un diario, ni pega sus fotos personales en un álbum de cartón. Hoy toda nuestra información, y toda nuestra vida, entra en un disco duro. ¿Y de verdad alguien se creía que quien tenga el poder para acceder a esa información iba a renunciar a él por cuestiones éticas o morales?

—Pero… ¿qué puede querer la NSA de mí?

—La idea es recogerlo todo y luego ya se verá lo que interesa. No es que tengan un interés a priori, sino que cuando encuentran algo puedan volver atrás y rastrearlo. En los Estados Unidos, tras los atentados del 11-S los ciudadanos tuvieron que elegir entre seguridad y privacidad, y eligieron lo primero.

—Pero entonces… estamos vendidos.

—Claro. Todos estamos vendidos. Pero si hablamos de piratillas informáticos, al menos podemos subir el precio.

—¿Qué quieres decir?

—Gene Spafford, profesor universitario de ciencias computacionales y experto en seguridad informática, dijo: «El único ordenador seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él». Y Spafford estaba cometiendo el error de confiar en la lealtad de los guardias… No hay garantías. No existe un sistema informático seguro al cien por cien, pero existen muchas herramientas para ponérselo un poco más difícil al atacante. Son capas de cebolla con las que proteger, capa a capa, tu vida digital. Y

si tienes suerte, y el atacante no va directamente a por ti o no tiene suficiente motivación o tiempo, probará con una víctima más fácil. Ocurre todo el rato. Igual que un leopardo preferirá cazar al antílope más lento o pesado, o un ladrón paseará por el aparcamiento de un centro comercial buscando el coche más vulnerable. Si el tuyo está bien cerrado, con las ventanillas subidas, un cepo en el volante y una cadena en los pedales, no significa que sea imposible robarlo, pero el ladrón preferirá probar con cualquier otro. Eso sí, con respecto a los servicios de Inteligencia, no importan demasiado las medidas que tomemos, sino el interés que podamos tener para ellos. Mejor olvidarlo.

—¿Y cómo puedo conocer esas medidas de protección?

—Saca tu cuaderno y toma nota, porque te espera un largo trabajo si quieres comprender cómo funciona ahora el mundo…

David R. Vidal no pertenece a la comunidad hacker. No asiste a los certámenes, congresos y reuniones, como CyberCamp, RootedCON, No cON Name, Navaja Negra, Secumática, las Jornadas TIC y demás CON. Ni tiene relación con los principales exponentes de la seguridad informática en el país, como yo lo haría a partir de entonces. Él va por libre. No le preocupa la investigación y divulgación de vulnerabilidades, no escribe *papers* con sus aportaciones informáticas, no intercambia (gratis) sus códigos con otros hackers… David es un profesional y prefiere explotar esas habilidades al servicio de la Seguridad Nacional… o privada. Quien pague mejor.

De hecho, durante aquella visita, David simultaneaba la corrección de *Diario de un espía,* con su nuevo proyecto informático vinculado a GlobalChase: el GlobalChase ORAK, una ambiciosa Plataforma de Análisis de Inteligencia e investigación de futuros…

Ante todo esto, no es de extrañar que David se convirtiese en sospechoso cuando la empresa rusa de protección informática Kaspersky descubrió el virus Careto, un *malware* espía que operaba desde 2007, infectando ordenadores en organismos, instituciones y empresas en treinta países, grabando conversaciones de Skype, haciendo pantallazos y robando información confidencial.

El hecho de que el código incluyese fragmentos en español, y su vinculación con Gibraltar y Marruecos, hizo que en 2015 algunos medios y blogueros marroquíes señalasen a David R. Vidal como el posible programador de Careto.[10] Sobre todo después de que David confesase públicamente, tras la publicación de su libro, que en 2005 el CNI le había encargado la misión de obtener los números de los teléfonos móviles de «personas de interés» en Marruecos… Por no hablar de que en otro capítulo de su libro mencionaba el diseño de un troyano y realización de pruebas en «cierto país africano», esta vez no para el CNI sino para un «estamento oficial» que no quiso aclarar. Eso sí, David siempre ha negado la menor relación con Careto o cualquier programa semejante. De hecho, lo ha negado con mucho énfasis… tal vez demasiado.

En cualquier caso, la acusación de ser el autor de Careto implicaría un nuevo viaje a su «búnker» en el norte en 2015. En 2013 eso aún quedaba lejos y yo debía regresar a Madrid. Al día siguiente tenía una cita con los compañeros de *Equipo de investigación* para hablar sobre los Ángeles del Infierno…

Cuando dejé el local de David, seguía lloviendo. Arranqué con la intención de regresar a la capital de una tacada, pero no había recorrido ni 60 kilómetros cuando el asfalto mojado y el exceso de carga me hicieron salirme de la carretera y sufrir mi primer accidente de moto.

No fue grave, aunque las cicatrices que conservo de aquel día me ayudarán a recordar que no se puede menospreciar a la lluvia sobre dos ruedas. La moto sufrió más que yo. La caída partió el pedal del freno trasero y el estribo derecho, y tuve que recorrer más de 500 kilómetros apoyándome en el estribo trasero y forzando la pierna derecha, cuya rodilla había recibido el mayor impacto.

A la mañana siguiente me presenté ante los compañeros de La Sexta lleno de magulladuras y cojeando ostensiblemente. Y así lo recogieron las cámaras de *Equipo de investigación* en el episodio «Golpe a los Ángeles del Infierno», que se emitiría ese mismo mes de octubre.[11]

Cuando Ana, la reportera de La Sexta que me entrevistó, me deseó una pronta mejora, le respondí con una sonrisa, creyendo que para conocer el mundo hacker bastaba con un teclado de ordenador y movilidad en los dedos:

—Tranquila, para el próximo libro no voy a necesitar las piernas.

Pensaba en horas de investigación, quizá en tardes de lectura… Tenía mucho por delante. En ese momento ni siquiera sabía que ese mismo mes de octubre, el FBI y la DEA (muy probablemente con la ayuda en secreto de la NSA) habían dirigido el primer gran ataque contra la Deep Web en los Estados Unidos, desmantelando el sitio Silk Road, la primera gran tienda *online* de drogas, y deteniendo a su webmaster, Ross William Ulbricht, alias «Dread Pirate Roberts». Una fecha que marcaría un antes y un después en la historia de la internet oscura.

Tampoco que casi por las mismas fechas, en León, se celebraba la séptima edición del congreso de seguridad informática del Instituto Nacional de Tecnologías de la Comunicación (INTECO), ahora conocido como Instituto Nacional de Ciberseguridad (INCIBE). Ni que en esa séptima edición de sus conferencias participaban algunos de los personajes clave para mi comprensión del mundo de la ciberseguridad. *Hacktivistas,* responsables de seguridad en alguna de las redes sociales más importante del mundo, informáticos forenses…

—Comparado con mis trabajos anteriores, esto será un paseo… —le aseguré a la periodista de La Sexta muy tranquilo. Me equivocaba.

Capítulo 2
Red de mentiras

«El que dice una mentira no sabe qué tarea ha asumido, porque estará obligado a inventar veinte más para sostener la certeza de esta primera.»

Alexander Pope

«Los bulos *(hoaxes)* que circulan por internet usan la debilidad del ser humano para asegurar su replicación y distribución. En otras palabras, utilizan los resquicios del Sistema Operativo Humano.»

Stewart Kirkpatrick

Solo por que mil voces lo repitan, no necesariamente es verdad

«Niño, tápate la cabeza, que por ahí se va el calor…» «Niño, no te bañes después de comer, que te va a dar un corte de digestión…» Mi madre, una santa, no es una excepción. También se ha creído las mentiras que le han contado sus mayores, y así me las transmitió. Pero lo cierto es que por la cabeza no se pierde más calor corporal que por un brazo, y el síncope de hidrocución (lo que los profanos llamamos corte de digestión) tiene más que ver con el cambio de temperatura que con la comida.

Durante nuestra infancia, el cine, los cómics, la televisión y a veces nuestra propia y querida madre van depositando en nuestro pequeño inconsciente miles de informaciones falsas, que vamos clarificando a medida que nos hacemos mayores, y nuestro nivel cultural aumenta.

Ni Vicky ni ningún otro vikingo utilizó jamás cascos con cuernos. Los guerreros escandinavos eran en verdad fieros y sanguinarios a ojos de los pueblos conquistados en sus expediciones, pero entre los miles de yelmos, cascos y armaduras descubiertos por los arqueólogos, jamás se encontró ningún cuerno ornamental. Estos solo se utilizaban como vasos. La idea de los cascos con cuernos fue un invento del romanticismo del siglo XIX para ilustrar la fiereza de aquellos guerreros.

Cristóbal Colon no descubrió América. Cinco siglos antes el explorador vikingo Leif Eriksson, «el Afortunado», pisó Terranova y creó el primer asentamiento comercial, que se mantuvo en suelo americano al menos hasta 1347. Y Colón tampoco empleó tres carabelas en su viaje, sino dos. Solo *La Niña* y *La Pinta* eran carabelas. La nave capitana, *La Santa María*, era una nao, una embarcación de casco redondo con velas cuadrangulares, inspirada en las cocas mercantes medievales.

Los Reyes Magos no eran tres, y no se llamaron Melchor, Gaspar y Baltasar. Al menos en la Biblia no se mencionan sus nombres ni su número en ningún versículo. Los armenios, por ejemplo, sugieren que fueron doce, y en las catacumbas del Vaticano se les representó como dos, cuatro… y ninguno negro. Baltasar no adquiere esa raza en la imaginería popular hasta el siglo XV.

Thomas Alva Edison no inventó la bombilla, solo tuvo éxito en su comercialización. El inventor alemán Heinrich Goebel ya la había registrado como patente en 1854, veinticinco años antes. El ruso Aleksandr Lodygin, por su parte, también registró una patente de la bombilla incandescente mucho antes que Edison.

Napoleón Bonaparte no era un tirano bajito. O al menos no lo segundo. Se calcula que medía metro setenta, un centímetro más que la media francesa de la época. El rumor sobre su estatura lo crearon los ingleses, dado que acostumbraba a emborracharse con su tropa para afianzar lealtades, haciendo correr el rumor de que el emperador de Francia era de «baja ralea».

Don Miguel de Cervantes no quedó manco en Lepanto. O al menos no perdió

ningún brazo en la histórica batalla naval de 1571 entre el Imperio otomano y la Liga Santa. Se le llamaba «el Manco» porque perdió movilidad en una de sus extremidades, pero no le amputaron la mano, ni por fortuna sus heridas le impidieron escribir *El Quijote.*

Sherlock Holmes jamás dijo «Elemental, mi querido Watson». En la saga de novelas sobre el genial personaje escrita por sir Arthur Conan Doyle, nunca se incluyó ese latiguillo. Lo más parecido aparece en la novela *El sabueso de los Baskerville,* cuando el detective dice a su ayudante*:* «Interesante aunque elemental». O «Me temo, querido Watson, que la mayoría de sus conclusiones son erróneas». No fue hasta 1939, nueve años después de la muerte de Conan Doyle, cuando se pronunció por primera vez esa frase en una película titulada *Las aventuras de Sherlock Holmes*. El resto de autores literarios y cinematográficos se limitaron a replicarla. Lo mismo ocurre con la célebre frase «Beam me up, Scotty», que jamás se pronunció en la serie original de *Star Trek.*

El Cid no ganó ninguna batalla después de muerto. Cuando Rodrigo Díaz de Vivar falleció en1099, Valencia estaba ya condenada, y sus soldados decidieron llevarse el cuerpo del héroe al monasterio de San Pedro de Cardeña, para evitar que cayese en manos enemigas.

Los toros no atacan ante el color rojo, sino ante el movimiento. El rojo de los capotes taurinos solo sirve para disimular la sangre del animal. Algo que cualquier aficionado a la tauromaquia puede comprobar poniéndose ante un miura vestido de verde, azul o blanco y agitando las manos. A ver qué pasa…

El profeta Muhammad (saas) jamás pronunció la frase «Si la montaña no va a Mahoma, Mahoma irá a la montaña». Esa sentencia no aparece en ninguna aleya ni azora del Corán, ni tampoco se recoge en ningún hadiz. Forma parte de una parábola inventada por el filósofo británico Francis Bacon, pionero del método experimental en cuestiones científicas, con el fin de ejemplificar un concepto de sus teorías. Y llamar Mahoma al fundador del islam es tan respetuoso como llamar Suso al fundador del cristianismo.

El polígrafo no detecta mentiras, ni es una «máquina de la verdad». El aparato que registra las variaciones de presión arterial y ritmo cardiorrespiratorio, inventado en 1938 por Leonarde Keeler, fue acogido con entusiasmo por el Departamento de Policía de Berkeley (California) a mediados del siglo XX, pero hoy ningún tribunal lo admite como prueba, por su cuestionable falibilidad.

No utilizamos el 10% del potencial del cerebro. El origen de ese mito radica en una mala comprensión de las investigaciones neurológicas de finales del siglo XIX y principios del XX, cuando se sugirió que solo un 10% de las neuronas están «activadas» en un momento determinado, y que solo el 10% de las células del cerebro son neuronas. En realidad, utilizamos el 100%, aunque algunos lo utilicen mal…

Isaac Newton no descubrió la gravedad por que le cayese una manzana en la cabeza (ya había formulado su teoría de la gravitación antes); los elefantes no acuden

a un cementerio de elefantes para morir, como bien saben los cazadores, y fue la película *Tarzán de los monos,* dirigida en 1932 por W. S. Van Dyke, la que cimentó en Occidente la leyenda africana; el caballo blanco (que no tordo) de Santiago se llamaba *Blanco,* pero era pardo con manchas negras (así aparece en la escultura de la catedral de Burgos); Walt Disney ni está criogenizado ni dibujó a Mickey Mouse (el autor del famoso ratón fue Ub Iwerks); los avestruces no esconden la cabeza bajo tierra al sentir peligro… atacan. Y así hasta el infinito y más allá.

Podría dedicar todo un libro a estos ejemplos. La lista de mentiras que damos por ciertas, de generación en generación, es inmensa. Todas esas falsas creencias se transmitieron y asentaron mucho antes de que existiese internet y/o las redes sociales. Seguro que todos conocemos a alguien que asegura haber visto el programa *Sorpresa, Sorpresa* con Ricky Martin en el armario…

Internet no genera falsas noticias. Solo amplifica las ya existentes.

Miguel Bosé murió en un accidente de tráfico en 2015. Alguien creó una web en Facebook con el siguiente mensaje: «El domingo (26 de julio), aproximadamente a las 11 a.m. PDT, nuestro amado músico falleció. Miguel Bosé nació el 3 de abril de 1956 en Panamá (ciudad). Lo vamos a extrañar, pero nunca lo vamos a olvidar. Por favor, mostrad vuestra simpatía y condolencias a través de comentarios en esta página», y se encendió la mecha. La noticia pasó a Twitter y se extendió rápidamente, haciendo que el mensaje «Murió Miguel Bosé» fuese durante horas tendencia en esa red social.

Pero no era la primera vez que el famoso cantante y actor «moría». En marzo de 1986 no existían las redes sociales, ni los blogs, ni la internet que conocemos. Y sin embargo, numerosos medios de comunicación publicaron la noticia de la muerte de Miguel Bosé. El bulo creció día a día. Surgieron testimonios de enfermeras que aseguraban haberle visto en varios hospitales, declaraciones de médicos, aseveraciones de testigos… Nadie dudó de la noticia, y todos la replicaron sin confirmarla. Con un agravante. La noticia aseguraba que Bosé había muerto de sida, todo un estigma social en 1986.

El 3 de abril de ese año Mercedes Milá tuvo la exclusiva en su programa *De jueves a jueves*. Mientras los medios lo daban por muerto de sida, Bosé se encontraba en Francia e Italia grabando con Celso Valli, para WEA, el disco *Salamandra*, en el que se incluyen temas legendarios del cantante y actor como «Nena», «Partisano», «Aire soy» o «Cuando el tiempo quema». Bosé detuvo la grabación de *Salamandra* yviajó hasta los estudios de RTVE en Madrid para conceder aquella entrevista y de paso resucitar de entre los muertos.[12]

José M. Hermida analiza el caso en su libro *La estrategia de la mentira: Manipulación y engaño de la opinión pública. De los grandes escándalos financieros al caso Bosé*.[13] Pero lo que Hermida no puede incluir en su ensayo es toda la angustia, el miedo y la desesperación gratuita que sintió, al menos durante algunas horas o días, la familia de Bosé y sus amigos más cercanos al leer la noticia de su

muerte. Como los insultos, burlas y amenazas que sufrieron durante años los componentes del grupo musical La Oreja de Van Gogh, porque en 2001 algún imbécil hizo correr el rumor a través de una cadena de emails de que habían sido expulsados de un programa de Pedro Ruiz por hacer apología de ETA. Ni los continuos desmentidos del humorista y presentador han conseguido evitar que la leyenda urbana resucite cada cierto tiempo.

Miguel Bosé sabía que no estaba muerto. Los miembros de La Oreja de Van Gogh sabían que jamás fueron expulsados de un programa de Pedro Ruiz por hacer apología de ETA. Y Ricky Martin sabía que nunca estuvo escondido en un armario, al menos para dar una sorpresa a una joven con un perro y un bote de mermelada… pero ¿y los demás?

Todos hemos sido víctimas de falsos rumores alguna vez. Las buenas personas, esas con amigos que las quieren de verdad, con frecuencia tienen la posibilidad de enterarse de las mentiras que circulan en el vecindario, el instituto o el puesto de trabajo: «En serio te has liado con fulanito? Me lo ha contado menganita…», «Es verdad que tienes cáncer?», «¿Es cierto que estuviste en la cárcel por tal delito?»…

Solo nosotros sabemos la verdad sobre nuestros actos. Nadie más. Pero lo que antaño se circunscribía al patio de vecinos, al colegio o a la oficina ahora navega por la red y llega a todo el mundo. Ese es el principio del ciberacoso.

Cuando tú eres el protagonista de los falsos rumores, mentiras y bulos, que se replican de forma exponencial a través de las redes sociales, blogs, webs y demás *sites* de internet, te encuentras en una situación privilegiada para comprender qué fácil es mentir en la red, y cuánto eco puede encontrar esa mentira en todo el planeta.

Un altavoz de mentiras

El 25 de febrero de 2014 mi perfil en Twitter recibió cientos de nuevos seguidores de una tacada. (Detesto el concepto «seguidores».) No llegué a *trending topic*, pero por alguna razón, mi nombre aparecía reseñado en cientos de tuits esa madrugada. Sentí curiosidad, y busqué la razón. No tardé en descubrirla.

El periodista de la CNN Fernando del Rincón había viajado a Caracas para realizar una serie de reportajes a raíz de los disturbios entre chavistas y antichavistas. Entre los entrevistados estaba Alberto «el Chino» Carías, mi mentor en Caracas durante mi infiltración en el terrorismo internacional.

Durante toda la entrevista, el Chino Carías, subsecretario de Seguridad Ciudadana de Caracas y jefe militar del Movimiento Revolucionario Tupac Amaru – Capítulo Venezuela, intentó mostrarse como un pacifista:

—Antes de nada yo quiero aclararle al público norteamericano, a los pueblos del mundo, que nosotros condenamos la violencia, que se escuche bien, condenamos la violencia… provenga de donde provenga —decía.

Mi antiguo «camarada», más delgado que de costumbre, respondió con ensayada retórica las incisivas preguntas del periodista. Y antes incluso de que Del Rincón expusiese el tema, Carías se le adelantó, afirmando que todos sus problemas legales eran culpa mía y no los homicidios, robos, torturas, etcétera, que me había confesado.

—Me han satanizado. A mí se me infiltró en la organización un sujeto de los servicios secretos europeos. Duró dos años en Venezuela. Y me hizo unos montajes de unos vídeos y me sacó un libro llamado *El Palestino,* con el único objetivo de satanizar la labor social que nosotros venimos desarrollando como revolucionarios. Y no es un delito, y no soy yo quien para determinar si el Chacal es o no terrorista. (…) A raíz de ese vídeo y de ese libro que va por la décima edición, es que yo he tenido ese conjunto de problemas no solamente en Europa sino en algunos países de América Latina. Eso se llama satanizar a una organización social y revolucionaria.[14]

El *hashtag* @chinomrta se convirtió esa noche en tendencia de Twitter en algunas provincias venezolanas como Valencia, la ciudad donde yo había tenido mi primer contacto con las guerrillas colombianas y donde conocí a la madre de Carlos el Chacal. Pero en todo Venezuela miles de televidentes antichavistas que estaban siguiendo la entrevista de Fernando del Rincón en CNN reaccionaron a las declaraciones enlazando el reportaje *El Palestino: historia de un infiltrado* que el canal de televisión Antena3 había emitido el 20 de octubre de 2010, resumiendo, de forma un poco simplista, mi libro *El Palestino,* que no tiene décima edición como dice. En dicho documental se incluían muchas de las grabaciones que había realizado durante los meses que pasé en Venezuela (no dos años, como afirmaba el Chino ante la CNN).[15]

Ante las cámaras de la CNN, el Chino intentaba desacreditar mi trabajo pero no

podía negar la evidencia de los asesinatos que confesó ante mi cámara, ni de que participé en la grabación de un comunicado donde él, y una docena de componentes del Movimiento Revolucionario Tupac Amaru, encapuchados y armados hasta los dientes, llamábamos a las guerrillas latinoamericanas a alzarnos en armas contra el gobierno de Colombia y los Estados Unidos tras la muerte del comandante de las FARC Raúl Reyes.[16]

Las imágenes que se recogían en el reportaje de Antena3 eran incontestables. El Chino, encapuchado y rodeado de hombres armados (yo era uno de ellos), justificaba el yihad, y la persecución de los imperialistas: «… hay que atacarlos dondequiera que se encuentren, así sea en sus casas».[17] Sin embargo, Carías aseguraba a la CNN que «nosotros condenamos la violencia… provenga de donde provenga». Y una vez más los antichavistas reaccionaron utilizando el reportaje de Antena3, irrefutable, para desacreditar las afirmaciones del Chino.

Me molestó y continúa molestándome que se instrumentalice políticamente mi trabajo. En cuanto se publicó mi libro hice llegar un ejemplar a Carlos el Chacal y otro al presidente Hugo Chávez. El 26 de mayo, un día después de su publicación, el embajador de Venezuela en España, don Isaías Rodríguez, emitió un comunicado oficial advirtiendo que «los medios españoles manipulan la información del libro *El Palestino*»[18]. Los medios antichavistas se unieron después a esa instrumentalización. Porque la mayoría de los internautas se limitan a repetir lo que otros dicen, sin molestarse en confirmarlo.

Lo que el Chino no dijo a la CNN, mientras intentaba presentarse como un pacifista ante la audiencia, es que antes, exactamente el 5 de octubre de 2012, había declarado públicamente a la periodista alemana radicada en México Sandra Weiss que me habían condenado a muerte:

—Somos aliados políticos de la ETA y las FARC, no te voy a dar más detalles por el mal antecedente que tuvimos con el español «el Palestino», que se infiltró en nuestra organización y grabó nuestras actividades con cámara oculta sin decir que era un periodista. Lo hemos condenado a muerte.[19]

De todas formas, tampoco era nada nuevo. El mismo Carías me había notificado personalmente esa sentencia de muerte. Y lo hizo vía email, el 28 de febrero de 2011:

> … tu maldito me tienes que indemnizar por los daños causados al negro cheo lo detuvieron los servicios secretos de europa por su relación conmigo y ilich todo loque hiciste fue engañarnos pero no te preocupes delator marico maniaco depresivo que tarde o temprano la larga mano de un juicio revolucionario contra ti se cumplirá en cualquier parte del mu do de eso puedes estar seguro tranfuga… (sic)

He respetado la literalidad y redacción del mensaje tal y como lo recibí. Fue la última vez que tuve noticias directas suyas. Sin embargo, el Chino continuó citándome en numerosas entrevistas, siguió extendiendo rumores por las redes, e incluso llegó a asegurar, ante las cámaras de Primicias Veinticuatro, que yo había sido

el autor de la fotografía del presidente Chávez, muerto y en féretro, que circuló por internet en enero de 2013.

Chávez muere en la red: un golpe digital a la credibilidad de los medios

En su delirio de odio, el Chino aseguraba que el agente secreto Antonio Salas había regresado a Venezuela de manera clandestina, para tomar la primera foto del presidente Chávez muerto, filtrándola a los medios capitalistas e imperialistas. Pero aquella foto era un *fake*, un fraude, como todo lo demás. El Chino no podía saberlo, pero mientras me buscaba obsesivamente por las calles de Caracas, yo estaba en México, trabajando en mi libro *Operación Princesa*.

Los delirios de Carías y su resonancia en las redes sociales tienen una explicación. Como aquella foto falsa de Hugo Chávez publicada mes y pico antes de su muerte real. Y es que internet es el mayor altavoz de la historia de la humanidad. Un megáfono que nos permite lanzar al mundo cualquier afirmación, falsa o real. Alguien la escuchará y la repetirá.

En enero de 2013, el estado de salud de Hugo Chávez era un secreto de Estado. Lo que no había conseguido la Casa Blanca, ni sus aliados en Israel o Europa, lo consiguió un sospechosamente oportuno cáncer: silenciar al Comandante. Y mientras los médicos cubanos luchaban contra viento y marea por salvar la vida al presidente más carismático de la historia de América Latina, los medios bolivarianos callaban sobre su real y precario estado de salud. Así que la oposición aprovechó el silencio para hacer ruido.

La primera foto falsa de Chávez muerto apareció en las redes el 8 de enero, y corrió por todo el mundo como un reguero de pólvora destinado a detonar un polvorín político. De inmediato, y sin contrastarla, reputados medios de comunicación en todo el planeta se hicieron eco, publicándola y creando una angustia, dolor y miedo totalmente innecesarios entre los devotos del Comandante.

Twitter se incendió. La oposición antichavista y sus aliados norteamericanos o europeos querían creer. Los seguidores del Comandante se negaban a hacerlo. Pero cuando una imagen digital da el salto al papel impreso, parece legitimada, y era tal el entusiasmo demostrado por los detractores de Chávez, que muchos medios no dudaron en imprimirla en sus periódicos y revistas.

Y Twitter, al igual que creó el engaño que el Chino Carías me atribuía a mí, también aclaró el *fake*. La imagen de Chávez en el ataúd era un fraude realizado a partir de un fotograma tomado de la serie de televisión *Lost (Perdidos),* en la que aparecía el actor Terry O'Quinn en un ataúd, en el capítulo 22 de la tercera temporada.

Apenas dos semanas después la historia se repetía con una nueva foto de Hugo Chávez al borde de la muerte…

El 24 de enero de 2013, día de San Francisco de Sales, patrón de los periodistas, el prestigioso diario español *El País* llevaba a su portada uno de esos titulares que

aspiran a hacer historia. Prohibiendo su reproducción y recalcando que poseía los derechos mundiales de la imagen, *El País* titulaba: «El secreto de la enfermedad de Chávez», y añadía:

> La imagen que hoy publica EL PAÍS, tomada hace unos días, muestra un momento del tratamiento médico en Cuba, según las fuentes consultadas por este diario. Ni el Gobierno venezolano ni el cubano han dado información detallada del tipo de cáncer que sufre Chávez, ni de los cuidados que está recibiendo, lo que ha generado una agria controversia y la exigencia de transparencia por parte de la oposición venezolana.

Una vez más, las redes se incendiaron. Solo que ahora no se trataba solamente de medios digitales, sino que uno de los diarios de mayor prestigio en Europa legitimaba la imagen llevándola a su primera página. Pero de nuevo era un fraude. Afortunadamente, en esta ocasión, nadie intentó responsabilizarme de ello…

Habían comprado la foto a la agencia Gtres OnLine por una suma, sin duda generosa.Gtres es en realidad una fusión de varias agencias de prensa muy veteranas y conocidas en España, doy fe.

La imagen de portada de *El País* en realidad pertenecía a un fotograma de un vídeo que circulaba por YouTube desde agosto de 2008. Se trataba de una operación a un paciente acromegálico de cuarenta y ocho años que, dependiendo del ángulo de la cámara, podía tener un parecido notable con Hugo Chávez.[20]

Inmediatamente *El País* retiró la imagen y publicó una editorial pidiendo disculpas.[21] Dos días después, José María Irujo y Joseba Elola salían al paso para explicar con detalle la historia de la fatal imagen que había asestado a *El País* uno de los mayores golpes en su credibilidad.[22]

La historia de la portada de *El País* es la historia de un engaño. Como tantos que se arrastran por la red. Pocas horas después de su publicación en Europa, varios medios latinoamericanos desvelaron la verdad: el autor del *fake* a *El País* se había identificado voluntariamente. Se trataba del periodista italiano Tommasso Debenedetti, que en declaraciones a Notimex se reconocía autor del fraude: «La falsa foto de Chávez, que tomé de un vídeo de YouTube, la envié la semana pasada a una agencia de Costa Rica, a la agencia estatal venezolana y a *Prensa Latina* (cubana) y nunca me imaginé que iría a terminar en la primera plana de *El País*».

Señaló que al enviar la imagen se hizo pasar por el ministro venezolano de Cultura y que su intención fue la de verificar la rigurosidad de los medios cuando deciden publicar material fotográfico.

Debenedetti había sido anteriormente autor de los rumores sobre la muerte del expresidente cubano Fidel Castro, del escritor colombiano Gabriel García Márquez y había suplantado a través de Facebook y Twitter identidades de personajes famosos, como Mario Vargas Llosa, el papa Benedicto XVI o Umberto Eco, entre otros.

No seré yo quien aplauda ni justifique la actuación de Debenedetti, ni el innecesario dolor que causó a los chavistas; sin embargo, sus «ciberexperimentos»

han demostrado una y otra vez nuestra vulnerabilidad al engaño.

Hoy, la mayor parte de la información fluye por la red. Los teléfonos fijos han pasado a convertirse en un objeto ornamental en la mayoría de las viviendas. Muchos únicamente los utilizan para conectar el módem a la red. Otros ni siquiera tienen ya teléfonos fijos. El correo postal se ha limitado al envío de paquetes, y las cartas o postales a un puñado de románticos. Las ventas de la prensa escrita han caído en picado. Y cientos de periódicos y revistas impresos tuvieron que cerrar sus redacciones, o despedir a cientos de profesionales, ante la implantación de la prensa *online*.

Hoy los equipos de redactores profesionales —y eso cuando lo son— no disponen de veinticuatro horas para completar un número finito de páginas. Antes bien, se impone la urgencia por llenar minuto a minuto los huecos inacabables de noticias, y en ese caldo de prisas proliferan los bulos. Rara vez son inocentes. Pero ¿qué es lo que buscan?

Del *hoax* de SM la reina, a la Wiki War: la información como propaganda

Todos los días, al abrir nuestros ordenadores, recibimos millones de noticias a través de los diarios digitales, las redes sociales o nuestras web habituales. La ventaja que te otorga ser el protagonista de esas informaciones es que tú, y solo tú, sabes hasta qué punto pueden ser falsas. Pero el resto de los internautas no. Como muestra un botón.

Tras su presentación en sociedad, los republicanos más recalcitrantes dirigieron sus críticas hacia su majestad la reina Letizia. Para mi sorpresa, uno de los ataques contra la todavía princesa de Asturias se amparaba en mi libro *El año que trafiqué con mujeres*. Al menos desde 2012, entre los comentarios de diferentes artículos sobre Letizia Ortiz Rocasolano publicados en las web de *El País, Hola, 20 Minutos,* etcétera, así como en los Twitter de Casa Real, Moncloa y demás, uno o varios individuos se dedicaron a colgar cientos de mensajes como este:

> **@mmousses-mmousse** @CasaReal @Hola En el libro de Antonio Salas aparece Letizia (L.O.) como prostituta de lujo. Que asco.

Evidentemente, todos los lectores de *El año que trafiqué con mujeres* saben que esa afirmación es falsa. Pero la inmensa mayoría de los internautas no leyeron mi libro, así que no era extraño que muchos se hiciesen eco de aquella falsedad.

Ingenuo de mí, yo respondí a varios de aquellos tuits identificándome como el autor del libro y explicando a los tuiteros que la información que estaban divulgando era falsa. En mi libro solo aparece una inicial, y no es L.O. Sin embargo, a aquellos internautas no les interesaba la verdad, sino utilizarme para desacreditar a la Casa Real.

«Antonio Salas, otros periodistas como usted han reconocido que Letizia aparece en su libro», me respondió el tuitero que fomentaba el bulo. «Este tío es tonto —pensé—. Qué importa lo que digan otros periodistas: yo soy el autor del libro». Estéril todo intento de razonar con los propagandistas. Inútil retarles a que explicasen en qué página aparecía esa información. Se limitaban a repetir una y otra vez, y en todo tipo de sitios de la red, la misma afirmación falsa. Ya lo dijo Francis Bacon: «Calumniad con audacia: siempre quedará algo».

En otras ocasiones son prestigiosos medios escritos los que divulgan informaciones falsas, en las que me he visto implicado.

El 26 de julio de 2012, el diario peruano *La Primera* publicaba un artículo titulado «Al Qaeda se infiltra», relatando la supuesta incursión de la organización terrorista que lideraba el jeque Osama Ben Laden en el conflicto sirio. Y para ilustrar la noticia, el periódico peruano colocaba una fotografía en la que aparece un grupo de supuestos yihadistas de Al Qaeda en lo que pretende ser un campo de entrenamiento terrorista en Siria. Bajo la foto podemos leer la siguiente leyenda:

El bloqueo de las sanciones en el Consejo de Seguridad de las Naciones Unidas contra el régimen sirio y la cercanía del país con Irak facilitaron que varias células del grupo terrorista Al Qaeda se hayan infiltrado en los grupos opositores, algo que está generando recelos en el Gobierno norteamericano y sus aliados.[23]

Pero esa foto no demuestra que Al Qaeda estuviese en Siria. Lo sé porque yo aparezco en ella. Y aunque he estado en Siria y también he tenido contacto con supuestos líderes de Al Qaeda, esa foto en concreto se tomó en Venezuela, durante la grabación del comunicado del Movimiento Revolucionario Tupac Amaru, encabezado por el Chino Carías, tras la muerte del comandante de las FARC Raúl Reyes.

El lema identificativo del diario peruano, tal y como aparece en su web es: «*La Primera*, el diario que inspira respeto». Y probablemente así sea en la mayoría de sus informaciones. Pero aunque los lectores del periódico peruano puedan argumentar en sus tertulias de café que han visto con sus propios ojos la foto de los terroristas de Al Qaeda infiltrados en Siria yo, y también todos los lectores de *El Palestino* que ya conocían esa imagen y cómo se obtuvo, sabemos la verdad.

Y ese es sin duda otro de los riesgos de internet. Podemos encontrar millones de foros y webs repletos de información contrastada, pero también millones de blogs, chats y *sites* donde tipos delirantes lanzan al mundo sus conjeturas basadas en especulaciones, sustentadas por creencias, argumentadas con elucubraciones, construidas sobre entelequias…

Hoy que la crisis económica ha mutilado el periodismo de forma tan brutal como otras profesiones, cuando redacciones enteras de reporteros se han ido a la puta calle porque sus gestores se veían impotentes para mantener abiertos sus medios, cuando cientos de diarios, revistas y magazines en papel han sido fagocitados por publicaciones *online*, programas de radio reducidos a podcasts y reportajes de televisión limitados a YouTube o Vimeo… Hoy, decía, que el periodismo de investigación cuenta con menos recursos y financiación que nunca, muchísimos de mis colegas limitan sus fuentes a dos herramientas digitales: Google y Wikipedia. Pero ¿son realmente fiables?

En agosto de 2007, todas las agencias de prensa del mundo se hicieron eco de un mismo titular: «La CIA y el Vaticano manipulan los artículos de la Wikipedia».[24]

Virgil Griffith, un joven estudiante de posgrado en el prestigioso Instituto Tecnológico de California, había desarrollado un programa informático que permitía identificar desde qué ordenadores se había modificado cada artículo en la Wikipedia, probablemente la fuente de consulta más utilizada en el siglo XXI. El WikiScanner posibilitaba identificar la dirección IP del ordenador que había realizado o modificado cada entrada y, oh sorpresa, Griffith había descubierto que, siguiendo ese rastro digital, llegaba a estamentos oficiales como la ONU, la CIA o el Vaticano.

Por ejemplo, desde ordenadores de la Agencia Central de Inteligencia se habían alterado las entradas sobre Richard Nixon, Ronald Reagan o el presidente iraní

Mahmoud Ahmadinejad. Desde un PC de la Santa Sede se habían realizado modificaciones interesadas al artículo sobre Gerry Adams, dirigente del Sinn Fein irlandés. Y también desde ordenadores asociados a las Iglesias de Jesucristo de los Santos de los Últimos Días (mormones) y Cienciología se habían manipulado entradas de la Wikipedia sobre sus respectivos cultos.

Asimismo desveló que algunos artículos habían sido modificados, de forma interesada, desde ordenadores pertenecientes a la ONU o al Gobierno de Israel, especialmente implicado en condicionar lo que los consultores de Wikipedia pudiesen leer sobre el muro de Cisjordania.

Griffith descubrió también que desde PepsiCo y ExxonMobil habían editado sus páginas para «despolemizar» sus productos o servicios. Y «desde ordenadores de la multinacional Microsoft se habría intentado disimular los masivos fallos de su consola de videojuegos Xbox…».

Y la prensa tampoco estaba libre de culpa. El WikiScanner descubrió que desde un ordenador propiedad de la agencia Reuters habían añadido «mass murdered» (asesino de masas) a la descripción de Bush. Y desde la redacción de la BBC se había corregido la biografía del exprimer ministro británico Tony Blair para afirmar que «prefería el vodka al café y que su lugar favorito para hacer ejercicio no era el gimnasio, sino el dormitorio».

Entiendo que la intención de Jimmy «Jimbo» Wales cuando fundó Wikipedia era totalmente lícita. La idea de una enciclopedia libre en la que todos podamos aportar

nuestro conocimiento, y de distribución y uso gratuito, encierra la esencia del pensamiento hacker. Compartir. Pero el hecho de que millones de periodistas, divulgadores y estudiantes la consulten como una de sus principales y más rápidas fuentes de información la convirtió de inmediato en una golosina para la difusión de propaganda. Y que tire la primera piedra quien esté libre del pecado.

En septiembre de 2015 Wikipedia llegaría a bloquear 381 cuentas de redactores que creaban entradas nuevas, o reescribían las existentes, en función de intereses comerciales o propagandísticos, y cobrando por ello.[25] Sabían que era una de las fuentes de consulta habituales por periodistas y usuarios, que luego replicarían esa información en sus medios, haciendo que la propaganda se expandiera como una mancha de petróleo sobre el océano. Y todos hemos caído en la trampa alguna vez.

Durante mi formación teórica para la preparación del personaje de Muhammad Abdallah, «el Palestino», yo mismo busqué en la red mucha información. Y también en la Wikipedia. Y me creí que aquella información era cierta. Sin embargo, yo intenté contrastarla… Perdí mucho tiempo y dinero siguiendo la pista de mitos como los «campos de adiestramiento yihadista» en Isla Margarita, o la supuesta presencia de Mustafá Setmarian en Caracas, o la organización Hizbullah Venezuela… La diferencia es que yo terminé controlando Hizbullah Venezuela (tras la detención de Teodoro Darnott), viajé a Isla Margarita y conocí a los supuestos «terroristas árabes» (cristianos maronitas libaneses cazando pichones) y descubrí que a Setmarian lo había detenido la CIA en Pakistán y jamás había pisado Caracas.[26]

Todas esas falsas informaciones, instrumentalizadas políticamente por la oposición venezolana, continúan hoy replicándose en la red. Y es probable que en el futuro otros autores crean esas y otras afirmaciones solo porque aparecen en Google o en Wikipedia. Imposible calcular cuánta desinformación similar fluye por la red.

A diario millones de perfiles sociales replican noticias como esta: «Irak podría ser el primer país en legalizar el matrimonio con niñas».[27] Se publicó en marzo de 2014 y de nuevo en julio de 2015, y prestigiosos medios de comunicación la reprodujeron en todo el planeta. Para ilustrarla utilizaban unas fotos que me resultaban familiares. Y quizá a los lectores de *El Palestino* también. Más de cuatrocientas niñas vestidas de «novia» emparejadas con hombres que podrían ser sus padres. Eran las mismas fotos que se utilizaron dos años antes para ilustrar otra noticia: «Matrimonio masivo de 450 niñas en Arabia Saudí», y antes aún, en 2009, para ilustrar otra noticia que dio la vuelta al mundo: «Casi 500 terroristas se casan en Gaza con niñas menores de diez años». Todo mentira.

Las imágenes pertenecen a una boda colectiva, sí, pero las niñas son las hermanas pequeñas de la novia que acompañan a sus cuñados al altar. Sin embargo, una y otra vez son utilizadas para ilustrar noticias falsas, que se convierten en virales en la red, y que tienen como objeto fomentar la islamofobia en Occidente. Y lo consiguen.

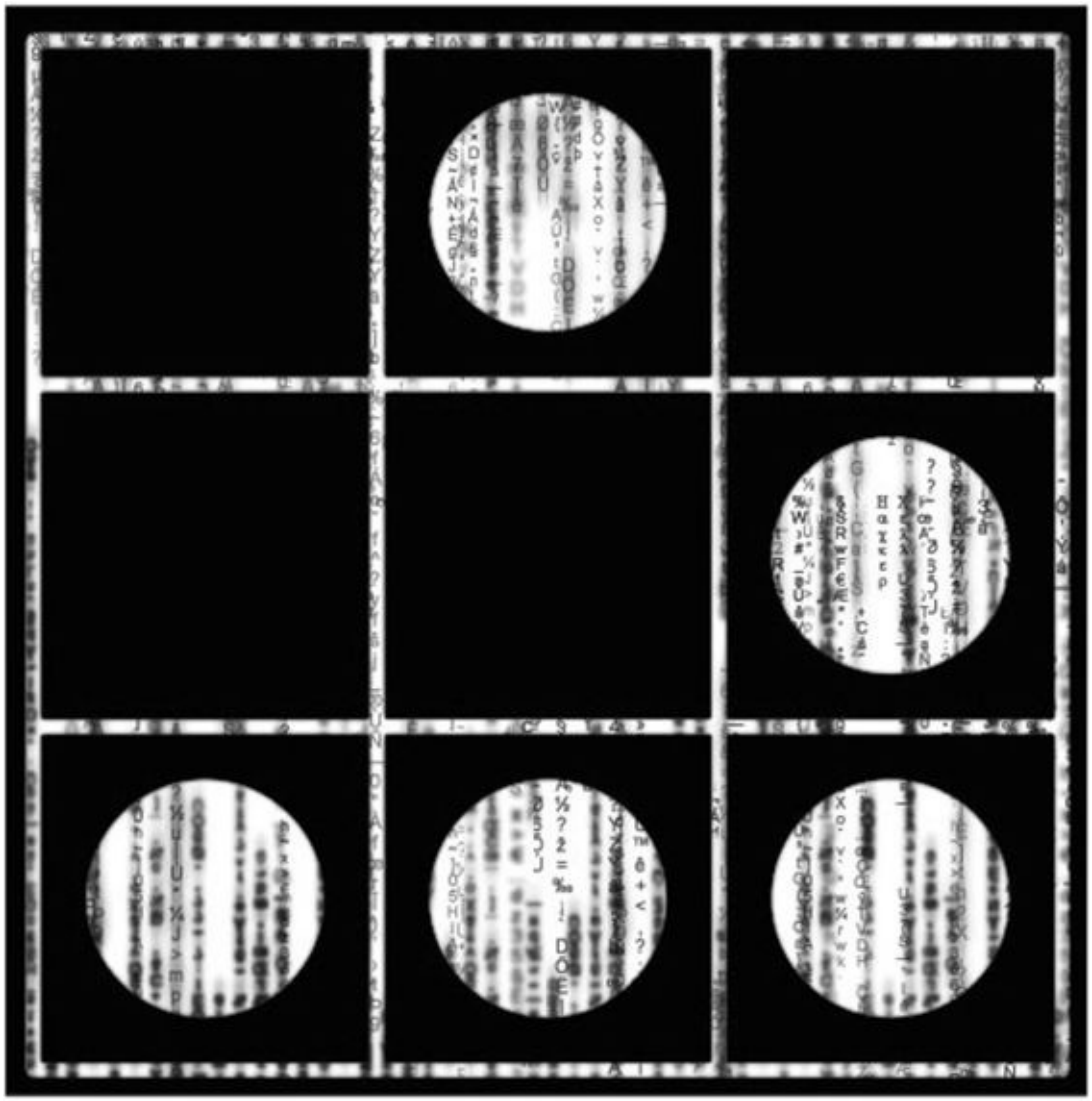
Ambar, una joven musulmana española, creó hace años el blog: «Mentiras sobre el islam»,[28] donde compila y aclara docenas de ejemplos de esas falsas noticias que

se extienden por internet como un reguero de pólvora. Infectando de odio y prejuicios, basados en falsas informaciones, a millones de internautas.

Las falsas bodas con niñas en Palestina. Sakineh, la falsa víctima. La falsa niña decapitada en Irán. La falsa fatua de Amina. El falso castigo a un niño en Irán…[29] La lista es interminable. Internet es una gran fuente de información, pero también un gran altavoz para la desinformación. Y antes de replicar un contenido, deberíamos asegurarnos de que es cierto. Sobre todo si puede generar odio o rencor hacia terceros. Las falsas noticias sobre el islam, que se multiplicaron exponencialmente tras la aparición de los asesinos del Estado Islámico y la crisis de los refugiados sirios de 2015, son solo un ejemplo. Pero este fenómeno afecta a todos los campos de la cultura, política, religión o ciencia.

Lo malo es que recibir desinformación, o contribuir a su difusión a través de nuestras redes sociales, es a veces el menor de nuestros problemas. En la red acechan otros riesgos mayores, y todos somos víctimas potenciales.

PARTE II



OBJETIVO TIGER88

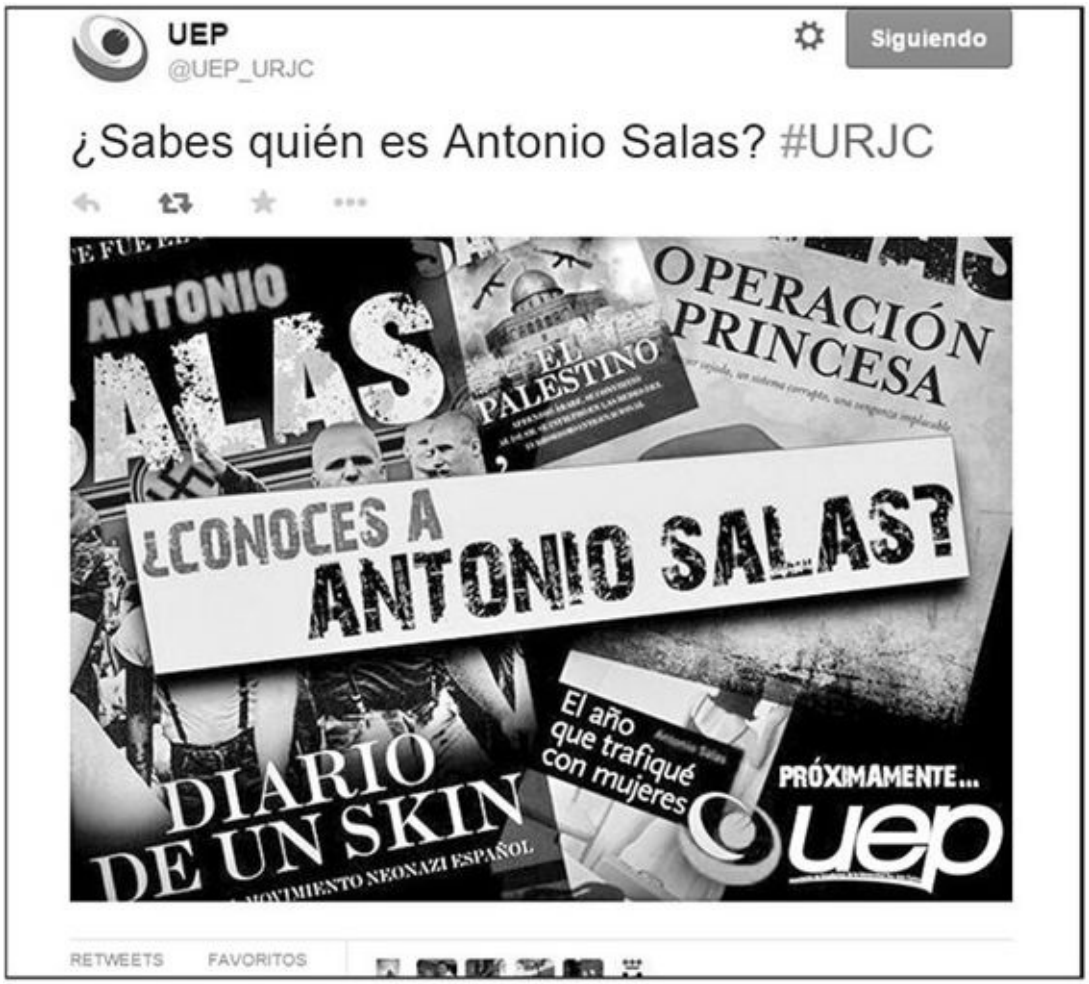
«Hay un solo derecho en el mundo, y este derecho está en la propia fuerza de uno.»

Adolf Hitler, 1928

El día 5 de marzo la Unión de Estudiantes Progresistas (UEP) de la Universidad Rey Juan Carlos de Madrid había organizado el I Congreso Nacional sobre Servicios de Inteligencia, en el campus de dicha universidad en Vicálvaro. Por alguna incomprensible razón, entre los prestigiosos participantes al evento —como el coronel del CESID Manuel Rey, la inspectora del CNP Rosa María Muñoz, el espiólogo Fernando Rueda o el colaborador del CNI David R. Vidal—, los organizadores tuvieron la amabilidad de invitarme a mí.

Diga lo que diga internet, yo no soy ni he sido espía, ni jamás he trabajado para ningún servicio de información policial o de Inteligencia. Sin embargo, los organizadores consideraban que mi experiencia sobre el terreno, durante las diferentes infiltraciones que había realizado para mis libros, podía aportar una perspectiva original y diferente en torno al trabajo del infiltrado. Sobre todo porque, como es lógico, cuando realizas trabajos de campo en ámbitos como el terrorismo, narcotráfico, crimen organizado, etcétera, es inevitable terminar coincidiendo en el tiempo y el espacio con agentes de diferentes servicios de Inteligencia. En mi caso, y como ya he relatado anteriormente, se acumulan las anécdotas vividas con agentes del SISMI italiano, la DGI cubana, la CIA norteamericana, el Mosad israelí o el CNI español, entre otros. Así que preparé una conferencia sobre las coincidencias y diferencias entre el agente y el periodista encubierto.

Con la mejor intención, eso lo sé, los organizadores del evento utilizaron una fotografía mía como parte de la promoción previa del congreso, y durante días un cartel con la leyenda: «¿Sabes quién es Antonio Salas?» fue retuiteado desde la cuenta de la UEP URJC. Supongo que debe de ser halagador que alguien considere tu imagen o tu nombre un reclamo publicitario, pero en mi caso eso entraña ciertos riesgos, y los alumnos de la Rey Juan Carlos no tardarían en sufrirlos en carne propia.



El poder de convocatoria de los organizadores nos dejó perplejos a todos los ponentes. El auditorio del campus se llenó hasta los topes. Tanto es así que muchos de los estudiantes no pudieron acceder a la sala de conferencias porque no quedaron sitios libres. Durante los días previos al congreso los interesados debían enviar un mensaje a la UEP con su nombre y DNI para reservar plaza, pero las solicitudes sobrepasaron con mucho la capacidad del auditorio, y hasta el último minuto no era posible saber quién había cancelado su reserva, y quién podría dejar la lista de espera para ocupar una plaza en la sala de conferencias.

Allí, discretamente situadas entre el público, se encontraban muchas caras que me resultaban conocidas. Funcionarios de las Fuerzas y Cuerpos de Seguridad del Estado, colegas periodistas y otros amigos que habían decidido asistir a las conferencias. Allí estaban Pepe y David Madrid. Ángel y Manu, funcionarios de una unidad especial de cuyo nombre no debo acordarme. David Castillo, comisario del Museo del Espía y personaje de *Operación Princesa.* Toni y Diego, policías y compañeros de experiencias en mundos muy distintos… Sin duda aquella sala era un lugar muy seguro. Todos lo sabíamos. La alta afluencia de policías a aquel congreso era previsible. Sin embargo, a él no le importó.

El congreso transcurrió sin incidentes… o eso creía. Las conferencias

lograron capturar el interés del público y ni un alma abandonó la sala, para permitir el acceso de quienes no habían conseguido una butaca en el auditorio: al final se quedó una larga lista de espera.

Durante los días previos a mi participación en el congreso, y como era previsible, aumentaron los insultos y las amenazas. Twitter, Facebook, el correo electrónico… Es sorprendente la fidelidad que puede inspirar el odio. A pesar de que habían transcurrido diez años desde la publicación de *Diario de un skin,* en la comunidad neonazi mi nombre continúa despertando el mismo rencor que cuando se editó. Y así me lo hacen saber a la primera de cambio, escudados tras sus nicks, como hacía uno de mis «habituales»: MarkoSS88. También lo hizo aquel día. Solo que aquella tarde Markos estaba especialmente violento. Sus innumerables mensajes en Twitter destilaban una rabia y un odio particularmente enérgicos.

> **@markoSS88** @AntonioSalas_ Si no fuera por la policía que te salva el culo ya estarías muerto…

Lo leí de pasada. Sí, era violento, pero uno más. Similar a docenas de insultos y amenazas similares que él y otros jóvenes neonazis, me dedicaban constantemente. No podía imaginar, en aquel instante, el mensaje que se ocultaba en aquellos caracteres, y cómo condicionaría mi vida durante el año y medio siguiente…

Para entonces MarkoSS88 no significaba nada. Uno más de los nazis obsesionados con Tiger88. ¿Y qué marcó la diferencia? Que Markos no solo dirigió su odio hacia mí, sino que llegó a amenazar a los organizadores del congreso a través de sus propias redes sociales.

> **@markoSS88** @UEP_URJC dais asco por defender a escoria como @AntonioSalas_ putos manipuladores de la verdad, lo lamentareis

Aquel 5 de marzo, y como me hicieron saber los estudiantes de la UEP que habían organizado el congreso, probablemente alguno de ellos se arrepintió de haber contado conmigo entre los conferenciantes. Nunca te acostumbras a las amenazas, pero comprendo que la primera vez que te sientes en el punto de mira de un neonazi violento, el temor es mayor. Y así me lo comunicó el grupo de estudiantes universitarios.

Esa fue la razón por la que decidí escribir a MarkoSS88. Podría ser comprensible, hasta cierto punto, que yo fuese el blanco de su odio, pero los insultos y las amenazas a los jóvenes de la UEP resultaban intolerables. Así que le escribí, en un tono conciliador, intentando abrir un canal de diálogo. Tenía la esperanza de que, con mis argumentos, podría convencerle de su error. Y de la misma forma en que cientos, quizás miles, de jóvenes neonazis habían abandonado el movimiento tras leer *Diario de un skin*, quizá yo podría calmar su ira y hacerlo entrar en razón… Fue un error. Un enorme error.

Capítulo 3
Internet: el invento que revolucionó la historia

«Sí, soy un delincuente… Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis. Soy un hacker, y este es mi manifiesto. Podéis eliminar a algunos de nosotros, pero no a todos…»

The Mentor: El Manifiesto hacker

La rueda del siglo XXI

Internet es, probablemente, el mayor invento de la historia de la humanidad desde la rueda. Revolucionó la sociedad. Y aunque todavía existen algunos colectivos que no han tenido acceso a ella, como existen tribus no contactadas que aún no conocen la rueda, ningún otro invento ha condicionado tanto la historia de este planeta.

Internet ha puesto al alcance de nuestro ordenador, o nuestro teléfono móvil, más información que toda la contenida en la Biblioteca de Alejandría. Nos permite comunicarnos con seres queridos o con perfectos desconocidos, en cualquier país del mundo. Nos posibilita un conocimiento real e instantáneo de sucesos que se producen al otro lado del globo. Nos facilita la interrelación con otros seres humanos de distinta cultura, religión, raza o nacionalidad. Ocio, cultura, amor, sexo… Y todo sin movernos del teclado. Es la mayor herramienta de conocimiento diseñada nunca por el ser humano. Pero también tiene su lado oscuro. Como la rueda.

La rueda nos permitió construir carros de transporte, máquinas de agricultura, ambulancias, coches de bomberos, aviones comerciales, transbordadores espaciales… Pero también sirvió para construir instrumentos de tortura, máquinas de guerra, carros de combate… Internet, como la rueda, no es una herramienta buena o mala en sí. Lo bueno o malo es lo que podemos hacer con ella. Y lo que es más importante, lo que otros pueden hacernos a nosotros.

La red es maravillosa. Está llena de posibilidades. Y de información… aunque también de amenazas.

El 17 de octubre de 2014, la Real Academia Española presentó su vigesimotercera edición del Diccionario de la lengua española. En un esfuerzo por estar con los tiempos, la RAE incluyó numerosas palabras de uso común en la nueva edición del diccionario de un idioma que hablan casi 470 millones de personas como lengua materna en todo el mundo —la segunda más hablada del planeta, tras el chino mandarín—. Y casi 559 millones de seres humanos, si incluimos a quienes lo hablan como segunda lengua. Con presencia en tres de los cinco continentes. Por eso, por su repercusión internacional, la labor de la RAE resulta tan importante.

En esta edición, el Diccionario incluyó palabras como *aminovio, papichulo, burka, homoparental, coach* o *birra,* que demuestran la evolución de la rica y antigua lengua de Cervantes. Y como no podía ser de otra manera, esta actualización incluyó también numerosas palabras vinculadas a las nuevas tecnología, ya asentadas en nuestra vida diaria: *tuit, wifi, bloguero, tableta, gigabyte, dron* o *intranet.* Sin embargo, un término generó una amarga polémica entre el colectivo de afectados: *hacker.*

> *Hacker. (Voz ingl.).* m. y f. *Inform.* pirata informático.

Y si acudimos a la definición que hace la Academia de dicho término, nos

encontramos lo siguiente:

> *Pirata informático, ca.* m. y f. Persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta.

Y eso es faltar a la verdad.

Para la comunidad hacker hispanohablante, la RAE la había «cagado» en su definición. Porque para ellos un hacker no es un pirata informático… sino todo lo contrario. Existen palabras, como *craker,* que se ajustarían más a la definición de «pirata informático». Mientras que, para la comunidad, la definición que hace la Wikipedia de la voz *hacker* se acerca más a la realidad: «Un hacker es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas».

Pero en el mundo de las nuevas tecnologías, que condicionan fundamentalmente nuestras vidas en el siglo XXI, las cosas no son blancas o negras. Por eso, con el paso de los años, los hackers comenzaron a colorear sus sombreros, en una pluralidad de tonalidades que, en teoría, pretenden definir sus intenciones ante la pantalla del ordenador. Y nacieron definiciones como *whitehat* (hackers de sombrero blanco), *blackhat* (hackers de sombrero negro), *greyhat* (hackers de sombrero gris), *bluehat* (hackers de sombrero azul), etcétera.

Antes de comenzar esta investigación, yo no sabía que gracias a hackers como GeoHot, hoy podemos descargarnos apps para el móvil, conocer las miserias de los políticos o recibir las actualizaciones de nuestros proveedores de internet para proteger nuestros ordenadores de los delincuentes. De no ser por el implacable y constante vapuleo al que los hackers someten a las grandes multinacionales de internet, descubriendo los errores de sus servicios, nuestros ordenadores serían un coladero mucho mayor para ladrones, *voyeurs,* chantajistas y acosadores.

Es probable que la Administración Obama jamás hubiese confesado las torturas y asesinatos cometidos en Guantánamo o Irak, de no haber sido porque Wikileaks filtró previamente miles de documentos, fotos y vídeos demostrándolo. Es posible que jamás hubiésemos conocido la contabilidad del Partido Popular si Anónymous no la hubiese hecho pública, antes incluso de que el juez Ruz hubiese concluido la instrucción del caso Bárcenas. Y estoy seguro de que jamás descubriríamos que los servicios de Inteligencia pueden captar todos nuestros emails, wasaps, conversaciones telefónicas y videoconferencias, si Edward Snowden no nos hubiese revelado cómo, dónde y cuándo lo hacen.

Es comprensible que, ante tales filtraciones, extremadamente incómodas para el poder, se califique a los hackers como piratas, que no corsarios. Porque mientras los corsarios podían ejercer la piratería, con la «patente de corso» que les confería el poder, los piratas saqueaban al margen de la ley.

A partir de julio de 2015, una fecha clave en la historia de la cultura hacker,

también existirán corsarios autorizados por los gobiernos para utilizar armas y herramientas de hacking, que se considerarán ilegales en manos de los piratas. Unos tendrán la autorización para realizar ataques, para testar equipos, para explorar vulnerabilidades, dentro de los límites de la nueva ley. Los otros, los de siempre, continuarán moviéndose en la clandestinidad, al margen de la legalidad del momento, sin molestarse en pedir permiso al poder para utilizar tal o cual programa, aplicación o código en sus investigaciones tecnológicas. Explorando los nuevos sistemas en busca de sus errores, porque esa es su pasión. Sin embargo, a partir de julio de 2015, con la entrada en vigor del nuevo Código Penal, cosas que antes no estaban penadas ahora pueden implicar prisión.

No es nada nuevo. Desde el nacimiento de internet, no fue la red quien se adaptó a la sociedad, sino la sociedad a la red. Nuestras rutinas, nuestras relaciones, nuestra formación, nuestras comunicaciones… Toda nuestra vida se ha ido adaptando lentamente a las nuevas tecnologías digitales. Y también nuestras leyes.

En los años anteriores a esa reforma del Código Penal de julio de 2015, la comunidad hacking española vivió una convulsión similar a la vivida por los hackers alemanes, franceses o norteamericanos, cuando fueron sus leyes las que comenzaron a adaptarse a las nuevas prácticas digitales. Y ha sido un honor vivir ese momento de cambio con ellos. Presenciar sus debates. Participar en sus reuniones. Contagiarme de su entusiasmo por la investigación y de su indignación por los límites que quiere establecer el Gobierno a la misma.

Y es que ellos, los hackers, tienen el poder. Siempre lo han tenido. Desde el instante en que las nuevas tecnologías se instalaron en nuestras vidas, en los despachos de los políticos, en las bases militares, en los depósitos bancarios o en los juzgados, esa casta de cerebros superdotados, capaces de hablar con los binarios y comprenderlos, recibió el poder de cambiar la sociedad. De alterar nuestras comunicaciones. De acceder a nuestros secretos. De desvelar los abusos de los gobernantes. De filtrar sus miserias al mundo.

Nunca antes en la historia de la humanidad un solo individuo, sin más herramientas que un ordenador, había tenido la capacidad de acceder a secretos de tal relevancia. Nunca antes había existido un canal capaz de divulgar dichos secretos a nivel internacional. Y sin moverse de su casa. Pero desde mediados del siglo XX, con el nacimiento de internet, esa situación es factible. Y de hecho, cada vez se producen más filtraciones incómodas, embarazosas y abochornantes para tal o cual Gobierno, a causa de un hacker. Sin embargo, no todos los genios, dotados de ese don para susurrar a las máquinas y obtener sus secretos, hacen un uso responsable de ese poder.

Un gran poder implica una gran responsabilidad

Cuando Edward Snowden lanzó la bomba al revelarnos que las agencias de Inteligencia norteamericanas podían espiar todos nuestros vídeos, fotos, emails, conversaciones por Skype, cuentas bancarias y cualquier otro dato personal que subimos a la red, tembló el mundo. Poco, y solo durante unos días, pero tembló.

Cuando nos desveló que las webcam y los micrófonos de nuestros ordenadores personales y nuestros teléfonos móviles podían activarse en remoto, para ver y escuchar lo que estamos haciendo, volvió a temblar. No porque la NSA pueda utilizar mi móvil o tu ordenador para vulnerar nuestra intimidad, sino porque ya habían espiado los teléfonos de líderes mundiales como Angela Merkel, y esos sí puntúan.

Nuestra vida digital transcurre en casas de cristal, pero las cortinas están al otro lado del vidrio. No tenemos control sobre ellas. Mantenemos nuestra fantasía de intimidad mientras no hagamos nada que pueda despertar la curiosidad del casero, porque él es quien puede correrlas, cuando le apetezca, para ver qué estamos haciendo.

Snowden nos enseñó muchas cosas, y llamó nuestra atención sobre otras. Como la historia de internet y su salto de los Estados Unidos a Europa, utilizando el mismo sistema de cableado telegráfico transatlántico establecido un siglo antes del primer ordenador. Y quien controla el cable controla la red. No es nuevo. Hoy conocemos cómo las agencias de Inteligencia norteamericanas, como el FBI, controlaban ilegalmente los hábitos de lectura de sus ciudadanos, rastreando quién leía qué libros marcados como peligrosos en las bibliotecas de los Estados Unidos… ¿En serio alguien pensaba que dichas agencias no harían uso de la capacidad de saber quién lee qué páginas, quién se comunica con quién, o quién busca qué en la red?

Existen numerosas historias oficiales sobre internet y los ordenadores. Y dependiendo de la profundidad del autor, se establecen unas fechas u otras.

A pesar de que muchos consideran al atormentado genio Alan Turing como el creador del primer ordenador analógico de la historia, utilizado para romper el código de cifrado nazi de la máquina Enigma durante la Segunda Guerra Mundial, existen precedentes. En el Museo de la Técnica de Berlín, Rafael Troncoso y Francisco José Ramírez, autores del delicioso ensayo *Microhistorias*,[30] se encontraron con un ejemplar de la computadora mecánica Z1, fabricada en 1936 por el ingeniero alemán Konrad Zuze, y que empleaba por vez primera un sistema binario como base de su programa.

A decir verdad, la idea de crear máquinas para facilitar los cálculos matemáticos en muy antigua, incluso utilizando el sistema binario inventado por Gottfried Wilhelm von Leibniz en el siglo XVII, pero ya enunciado en el *I Ching* chino, y teorizado antes aún, en el siglo III a. C., por el matemático indio Pingala.

Esos primitivos «ordenadores» de números y cálculos, tatarabuelos de nuestros

ordenadores personales, los idearon en distintos momentos de la historia, y en diferentes lugares del mundo, sabios, científicos y pensadores, que «hackearon» sus limitaciones para imaginar algo nuevo: máquinas que nos ayuden a pensar mejor. Como la Máquina Diferencial de Babbage, el «telar automático» de Hollerith, o la desconcertante y mucho más antigua Máquina de Anticitera.

Como todas las guerras, la Segunda Guerra Mundial agudizó la creatividad de los ingenieros, y tras derrotar el cifrado de la Enigma, Turing y otros científicos continuaron investigando. Así dieron lugar a máquinas, primero mecánicas, luego analógicas y por fin digitales, cada vez más sofisticadas. Como la Colossus (heredera de la Atanasoff Berry Computer norteamericana) o la ENIAC (Electronic Numerical Integrator And Computer).

No es casual que en el desarrollo informático tal y como lo conocemos, la investigación científica con frecuencia esté impulsada, financiada o tutelada, por intereses militares. La información es poder.

Tras la Segunda Guerra Mundial, la Guerra Fría supuso un nuevo acelerador a la investigación tecnológica. La idea de la «conmutación de paquetes», el envío de información de unos ordenadores a otros surgido en los años cincuenta, se desarrolló primero a nivel teórico y después en laboratorio. Y ya en los sesenta, la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA), del Ejército norteamericano, desarrolló las ideas del visionario Joseph C. R. Licklider, el primero en soñar con una «red de muchos [ordenadores], conectados mediante líneas de comunicación de banda ancha», las cuales proporcionan «las funciones que existen hoy en día de las bibliotecas junto con anticipados avances en el guardado y adquisición de información y [otras] funciones simbióticas».

Aunque la palabra *internet* no se utiliza hasta los años setenta, en 1969 ya funcionaba ARPANET, la red de ordenadores de DARPA. Según Troncoso y Ramírez:

> ARPANET era un proyecto del Departamento de Defensa estadounidense, que se usaba para investigaciones científicas. Muchos consideran que ARPANET se creó para tener un sistema de comunicaciones que pudiera sobrevivir a un ataque nuclear, pero en realidad la interconexión entre ordenadores se llevó a cabo para aprovechar mejor la inversión en los sistemas de computación. Estos eran muy caros y el Departamento de Defensa quería que se pudieran interconectar de forma que un laboratorio en el punto A fuera capaz de poder usar los recursos de un servidor en el punto B.[31]

Y así, poco a poco, cada vez más universidades norteamericanas comenzaron a interconectar sus ordenadores. En 1969 eran solo cuatro, dos años después casi llegan a la treintena. En 1972 se crea el InterNetworking Working Group, la organización responsable de gestionar internet en los Estados Unidos, pero un año después la red cruza el océano, extendiéndose año a año por las universidades del mundo, a través de las líneas telefónicas.

No todos los científicos supieron ver que aquel nuevo canal de comunicación cambiaría el mundo. Y los que lo vieron no estaban por la labor de que internet

cayese bajo el control militar. De hecho, aquella revolución tecnológica que se avecinaba posibilitaba algo único en la historia de la humanidad: el intercambio ilimitado de conocimiento, información y comunicación entre todos los pueblos del mundo. Sin fronteras, sin distancias, sin más límite que nuestra imaginación. Y sin el control de los gobiernos…

Aun así, los procesadores eran lentos. El envío de un simple paquete de datos a través de la línea telefónica era muy caro. Por eso inicialmente solo las universidades y los laboratorios podían permitírselo. Y de ese modo nacieron los primeros hackers.

Genios, como John Draper, el «Capitán Crunch», que con la ayuda de su amigo invidente Denny Teresi comercializó las primeras *blue box* —un artefacto que imitaba la frecuencia de 2.600 herzios que utilizaban las compañías telefónicas, sobre la base de un silbato que regalaban los cereales Capitán Crunch—, para poder llamar gratis. Así nació el *phreaking;* el hackeo de las líneas telefónicas tirando de ingenio y un silbato infantil.

Desde entonces miles de genios, igual de creativos e imaginativos, pusieron su empeño en estudiar las nuevas tecnologías en busca de sus puntos débiles. Y los encontraron. Pero lo que caracterizó a aquellos primeros hackers es que cada hallazgo de una nueva vulnerabilidad en los sistemas no se guardaba para el uso y disfrute de su descubridor, sino que se compartía con la comunidad. Como tipos inteligentes que eran, sabían que cien cerebros piensan más y mejor que diez. Y mil mejor que cien. De ese modo, al final todos sacaban provecho de las aportaciones de la comunidad.

Y mientras en los años setenta y ochenta surgían las grandes multinacionales de internet —que desarrollaban nuevos lenguajes de programación, nuevos protocolos y nuevas herramientas, dando lugar a gigantescas fortunas como las de Steve Jobs o Bill Gates, que patentaban sus descubrimientos y cerraban sus códigos para su comercialización—, otros, como Richard Stallman, aseguraban que internet era una puerta hacia el futuro de toda la humanidad, y abogaban por el código abierto. Por una internet de todos y para todos. Cuando en 2014 tuve la oportunidad de conocer a Stallman, su discurso no había variado un ápice. Salvador Allende decía que «ser joven y no ser revolucionario es una contradicción hasta biológica». Stallman, a sus más de sesenta años, continúa siendo un joven revolucionario.

Hoy internet controla el mundo. Todas nuestras conversaciones privadas, nuestras transacciones bancarias, nuestros historiales médicos, nuestras fotos y vídeos personales, nuestras declaraciones fiscales… todo viaja por la red. Y el control de esas autopistas de la información ya no es el monopolio de los organismos militares, científicos o políticos. Otros científicos e investigadores, tan geniales y creativos como sus descubridores, incursionan en los sistemas para explorar sus mecanismos buscando mejorar los que ya existen. Con frecuencia identificando sus errores y vulnerabilidades. Tienen un gran poder. Pero un gran poder implica una gran responsabilidad. Y otro tipo de hackers, aquellos que convierten la tecnología en una herramienta para el activismo social o político, no se limitan al estudio, sino que

ejercen ese poder… a veces con consecuencias terribles para los usuarios. Porque una buena intención no garantiza que un poder tan enorme no escape a su control, cobrándose incluso vidas humanas. Quedó patente, por ejemplo, cuando los *hacktivistas* de Impact Team hackearon la página Ashley Madison, en 2015, filtrando las identidades de esa página para aventuras extraconyugales, y comenzaron a producirse los primeros suicidios. Aún me quedaban meses de investigación por delante hasta ese momento.

Policías 2.0

Fue Pepe, un veterano policía del Grupo de Actuación de Menores (GAM), habitual en las cenas tertulia organizadas por David Madrid, quien me puso en la pista de mi nuevo mentor. Mi primer guía en el viaje hacia la comunidad hacker…

Pepe es un policía de la vieja escuela, con años y años de servicio a su espaldas. Sin duda ha quemado las suelas de muchos pares de botas pateando las calles de su ciudad, lo que le convierte en una voz autorizada a la hora de analizar lo que ocurre y por qué ocurre. Y aunque tanto la Guardia Civil, como el Cuerpo Nacional de Policía o el Centro Nacional de Inteligencia menosprecian con frecuencia el trabajo de la Policía Municipal, me consta que en muchas ocasiones ellos, los «munipas», son la primera línea en la prevención y lucha contra el delito. Son los que dialogan con las familias, los que vigilan a los chavales, los que mejor conocen los accesos y salidas en los polígonos y barrios más conflictivos. Y yo he sido testigo en más de una ocasión de cómo CNP o Guardia Civil acudía a Pepe y a sus compañeros para obtener o contrastar una información relevante sobre tal o cual operación. Especialmente en casos relacionados con los skinhead, las bandas latinas u otras tribus urbanas. Porque, al fin y al cabo, ellos son los que están todo el día a pie de calle.

Durante sus años de servicio, Pepe se curtió en los barrios, polígonos industriales, parques y glorietas. Ha visto de todo. Y su memoria conserva una legión de anécdotas compiladas durante décadas. Una de las que me afecta personalmente es que, por esas cabriolas del destino, ha terminado compartiendo vestuarios y patrulla con uno de mis viejos camaradas en los tiempos de *Diario de un skin:* Jorge V.

En 2005, Jorge fue detenido junto con toda la cúpula de Blood & Honour España, durante la Operación Espada, ejecutada impecablemente por el Grupo 7 del servicio de información de la Guardia Civil. Los mismos que habían realizado, con idéntico éxito, la Operación Puñal contra Hammerskin. Un año después de aquella detención, Jorge aprobó el examen de ingreso a la Policía Municipal, donde ha mantenido, según la alcaldía, «un expediente limpio y una trayectoria impecable». El consistorio nunca tomó medidas contra él.

En 2007, Jorge fue uno de los doce policías escogidos en su jefatura, entre cincuenta aspirantes, para protagonizar un calendario solidario destinado a una ONG. Doce agentes, especialmente atractivos, posaban en ropa interior o con el torso desnudo, con sus armas, grilletes y radios, para recaudar fondos por una buena causa. Jorge fue Mister Junio en ese calendario. Y en sus fotos semidesnudo, y esto es lo que a mí me interesó, pudimos contemplar sin interferencias los elocuentes tatuajes que decoran su piel, recuerdo para toda su vida de su pasado en el nacionalsocialismo.[32]

En 2010, y durante el macrojuicio contra la organización neonazi Blood & Honour, se daba la circunstancia de que por la mañana Jorge tenía que asistir al juzgado como imputado, y por la tarde se vestía el uniforme de policía y patrullaba

las calles como compañero de Pepe. El destino es caprichoso.

Destinado en el GAM, durante los últimos años Pepe ha concentrado su actividad profesional en la prevención del acceso de los jóvenes al mundo de la delincuencia. Sobre todo de los que se hallan en riesgo de captación por las bandas. Eso implica charlas en los colegios, el seguimiento en domicilio de los casos más conflictivos, el diálogo con padres y educadores, etcétera. Probablemente por esa razón Pepe asumió antes que muchos que es imposible comprender el mundo en el que se mueven los jóvenes del siglo XXI sin comprender cómo funciona su vida digital, su presencia en las redes. Y por eso Pepe es uno de esos funcionarios de policía que se ha preocupado en matricularse en cursos, formarse y estudiar, asistir a conferencias y, en definitiva, fagocitar toda información que caía en sus manos sobre la red y su relación con los más jóvenes. Pepe es un policía 2.0. Porque sabe que lo que ocurre en las calles tiene su continuación en la red, y viceversa.

Él fue el primero a quien oí hablar de los crackers.

Había ido a verle para contarle en qué andaba metido ahora, y medio en broma medio en serio me soltó que ya podía tener cuidado con los crackers.

—¿Con los calamares gigantes? —le pregunté entre risas.

—No, hombre, eso eran los Kraken, monstruos marinos mitológicos. Yo te hablo de los monstruos del cibercrimen. A los que se confunde a menudo con los hackers. Pero los hackers son los buenos, y los crackers los malos.

—¿No son lo mismo?

—Al contrario. Son antónimos. Un hacker es un investigador y un cracker es un delincuente informático. Y dentro del crimen organizado, ahora están reclutando a muchos chavales, expertos en informática, para utilizarlos dentro del cibercrimen. Y con los amigos que te has ido haciendo en esos mundos, Toni, deberías andarte con ojo. Sobre todo con los nazis.

—Creía que eso del ciberactivismo era cosa de los grupos antisistema…

—Sí, y esos también te tienen ganas, pero cada vez hay más presencia neonazi en la red, y algunos son auténticos expertos.

Pepe fue el primero en concienciarme de los riesgos que añadía a mi vida la revolución tecnológica. Y también fue el primero en orientarme en la buena dirección. Había salido del búnker del agente Juan con muchas ganas, pero desde entonces me había limitado a dar palos de ciego.

—¿Ya has leído algo?

—Joder, Pepe, algo no, mucho. Me he ido a Móstoles y me he comprado todo lo que he podido de una editorial llamada Informática 64, pero no consigo pasar del primer capítulo de ninguno de los libros. Todos son demasiado técnicos. Y si no eres un experto, no entiendes ni una palabra. Los únicos que me he podido leer son un ensayo titulado *Microhistorias* y una novela: *Hacker épico*, buenísimos…

—Olvídate de todo eso —me dijo mientras escribía algo en una servilleta de la cafetería—. Busca este libro y visita este blog. Y dame un poco de tiempo para

ponerte en contacto con su autor o con uno de sus editores. Yo los conocí durante la presentación del libro hace unos meses, y he asistido a alguno de sus talleres de seguridad informática. Si alguien puede ayudarte a introducirte un poco en este mundo, son ellos.

Fue una revelación. El título que Pepe me escribió en aquella servilleta era *x1red+segura,* escrito por un tal Ángel Pablo Avilés, «Angelucho», y fruto de una autoedición patrocinada por la Fundación y el Grupo de Delitos Telemáticos de la Guardia Civil y de varias empresas de seguridad informática como Buguroo o Aiuken, liderada esta última por el veterano *business-hacker* Israel Córdoba.

No tuve que esperar mucho para hincarle el diente al libro. Tampoco para conocer a mi nuevo mentor. A pesar de su frenético día a día como fundador y director de tecnología y estrategia de negocio de Aiuken Solutions, empresa responsable de la seguridad informática de grandes firmas dentro y fuera de España, Israel Córdoba tuvo la amabilidad de hacerme un hueco en su dilatada agenda, ante la incombustible persistencia de Pepe. Inasequible al desaliento, Pepe insistió e insistió hasta que Israel Córdoba accedió a comer con el policía, y con un misterioso periodista del que se negó a darle más datos. Ese fue el primero de una serie de encuentros. Gracias a él, fui adentrándome, paso a paso, en el mundo de los hackers.

Hackstory

A Israel Córdoba le gusta definirse como *business-hacker,* pero un hacker muy distinto a esos «piratas informáticos» que propone la Academia de la Lengua. Y muy distinto, también, a los primeros que abrieron nuevos senderos dentro de nuestras fronteras.

Conocí a Mercè Molist ese 2014, durante una de sus conferencias sobre *Hackstory.es,* el primer libro monográfico sobre la historia del hacking en España. Mercè es la periodista de referencia en la cultura hacker patria, y creo que no exagero si afirmo que ningún otro colega ha explorado tan a fondo, y durante tantos años, el movimiento hacking en Cataluña, y también a nivel nacional.

Entrevistas, crónicas de eventos, reportajes… Los artículos de Molist en *El País*, *El Mundo* o Catalunya Radio entre otros medios han contribuido a inmortalizar el rastro del *hacking* español para futuras generaciones. Y aunque cuando la conocí ya estaba esbozando *Cibercrimen*, su siguiente libro —escrito en coautoría con el catedrático de la Universidad Politécnica de Catalunya, Manel Medina (Tibidabo ediciones, 2015)—, sin duda fue su primera obra la que me permitió comprender cómo, cuándo y por qué llegó el hacking a España.

Afirma que «en España en los años setenta, los hackers eran cuatro gatos. En 1985, los centros de cálculo de cada universidad no tenían más de dos, máximo tres ordenadores, según el estado de Situación Proyecto IRIS, recuperado gracias a Francisco Monserrat, de IRIS-CERT. La cosa no estaba mejor para las empresas, pues solo las grandes tenían ordenadores».

Según su investigación, y gracias a los documentos oficiales que ha podido rescatar, hoy conocemos los nombres de aquellos primeros españoles que accedieron a la red, en los años setenta,[33] pero ninguno de ellos llegaría a prosperar en la comunidad hacker; antes bien establecieron con un esfuerzo épico la red que después explorarían otros, y se retiraron a sus puestos de profesores universitarios.

Los ochenta implican el nacimiento de la industria de los videojuegos, en la que España ha alcanzado un meritorio protagonismo. Y el estreno, en 1983, de la película *Juegos de guerra*, de John Badham, que tanto influyó en aquella primera generación de chavales españoles, que decidieron que de mayores querían ser David Lightman, el personaje protagonista interpretado por Matthew Broderick.

Son los años del Spectrum, las primeras BBS[34] en español y los videojuegos pirateados. Los años en que los nicks de Ender Wiggins, Akira, CenoIx, D-Orb, Partyman, Quijote/AFL, Pink Pulsar, HorseRide, Wendigo/Khk, El Enano, Bugman, Spanish Taste, Cain, Spectro o GURU JOSH, entre otros, se asomaron a la red. Los años en que, utilizando austeros ordenadores Atari o Amina, nació la «escena warez» o la Scene, donde los primeros hackers españoles pirateaban los programas que llegaban de los Estados Unidos y los divulgaban gratuitamente.

Cuando un pionero como Dan Sokol copió por primera vez una tarjeta perforada, crackeando el BASIC para distribuirlo clandestinamente entre sus compañeros de pasión. Cuando nacen Glaucoma y Apostols, posiblemente los primeros grupos hacker españoles, que exploraban el incipiente ciberespacio utilizando las pocas conexiones universitarias existentes. Y cuando un chaval de catorce años, Agnus Young, un *phreaker* devoto de AC/DC, regalaba llamadas telefónicas a las ancianitas, hackeando la línea telefónica de las cabinas por medio de una «caja azul» de fabricación casera, inspirada en el descubrimiento del Capitán Crunch.

La piratería que en el siglo XXI sufrimos escritores, músicos y cineastas comienza allí. En 1986, según la histórica revista *Microhobby,* el 80% de los programas instalados en ordenadores españoles eran piratas. Como ocurría en el resto del mundo.

En los noventa la cosa no fue mejor. Con la nueva década, el pirateo de videojuegos se popularizó, y también comenzó la persecución policial de los «piratas». «A principios de los noventa —señala Mercè Molist— el Rastro de Madrid y el Mercat de San Antoni de Barcelona congregaban a decenas de vendedores de videojuegos y programas pirateados, siendo habituales las redadas…»

Los noventa trajeron la World Wide Web, la famosa WWW que encabeza hoy la mayoría de páginas web, y con ella los primeros escritores de virus españoles, como Los Dalton o el legendario GriYo, al que me referiré más adelante. Y Geocities, el primer servicio de webs gratuito. Después de 1995, Infovía diversificaría a los proveedores de internet, y todo el mundo quiso tener su propia página.

Las BBS evolucionarán hacia ISPs, Hispahack se hace un sitio en la escena hacker mundial y se producen las primeras detenciones de sus miembros a manos de la Guardia Civil. En respuesta, Hispahack realiza uno de los primeros ataques hacktivistas en España, redireccionando la página oficial de la Benemérita hacia una de contenido homosexual.

A los pioneros Glaucoma o Apostols, comienzan a unirse otros grupos: La Katedral, The Demons, Esphreak… imposible mentarlos a todos. Son los años de Isla Tortuga, los fanzines y los canales de MIRC, los canales de chateo en internet, que en aquellos años yo frecuentaba. Pero mientras yo me pasaba las noches chateando con neonazis en canales como #Nueva Europa, #Ultras o #Nacionalsocialismo, preparando el terreno para mi infiltración en el mundo skinhead, aquella nueva generación de hackers utilizaba el IRC Hispano para intercambiar programas, convocar reuniones y transmitir un conocimiento tecnológico de valor incalculable, que no se pagaba con dinero.

Mi colega Mercè Molist compiló toda esa historia, imposible de resumir sin cometer olvidos, en su *Hackstory.es.* A ella remito a los interesados. Allí están los nombres de la mayor parte de los primeros hackers españoles, que antes de la llegada del siglo XXI ya habían establecido las bases y los caminos que ahora transitan las nuevas generaciones. Durante mi viaje terminaría conociendo y entablando amistad

con algunos de aquellos hackers de la «vieja escuela», y con sus descendientes.

Israel Córdoba, el *business-hacker,* era uno de ellos…

Ya estamos en Matrix

Israel Córdoba es un ejecutivo dinámico y emprendedor. Con una agenda, por supuesto electrónica, repleta de reuniones y compromisos. Tras nuestro primer encuentro en el restaurante, Pepe había conseguido convencerlo para que me echase una mano en mi viaje hacia el mundo del hacking, y aceptó hacerlo, pero había que encontrar el día y la hora oportuna.

Y el día llegó, como no podía ser de otra manera, a través de la red. Aquella mañana había encontrado un cíber nuevo, donde podías disfrutar de unos bollos y un café caliente mientras consultaba el correo electrónico. Una a una revisaba las diferentes cuentas de email y de pronto, en una de ellas, me encontré con un mensaje extraño. Nunca había visto una convocatoria similar.

Israel Córdoba había utilizado una aplicación de su agenda, que enviaba una cita estableciendo la hora de comienzo y final de la misma, el lugar y la fecha. De paso, solicitaba al receptor que confirmase la recepción del mensaje aceptando las condiciones del encuentro o anulándolo. Reconozco que flipé. Estaba claro que a Córdoba no le gustaba perder el tiempo, y a mí tampoco. Tenía un hueco en su agenda de 90 minutos. O lo tomas o lo dejas. Y lo tomé.

Israel no se parece en nada a la imagen estereotipada del hacker. No viste sudaderas con capucha, ni toma bebidas energéticas. Todo lo contrario. Amante de los buenos coches, la buena mesa y los buenos trajes, tengo que reconocer que inicialmente me recordó a David R. Vidal, pero a diferencia del «agente Juan», a Israel Córdoba le gustan los deportes de riesgo. Motero consumado, ha participado en concentraciones como la legendaria Pingüinos. Surfista apasionado, le gusta surcar las crestas de las olas con la misma intensidad con que explora los binarios del código fuente.

Aiuken Solutions tiene su sede central en la calle Ayala de Madrid, entre Serrano y Velázquez, en pleno barrio de Salamanca. Está claro que les van bien las cosas. El edificio donde se encuentran las instalaciones es añejo. Un pedazo de la historia de Madrid. Techos altos. Patio interior. Portero vigilante que controla quién entra y sale del viejo ascensor enrejado, que sin duda fue un adelanto tecnológico envidiable en su día, pero que hoy resulta incómodo y aparatoso cuando lo comparten más de tres personas. Y más si uno de ellos va pertrechado con la chupa y el casco de la moto, y una aparatosa bolsa llena de cámaras y grabadoras.

Me apeo en la segunda planta. La puerta es imponente. Buenos materiales, como antaño. Llamo al timbre y espero hasta que una señorita muy amable me abre. «Hola, busco a Israel Córdoba.» Me pregunta de parte de quién. Le respondo simplemente que de parte de Toni, el amigo de Pepe. Me dice que está reunido y me invita a sentarme en un pequeño recibidor, a la izquierda, mientras le comunica que he llegado.

En el recibidor, una mesa camilla, sobre la que se amontonan algunas revistas de

informática y actualidad, y un par de sillas. Una de ella la ocupa un tipo elegante, trajeado, con pinta de ejecutivo, que también está esperando para reunirse con alguno de los directivos de Aiuken, mientras manipula frenéticamente su tablet de última generación, quizá consultando movimientos bancarios, vigilando las oscilaciones de la Bolsa o cualquiera de esas cosas que hacen los ejecutivos trajeados.

La espera es breve. De pronto se abre la puerta de uno de los despachos que da al recibidor y aparece un Israel Córdoba en mangas de camisa, aunque como siempre con corbata, que despide muy sonriente a otros dos tipos con pinta de ejecutivos. Parece que la negociación ha sido satisfactoria para todas las partes.

En cuanto me ve, se acerca a saludarme. Estrecha mi mano con energía.

—Dame un segundo y ahora estoy contigo.

Le observo mientras despide a los clientes y da unas indicaciones a la chica amable que me abrió la puerta. Esa sería solo la primera de mis visitas a la sede de Aiuken. Después vendrían muchas más. Porque Israel tendría la paciencia y la amabilidad de dedicarme muchas horas de su valioso tiempo, sin pedirme nunca nada a cambio. Y desde que pisé por primera vez sus instalaciones fui consciente del valor que tenía esa generosidad, porque para los profesionales como Córdoba el tiempo es oro. Literalmente.

—Ya estoy contigo, Toni. Disculpa la espera, teníamos que solucionar un problema que le ha surgido a esta empresa, y cada minuto que pasa significa pérdidas. Ven, acompáñame. ¿Quieres tomar algo?

El piso es enorme, heredero sin duda de la generosa arquitectura madrileña del XIX en un barrio como el de Salamanca, erigido en buena parte por el constructor malagueño José de Salamanca y Mayol que le dio nombre, y lo convirtió, desde el siglo XIX, en una de las zonas comerciales más importante de Europa. Recorremos el interminable pasillo dejando a derecha e izquierda distintas dependencias, y no puedo evitar fijarme en un cuarto que, a mi izquierda, acoge a un grupo de tres jóvenes aporreando sendos ordenadores. Intuí que ellos también serían hackers. Investigadores apasionados por la tecnología, capaces de hablar con los binarios. Probablemente de otra forma no se encontrarían allí.

—Cuando Pepe me explicó lo que querías hacer, me pareció una idea fantástica. Urgente y necesaria. Y puedes contar con todo nuestro apoyo: es necesario que la gente sea consciente de lo que está pasando lo antes posible.

Israel comenzó su declaración de principios antes incluso de que nos acomodásemos en uno de los despachos. Sobre la mesa solo había un ordenador portátil. Nada más. Me di cuenta de que la cámara del ordenador estaba tapada con un trozo de cinta adhesiva.

—Te lo agradezco muchísimo, Israel. Sé que no te sobra el tiempo.

Tenía 90 minutos y no iba a desperdiciar ni uno. Él tampoco. Mientras sacaba la cámara fotográfica y la grabadora, el *business-hacker* me confesó que él también tenía otras expectativas en mi investigación.

—No solo es importante que los usuarios se hagan conscientes de lo que está pasando con sus vidas digitales. También es hora de que alguien explique de verdad qué es un hacker y aclare un poco toda la desinformación que ha generado el cine y la televisión. Los hacker no son malos…

Me sorprendió la expresión. Israel había utilizado casi las mismas palabras que David R. Vidal, y ambos eran profundamente conocedores del tema. Y no solo eso, sino que durante los meses sucesivos otras fuentes me transmitirían exactamente el mismo mensaje. La comunidad hacker estaba cansada de que los medios de comunicación utilizasen incorrectamente su nombre para referirse a sus antónimos naturales. Y sin perder un segundo más, Israel entró a saco en el tema.

—La ciberdelincuencia está creciendo. España es el tercer país con mayor impacto de la ciberdelincuencia.

—¿Como víctimas o como generador del delito?

—Como ambas cosas. Cuando se va a generar un ataque, lo que buscan es un país donde no haya acuerdos de colaboración. A veces nos encontramos con que nos llega un cliente, y dependiendo de dónde esté el origen del ataque, sabes que no vas a poder hacer nada… Eso es un problema para él, y también para nosotros, porque nos coarta un poco el negocio. Porque si eres honesto, le dices: mira, yo te hago el análisis forense, te digo exactamente qué ha pasado, puedo decirte por dónde ha venido, incluso identificarte quién ha sido, y eso cuesta mucho dinero porque implica un coste de tiempo brutal, pero no te va a servir para nada.

El panorama era desalentador. Todas las estadísticas oficiales y privadas coinciden en que durante los últimos diez años el número de ciberataques crece proporcionalmente año a año. El problema es que muchos de ellos se realizan desde otros países, donde la legislación no ampara a las víctimas del país receptor del ataque. Y ni siquiera es necesario que el delincuente se encuentre físicamente en el país donde están los servidores informáticos que lanzan la agresión, lo que complica todavía más la investigación.

—Qué impotencia, ¿no?

—Sí. Ahora mismo hay dos problemas muy serios. Uno, que a nuestro entender no hay recursos en las Fuerzas de Seguridad del Estado para enfrentarse a esto. Te pongo un ejemplo muy claro. ¿Cuántos policías hay?, de calle me refiero… Miles, ¿no? Los grupos de Policía Nacional y Guardia Civil dedicados a los ciberdelitos, ¿cuántos pueden ser…? ¿Cien personas? ¿Cómo vas a proteger al ciudadano de la ciberdelincuencia? Al final el ciudadano, el usuario de internet, también se va a ver afectado, porque va a ser utilizado para agredir a una empresa…

—¿Cómo funciona eso?

—Los zombis… Un atacante, por medio de las vulnerabilidades de los sistemas operativos, de los navegadores o de los *routers*, incluso de las operadoras, tiene acceso a ellos y los utiliza como trampolín para dar el siguiente salto, y para esconder su rastro. Al final, la IP o la MAC adress que queda es la tuya, la de tu equipo. Claro,

luego tendría que venir alguien muy especializado, de Guardia Civil o Policía Nacional, hacer un análisis forense y decir, no, este señor no ha sido, lo que pasa es que no tiene los antivirus o los sistemas de protección necesarios, y el autor lo ha utilizado como puente… pero por de pronto te comes un marrón importante. Y ya le ha pasado a mucha gente.

Durante los meses siguientes tendría la oportunidad de conocer, entrevistar e incluso colaborar con los responsables tanto del Grupo de Delitos Telemáticos de la Guardia Civil, como de la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, y de las unidades de especializadas de otras policías, como la Ertzaintza, y todos coincidían en que los recursos del cibercrimen organizado, como ocurre en el caso del narcotráfico, superan con creces los de nuestras Fuerzas y Cuerpos de Seguridad.

En cuanto al uso de los «zombis», en agosto de 2015 se produjo la enésima polémica. El partido Ahora Madrid denunció que el Partido Popular utilizaba *botnets*, redes de ordenadores automatizados, para atacar a la recién elegida alcaldesa de Madrid Manuela Carmena, basándose en que su cuenta de Twitter recibía oleadas de críticas simultáneas y redactadas de forma idéntica. Un indicio evidente de ataque utilizando *botnets*.[35]

—¿Y cómo evito que conviertan mi ordenador en un zombi?

—Lo primero, no usando un antivirus pirata. ¿No habrás pirateado tu antivirus?

—Si te soy sincero… —dije sintiendo verdadero pudor—, no tengo antivirus. Nunca pensé que fuese importante…

—Increíble —resopló Israel negando con la cabeza, y repitió—: Increíble… Bueno, pues lo primero es instalarte un antivirus. Pero nunca uno pirata. Muchos de esos ya vienen con el «bicho» dentro. Tienes antivirus muy económicos, e incluso gratuitos, que se van actualizando con los nuevos «bichos» que se descubren cada día. Y eso también es importante. Actualizar tus servicios de internet. Cuando te llega el aviso de las actualizaciones de Google, Microsoft, etcétera, ¿lo ejecutas?

Negué con la cabeza sin atreverme a verbalizar mi incompetencia. Siempre había pensado que aquellos mensajes eran algún tipo de publicidad de los proveedores y me limitaba a ignorarlos.

—Madre mía… Pues a partir de ahora, no dejes de actualizar. Siempre. Esas actualizaciones se deben a todas las vulnerabilidades que se descubren cada día, y son los parches para repararlas. Si no los instalas, dejas tu equipo abierto. Luego está lo del sentido común: no abrir correos extraños, evitar el spam, etcétera. Pero visto lo visto, parece que a ti esto te da igual. Luego hay otras medidas, como salir por una VPN, un servicio que cifra lo que entra o sale de tu ordenador, dándote más seguridad… Son medidas de protección básicas. Aunque nada te garantiza la seguridad al 100%.

Lo mismo que me había dicho el «agente Juan». Lo mismo que me repetirían muchos por el camino. No era como para estar tranquilo.

—La NSA y los servicios secretos tienen sondas por todo el mundo que ven pasar el tráfico de la red. Sobre todo con el tema de la pederastia o el terrorismo, y cuando ven que llega a un ordenador, y como tienen poder para hacerlo, llaman a la Policía de ese país, por ejemplo aquí, y dicen: ese. Y claro, al final no eres tú, pero la patada en la puerta a las tres de la mañana, y las setenta y dos horas de prisión preventiva ya te las llevas.

—Por no hablar —añadí yo— del estigma social que te queda si en tu barrio se enteran de que te han detenido por un delito de pederastia en la red, o por terrorismo.

—Exacto. A ver quién es el guapo que te compensa de eso. Mira lo que le pasó a Hache.

—¿Quién es Hache? —pregunté sinceramente desconcertado.

De pronto, Israel cambió el gesto. Me dio la sensación de que había mencionado, sin quererlo, un asunto incómodo, desagradable, en el que no quería profundizar. Y no lo hizo. Cambió con elegancia de tema y obvió mi pregunta. Respeté su decisión. Pero anoté mentalmente averiguar quién era Hache y por qué su nombre había surgido en una conversación sobre pedofilia en la red y servicios secretos. Tardaría un año en llegar hasta él: una de las historias más sorprendente e ilustrativa de los riesgos que asumen los hackers en su cruzada contra la corrupción de la red oscura.

—Por eso —continuó Israel, cambiando el argumento— este tipo de iniciativas, como *x1red+segura,* que te enseñan a navegar, son tan importantes. Y por eso publicamos ese libro, para intentar minimizar el impacto de estas situaciones en la población, que es la más desprotegida.

—¿Y la administración? Supongo que igual que gastan nuestros impuestos en asfaltar carreteras o poner alumbrado, deberían preocuparse de las autopistas de la red…

—La administración tendrá que poner medios y gastarse el dinero. Antiguamente los bancos ponían un guardia jurado en la puerta, que ahora ha sido sustituido o complementado con cámaras. Ahora no basta con tener un ordenador bonito y que funcione bien. Debes tener otro equipo dedicado a la seguridad informática. Los diseñadores de programas y equipos se han concentrado en la operatividad de los sistemas, en que sean intuitivos, fáciles de manejar, que naveguen rápido… pero descuidaron la seguridad. Y ahora en los Estados Unidos están ofertando miles de trabajos en seguridad informática, porque es la gran amenaza. Si necesitamos cien mil o doscientos mil policías para asegurar nuestras calles… ¿Cuántos necesitamos para asegurar el ciberespacio? No serán doscientos mil, porque hay muchas herramientas automatizadas, pero te aseguro que no van a ser cien.

Suena el teléfono móvil de Israel, pero lo apaga sin mirar siquiera quién llama. Lo interpreto como una señal de que está cómodo hablando conmigo y de que cuando me concedió esos 90 minutos, son todos para mí. Un tipo de palabra. Así que me apresuro a continuar con las preguntas.

—Supongo que es como en todo. Yo lo he visto en otros trabajos anteriores. Pasó

con el tema de las bandas callejeras, el tráfico de personas o el narcotráfico. El delito siempre va por delante de la policía, así que supongo que tendrán que ponerse las pilas en lo referente a ciberdelitos…

—Tenían que haberse puesto las pilas ya.

—Yo soy un simple usuario, Israel. Utilizo mucho la red para buscar información, y me parece una herramienta maravillosa, pero desde que empecé a informarme sobre vuestro mundo, estoy aterrado. No era consciente de que existían tantas amenazas.

Al decir esto saqué de la mochila un ejemplar del último número de una conocida revista de informática, que publicaba un reportaje sobre las tendencias del cibercrimen en 2014: ataques a cajeros automáticos, virus para teléfonos móviles, campañas masivas de publicidad engañosa… Lo puse sobre la mesa señalando el artículo. Israel sonrió irónicamente. Estaba al corriente de esas tendencias.

—Es que ya no es como antes. Ahora cada vez más la justicia, la administración, los negocios, todo va por internet. Tu vida está en la red. Ahora, como no tengas unas credenciales en la red, no existes. Imagínate que alguien las borra…

—No entiendo.

—Tú imagínate que alguien borra tu DNI. Ahora tu identidad está en sistemas informáticos. Además, en sistemas interconectados. Si alguien consigue borrar toda la base de datos de la DGT, ¿qué pasaría? ¿Cómo comprueban que ese carné que llevas no es falso, o si el seguro de tu coche está al día? ¿Cuánto costaría arreglar eso? ¿Qué problemas causaría? ¿Y si alguien simplemente introduce en la red que estás muerto?

Un año después los hackers harían real la reflexión de Israel. Durante la DEF CON 2015, una de las conferencias de hacking más prestigiosas de los Estados Unidos, el investigador Chris Rock materializó la angustiosa fantasía cinematográfica que vive Sandra Bullock en la película *La Red* (1995), al presentar su conferencia «I Will Kill You» («Te mataré»), en la que explicó las vulnerabilidades del sistema de notificaciones funerarias norteamericano. Rock expuso cómo era factible hackear el sistema para introducir un informe de defunción, falseando los credenciales de un médico. A partir de ese instante la víctima está legalmente muerta, y sus problemas comenzarán cuando tenga que renovar algún documento oficial, o realizar algún trámite legal. En la misma comunicación, Chris Rock explicó cómo el proceso podía utilizarse también para «crear» a una persona, aprovechando las vulnerabilidades del sistema para insertar una partida de nacimiento en el registro.

—Y como eso muchas cosas. Ahora toda nuestra vida está en sistemas. Y no basta con que estén operativos, sino que deben estar asegurados. Cuando hablamos de las estructuras críticas (agua, electricidad…), el gran problema es que las aplicaciones que rigen los sistemas, las bases de datos, los programas, se han desarrollado sin tener en cuenta aspectos de seguridad. Cuando construyes un banco te aseguras desde el principio de que los cristales sean blindados, las alarmas operativas, las cajas fuertes sean inviolables… Cuando haces una aplicación de banca *online* también deberías asegurarte de que sea blindada, no solo fácil de usar… Pues esa parte nos la hemos

saltado en la mayoría de los casos.

—O sea, que cuando consulto mi cuenta bancaria por internet, puedo estar poniendo en peligro mi dinero… Joder, Israel, no sé si quiero saber todo esto. Vivía más tranquilo en la ignorancia.

—No te vuelvas loco. Los mayores ataques no se consiguen vulnerando sistemas de protección. Se consiguen desde dentro, utilizando usuarios. O trabajadores que se han ido de la empresa. Habrás oído lo de Sony…

Asentí con la cabeza sin atreverme a interrumpirlo. Israel Córdoba se refería al ataque informático que Sony Online Entertainment (SOE) recibió en abril de 2011, y que afectó a 24,6 millones de cuentas de usuarios en todo el mundo, incluyendo a 3 millones de españoles. El gigante se vio obligado a cerrar los servicios de su red PlayStation Network (PSN) mientras investigaba el origen del ciberataque.

—El ataque a Sony fue muy famoso —continuó—. Robaron todos los passwords y contraseñas de los usuarios… fueron 18 millones incluyendo tarjetas de crédito, porque es lo que utilizas para bajarte aplicaciones, juegos… Tú imagínate la pérdida que supuso para Sony, además de las demandas que le cayeron… Esto puede hundir a una empresa. A lo mejor no una del tamaño de Sony, pero sí a la mayoría.

—Y supongo que eso es lo que evitaréis aquí, ¿no?

—Nosotros solo nos dedicamos a la seguridad telemática. Esto significa seguridad en sistemas y comunicaciones. Ofrecemos servicios de protección y asesoramiento a las empresas. A todos los niveles. No solo tecnológicos, sino también humanos. Si blindas la web de una empresa de comercio *online*, y luego viene un empleado despechado y filtra las contraseñas del servidor, sigues teniendo un problema. Si tú tienes un portal de venta *online* y por un ataque o un sabotaje está *offline,* la gente no compra y tú no ganas. Y si nuestro cliente no gana, nosotros tampoco.

A mediados de 2014, según el informe del Centro de Estudios Estratégicos Internacionales (CSIS), patrocinado por McAfee, se calculaba que las empresas sufrían unas pérdidas de 445.000 millones de dólares.[36] Pero en 2015 será mucho peor.

—O sea, que vuestra misión es garantizar que la empresa está en línea…

—Bueno, eso y mucho más. No basta con que tú garantices que el servicio está en la red. También tienes que monitorizar que nadie hace cosas raras, como comprar sin pagar… que eso también pasa. Hay quien reserva hoteles sin pagar, compra vuelos sin pagar, utiliza tarjetas *fakes,* etcétera, y todo eso supone pérdidas para las empresas. De hecho, las tarjetas son una de nuestros mayores quebraderos de cabeza.

—Te refieres a las tarjetas de crédito…

—También, pero no solo eso. Las tarjetas que ahora te dan todos los comercios para fidelizarte, las de las gasolineras, los centros comerciales… todas esas tarjetas llevan un montón de información sobre ti. Y esa información puede ser utilizada en tu contra si cae en malas manos. Por eso nosotros también tenemos que vigilar el uso

que se hace de las tarjetas de nuestros clientes. Imagínate qué pasaría si mañana alguien subiese a internet los datos personales incluidos en las tarjetas de todos los clientes de Carrefour, El Corte Inglés o Ikea… O los vendiese a empresas especializadas.

—¿Big Data?

El Big Data o procesamiento masivo de datos es la nueva tendencia en la red. Ante el torrente brutal y gigantesco de datos que manejan los proveedores de internet, las tecnologías de la información y la comunicación comenzaron a desarrollar técnicas para la captura, almacenamiento, búsqueda, compartición y análisis de esa ingente cantidad de datos con objeto de rentabilizarlos publicitariamente, como análisis de negocio, para control social o espionaje.

Cuando entras en Google, por ejemplo, en la parte inferior de la pantalla de tu dispositivo aparece el botón «Privacidad». Púlsalo y lee lo que Google te dice que hace con tus datos e historial de búsquedas… Te sorprenderás.

—Por ejemplo. En esas tarjetas no solo están tus datos personales. También está lo que has comprado, cuándo y dónde lo has comprado. Y esa información es muy valiosa para el Big Data. Cada página que visitas. Cada búsqueda que haces en Google. Cada comentario que dejas en tu Twitter. Toda esa información ayuda a definir tu perfil de usuario, y los verdaderos marketinianos y los profesionales de *business inteligence* asocian esas tarjetas a otras para definir tus comportamientos de usuario. ¿Tú por qué crees que cuando navegas por la red empiezan a aparecer en tu pantalla anuncios de productos que te interesan? ¿Crees que es casualidad? Pues la mala noticia es que no solo Amazon, Google o eBay están interesados en tus conductas en la red, porque reflejan tus conductas en la vida.

—Hablas como si estuviésemos en la película *Matrix*.

—Hace tiempo que entramos en Matrix…

Quien entró en ese momento fue David Pérez, uno de los agentes destinados en la Brigada de Delitos Informáticos del Cuerpo Nacional de Policía con sede en la comisaría de Canillas. Israel y él son buenos amigos, y gracias a eso David se convirtió en otro de mis guías en este viaje. David, un *rara avis* en su brigada, fue hacker antes que policía, y conocía perfectamente a toda la comunidad.

Me fui de allí con bastantes dudas, y un par de decisiones tomadas. Esa misma tarde me compré un antivirus, actualicé los servicios de internet y contraté una VPN. También aprendí a buscar el candado que aparece en el navegador, y el encabezado https en lugar del http, al entrar en mi cuenta bancaria. Israel me explicó que ese candado y el protocolo https implican el cifrado de mis operaciones y por tanto mi seguridad. Pero ni con todo eso me sentí más seguro. Por si acaso, al final tapé con un trozo de celo la webcam de mi ordenador. No lo he quitado desde entonces.

MARZO DE 2014
EL CACHORRO DE ULTRASSUR

«Esta es una táctica basada en un cálculo preciso de toda debilidad humana, y su resultado llevará al éxito con certeza casi matemática. (…) Logré comprender igualmente la importancia del terror físico para con el individuo y las masas.»

Adolf Hitler, *Mein Kampf*, cap. 2

MarkoSS88 tardó tres días en contestar a mis mensajes e interpreté aquel silencio como fruto de la sorpresa. Por fin, el 8 de marzo, dio señales de vida. En mi primer email intenté ser conciliador:

Estoy dispuesto a aclararte cualquier duda. Si has encontrado en mi libro algo que no sea cierto, estoy dispuesto a corregirlo… Dime cualquier cosa que hayas visto que creas que no es real y si tienes razón, te prometo reconocerlo.

Nuestra relación «ciberespistolar» comenzó con energía. MarkoSS88 era directo en sus respuestas, pero su actitud resultaría cómica de no ser tan trágica:

¿Algo? ¿Es que acaso en tu libro hay algo cierto? No, no me he leído el libro ni lo voy a hacer, eso es traicionar a los míos, más que nada no me voy a gastar un pastón para enfadarme más contigo, partes que me han comentado del libro, hay cosas que no cuadran; exactamente a ti ¿qué te pasó con nosotros? ¿Por qué solo persigues a los NS? ¿Y los anarquistas? ¿Y los comunistas? Has metido a muchos camaradas míos en la cárcel y sé que tú has tenido algo que ver con lo de US, has jodido a mucha gente… No sabes con quién has dado. Hace un par de semanas estuviste en la universidad de Madrid dando una charla, no conseguí entradas, si no, me hubieses visto en primera fila. Eres con Alfonso el bukanero, las personas a las que más odio…

Ciertamente era previsible. De hecho, lo contrario habría sido sorprendente. En muchas ocasiones me había enzarzado en discusiones similares con jóvenes neonazis que me acusaban de lo mismo y que, como Markos, confesaban cuestionar un libro que no habían leído. Sus prejuicios, tópicos, y retóricos reproches se sustentaban en los comentarios de sus camaradas, que tampoco habían leído el libro, o en las burradas que podían haber leído en la red.

Lógicamente, cada uno se siente afectado por lo que le duele, y Markos, como otros muchos antes que él, ignoraba que después de *Diario de un skin* había realizado otros trabajos similares, infiltrándome en grupos de extrema

izquierda, terroristas, de crimen organizado, etcétera, así que me lo puso en bandeja para romper sus prejuicios demostrándole que estaba equivocado en su afirmación de que «solo persigues a los NS». Esa parte era fácil. Tengo publicados suficientes trabajos sobre la violencia antifascista, así que solo necesitaba enviarle unos cuantos enlaces para poner de manifiesto su error. Mi siguiente email fue largo y enérgico.

> ¿Que por qué no me meto con los comunistas, los anarquistas…? Dios… es que no has leído nada de lo que yo he escrito. He hecho exactamente lo mismo que con el movimiento NS, con los «guarros», con los comunistas, con los narcos, con la extrema izquierda… Y recibo el mismo odio de gente de esos grupos que, como tú, no se molestó en leer lo que critica. *El Palestino,* que es el doble de gordo que *Diario…* es precisamente sobre el mundo de la extrema izquierda. De ETA a las FARC, pasando por los grupos armados bolivarianos o las guerrillas comunistas. No fuisteis vosotros los que me condenasteis formal y públicamente a muerte, sino los grupos de ultraizquierda. Comprendo que alguno de tus colegas, los condenados en el juicio a Hammerskin, me odie. Pero no los condenaron por mi libro, sino por la investigación policial… Vale que no quieras leer mis libros, y aun así opines sobre ellos, pero tío, joder, podías leerte al menos mis artículos. Estoy harto de escribir sobre las «cacerías» de los antifas, y sobre la violencia de extrema izquierda… Pero nada, tú has preferido hacerte tu película, en base a lo que te contaban, sin molestarte en leer ni un solo trabajo mío sobre ese tema, que niegas que exista: http://www.antoniosalas.org/neonazis/articulo/la-caza-del-nazi-el-nuevo-deporte-de-la-ultraizquierda
>
> Pero es que hay más, mucho más. Supongo que fliparás cuando te diga que tengo grandes y queridos amigos NS. Ellos sí se leyeron el libro y reconocieron que todo lo que contaba, TODO, era absolutamente real. Tanto lo bueno, como lo malo, porque no sois santos, Markos, nadie lo es. Tampoco yo. Pero ellos, a diferencia de ti, decidieron hablar conmigo antes de montarse una película paranoica. Se ahorraron las horas y horas que tú has perdido navegando por la red, y la mala leche que has pasado por nada. Y era tan fácil como abrir mi web o mi Facebook y escribirme un correo… ¿Ni eso pudiste hacer? Pregunta a cualquier lector que me haya escrito. Todos te dirán lo mismo. Yo respondo todos los mails. Todos, incluso cuando me ponen a parir. Y lo habría hecho contigo desde el primer momento. Porque creo que tengo razón en lo que escribo, y estoy dispuesto a defenderlo ante quien sea. Y si me equivoco, quiero saberlo. Pago un precio muy alto por mi libertad. No tengo sueldo, ni paro, ni vacaciones. No trabajo para ningún medio, ni grupo editorial, ni colaboro con ningún cuerpo policial… Así que soy el único responsable de lo que hago, para bien o para mal. Pero conmigo no cuela lo de «perro del sistema». Eso resérvatelo para otros. Yo voy por libre. Y te juro que en este curro, y en esta puta crisis, mantener la independencia es jodidamente difícil.

Demostrarle que no solo había escrito sobre sus camaradas era sencillo. Pero convencerle para leer el libro iba a ser un poco más complicado.

Muchos cientos de jóvenes skinheads y skingirls habían dejado el movimiento neonazi tras leer *Diario de un skin,* y estaba tan seguro de que podría convencer a Markos para que los imitase que me ofrecí a enviarle un ejemplar con el fin de que valorase por sí mismo si lo que yo contaba era cierto o no. Se lo enviaría a cualquier dirección que él me diese, un apartado de correos, el bar de un colega, la casa de un camarada… Y gratis. «Solo si lees los libros te darás cuenta de cuánto tiempo has perdido odiándome por nada, y de lo profundamente equivocado que estás en todo… La pelota está en tu tejado», le dije.

Esta vez su respuesta no se hizo esperar. Markos no tardó ni veinticuatro

horas en contestar a mi provocación, en un email tan extenso como el mío. Abordaba todas las cuestiones con la misma convicción que yo. Y no parecía dispuesto a ceder ni un ápice en sus planteamientos.

Markos había leído los enlaces que le envié y lo que era más importante, quería leer más. Pero lo más importante es que en otro de sus párrafos no se cerraba a la posibilidad de que le enviase mi libro. Más bien mantenía una prudente desconfianza, comprensible dadas las circunstancias.

> No, claro que no he leído nada de lo que has escrito, te lo he dicho, es odio, tío, es puro odio, pero bueno, lo leeré para poderte decir lo que veo injusto, lo que no, bien o lo que veo mal, tienes razón en eso de que no «tengo derecho» a opinar si no he leído nada de lo que has escrito, no te lo niego, vale, pero sigo pensando en lo mismo…
>
> … Me gustaría tener esos libros personalmente y no por internet, todo libro hay que leerlo en hojas pero si te doy mi dirección, la de un camarada o la de algún lado para recogerlos nos van a detener o al camarada que lo recoja o a mí en cuanto vaya a recogerlo…

Entonces ocurrió algo sorprendente, pero que definiría mi siguiente paso en relación a MarkoSS88. Más de ochenta funcionarios de las Unidad de Intervención Policial fueron heridos en las Marchas por la Dignidad del 22 de marzo. La Providencia, como siempre, decidió mover ficha de la forma más inesperada.

El día 22 de ese mes de marzo, el Cuerpo Nacional de Policía, y más concretamente las Unidades de Intervención Policial (UIP, conocidos como «antidisturbios»), vivieron uno de los episodios más desconcertante de su historia. Durante las Marchas de la Dignidad —una manifestación de protesta contra los abusivos recortes justificados con la crisis económica— se produjeron altercados violentos… Eso no es ninguna novedad. Las imágenes de las UIP cargando contra los manifestantes (según las fuentes policiales, contra los alborotadores que inician los altercados) tampoco eran ninguna novedad. Pero en esta ocasión algo salió mal. Aquel 22 de marzo, pasada la medianoche, la violencia se desató en las calles de Madrid, y la pésima coordinación de las unidades antidisturbios nos dejó unas imágenes inéditas en los informativos. Esta vez eran los policías de las UIP los que sufrieron brutales agresiones.

Más de ochenta funcionarios salieron heridos de diversa consideración en los altercados, y eso no había ocurrido jamás. No hacía falta ser un observador demasiado avezado para intuir que allí había sucedido algo extraño, y yo tenía unas fuentes privilegiadas. Las víctimas.

Unos días después de los altercados, David Madrid convocó una de las cenas-tertulia que organizaba en su domicilio, y a las que asistíamos periódicamente un grupo de amigos, todos policías menos su esposa y yo.

María, la pareja de David, es criminóloga. Tras la publicación de mi primer libro se había puesto en contacto conmigo porque estaba interesada en hacer un trabajo sobre los grupos violentos, y quería entrevistarme. En aquel momento yo andaba sumido en la infiltración en la trata de blancas y de todas formas tampoco podía prestarme a una entrevista personal, así que la puse en contacto con David Madrid, y de aquella relación profesional surgió el amor… y un hijo encantador. Y hasta hoy.

Aparte de María y yo —bueno, y de Yoda, el gran gato de David y María que observaba nuestros apasionados debates acurrucado en el sofá del salón—, todos los demás: Álex, Rubén, Toni, Pepe, etcétera, pertenecían a uno u otro Cuerpo.

Siempre era igual. La cena, que se prolongaba hasta altas horas de la madrugada, era una excusa para reunirnos e intercambiar puntos de vista o información sobre los temas que a todos nos interesaban: crimen organizado, tribus urbanas, terrorismo… Esa vez, los sucesos del 22 de marzo anterior casi monopolizaron el debate. Y era lógico. Varios de los presentes en la cena pertenecían o habían pertenecido a las UIP, y habían sido agredidos aquella noche.

—¿No has visto a Rubén en los informativos? —me preguntó David—. Ahora es famoso, fíjate, hasta es portada en la web del sindicato…

Miré a Rubén de reojo, y vi que encogía los hombros con una sonrisa de complicidad. Rubén, como la mayoría de los funcionarios de las UIP, es un tipo fuerte. Grande como un armario ropero de madera de roble. No es un tipo al que puedas agredir fácilmente.

—Míralo, míralo tú mismo —insistía David mientras tecleaba en su ordenador la dirección de la web del SUP.

En la página de cabecera del Sindicato Unificado de Policía se había situado como imagen de portada la foto de un policía recibiendo un palazo en la cabeza, propinado por una de las manifestantes. Era Rubén.

Bajo aquel uniforme, que confiere a las UIP el aspecto de una temible legión romana, Rubén es mucho más que una masa de músculos. Nadie sospecharía que aquel funcionario de policía, que encabeza las cargas policiales cuando los disturbios se desatan en cualquier manifestación, dedicaba su tiempo libre a fomentar valores como la deportividad, el compañerismo y la superación personal, como voluntario en un centro de acogida de niños con problemas familiares. Y los chavales le adoran. Pero también es consciente de que la brutalidad de algunos de sus compañeros —cuando el oficial al mando da la orden de dejar de aguantar los insultos y las provocaciones y disolver a los manifestantes— los ha encasillado en la mala imagen que tienen esas unidades policiales entre el resto de la población. Una mala imagen generada por algunos de sus componentes,

especialmente cretinos.

Aquella noche, año y medio antes de que se aplicase la Ley Mordaza, fui testigo de cómo varios miembros de las UIP intuían que habían sido «marionetas» del sistema, intencionadamente mal coordinados por sus superiores para sufrir una brutal agresión que justificase un endurecimiento en las leyes de seguridad ciudadana.

—Lo hemos comentado muchos compañeros, Toni. No fue normal. Nos enviaron al matadero para que nos forrasen a hostias, sabiendo que no teníamos ni la cobertura ni la equipación apropiada para ese operativo… Y muchos pensamos que lo hicieron para tener una justificación gráfica que les permitiese endurecer la ley… Fuimos su excusa.

Cuando escuché sus comentarios sobre el operativo de aquella noche, cómo analizaban una y otra vez el modo en que habían sido desplegados sobre el terreno sin el debido apoyo, y cuando me mostraron las imágenes de las brutales agresiones que sufrieron algunos de sus compañeros, heridos de gravedad en los altercados, pensé que estaban paranoicos. Que ni siquiera los políticos más carroñeros podrían haber ideado un plan tan maquiavélico: utilizar a sus policías masacrados como justificación para el endurecimiento de una ley. Quizá me equivoqué. Lo que se estaba gestando en aquellos momentos en los despachos del Gobierno de España era una remodelación total de la Ley de Seguridad Ciudadana, que afectaría de forma demoledora a nuestras libertades. No solo en las calles. También en la red. Y yo tendría el privilegio de seguir el proceso tal y como lo vivió la comunidad hacking. Porque en buena medida las reestructuraciones legales que popularmente se denominaron Ley Mordaza comenzaron esa noche, y

entre ellas se convirtieron en delito varios comportamientos en la red que antes no lo eran. Aunque lo que más afectó a la comunidad hacker fue la ilegalización de ciertas herramientas de hacking utilizadas a diario por los consultores de seguridad informática, pero que un año y medio después del 22-M podrían considerarse armas.

Años atrás, durante una infiltración en el movimiento antiglobalización, había tenido la oportunidad de recibir adiestramiento para enfrentarme a las UIP, en una casa okupa en Barcelona. Si yo me limitase a hacer una afirmación tan osada, solo avalada por mi testimonio, es probable que no tuviese la menor repercusión. Pero para eso existía la cámara oculta. El peso de la evidencia audiovisual concluye todo debate. Quizá por eso, en 2012, el Tribunal Constitucional prohibió su uso en periodismo.

Mis grabaciones de cámara oculta de aquellos talleres todavía estaban en mi archivo, y aunque el instructor cubano de artes marciales que nos enseñó a aquel puñado de jóvenes antisistema a enfrentarnos a los antidisturbios presumía de ser campeón de karate, ochenta miembros de las UIP heridos se me antojaba demasiado. Incluso para una legión de guerreros antisistema debidamente coordinados.

De vuelta a casa, y al recibir un nuevo email de MarkoSS88, se me ocurrió rescatar aquellas imágenes de mi archivo y escribir un post para mi blog. Y así lo hice. Aproveché la percha de actualidad para redactar aquel pequeño texto cuyo principal destinatario era Markos. Quería demostrarle, por si le quedaba el menor asomo de duda, que yo también me había infiltrado entre sus odiados enemigos, y que también había utilizado la cámara oculta con ellos. Ese fue el objetivo principal del post «Cazar policías».[37] Pero se me fue de las manos. De inmediato, diferentes webs y blogs replicaron la entrada de mi página, y el vídeo, subido a YouTube, recibió miles de visitas en pocas horas. Más tarde, los informativos de algunas cadenas de televisión nacional también lo utilizarían.

Pocas horas después de que hubiese enviado a Markos este escueto email con el enlace al artículo: «Lo escribí pensando en ti. Te contesto esta tarde desde un cíber trankilo», miles de espectadores habían visto ya mi vídeo en los informativos. Alfonso Merlos, el periodista televisivo más mediático de 13TV en ese momento, fue uno de los colegas que se interesaron por entrevistarme al hilo de aquellas imágenes. Aunque tuviesen más de diez años de antigüedad. Supongo que tras lo ocurrido el 22-M, les pareció oportuno. Merecería la pena analizar cómo los medios conservadores utilizaron mis imágenes para criminalizar a los manifestantes como si se tratase de violentos «cazadores de policías» adiestrados en locales okupas para agredir a las UIP… Y no era la primera vez que lo hacían.

Aun así, mi objetivo era Markos. Lo único que quería era ganarme su confianza. Que supiese que no era el antinazi que le habían vendido sus camaradas, sino un periodista que hacía su trabajo, en un extremo y otro del espectro político, intentando mantener la independencia y la objetividad. Y funcionó. Cuando me contestó el correo supe que había pillado el mensaje:

> Gracias por sacar eso a la luz, a pesar de que te tachen de «nazi»; la gente tiene que darse cuenta de que la extrema izquierda no son tan buenos ni nosotros somos tan malos. La verdad es que me tienes un tanto desconcertado…

Como también era previsible, las grabaciones de cámara oculta en el taller de artes marciales contra la policía —o más bien el uso que hicieron los medios conservadores de las mismas— desataron las iras del movimiento antifascista y anticapitalista. Muy pronto los foros y las web que reproducían mis grabaciones se llenaron de insultos y amenazas. Me acusaban de fascista, vendido, nazi… Ni uno de aquellos críticos se tomó la molestia de leer el texto que acompañaba las imágenes y que explicaba quién era el responsable de aquellos talleres y las implicaciones políticas y geoestratégicas de aquella investigación. De haberlo hecho, se habrían dado cuenta de que yo apuntaba en otra dirección. Pero es lo que suele ocurrir cuando las ideologías se defienden con las tripas y no con el cerebro.

Tampoco me importó demasiado. El objetivo de aquel post era que Markos no me viese como un adversario, que se leyese mi libro y quizá, con un poco de suerte, que se diese cuenta de lo absurdo del mundo de violencia en que vivía y decidiese abandonarlo. Y al menos había accedido a la primera parte.

Por fin, Markos aceptó facilitarme la dirección de una antigua vecina. Preparé el paquete y le envié mis libros con la esperanza de que, tras leerlos, se diese cuenta de que sus ideales neonazis, su justificación de la violencia, y el odio irracional hacia mí que le corroía por dentro eran un absurdo. Ahora solo quedaba esperar.

Capítulo 4
Inmigrantes digitales en una red más segura

«Los ordenadores son buenos siguiendo instrucciones, no leyendo tu mente.»

Donald Knuth

«Ahora, cuando miramos a nuestros amigos a los ojos no vemos más que nuestro propio reflejo en el monitor.»

Ángel Pablo Avilés, «Angelucho»

El mejor antivirus eres tú. Tu mayor vulnerabilidad, también

Durante nuestro primer encuentro, Israel Córdoba me descubrió un concepto que era nuevo para mí: el de «nativos digitales» frente a los «inmigrantes digitales».

—Nosotros llamamos nativos digitales a la generación nacida a partir de los ochenta, cuando las nuevas tecnologías ya empezaban a implantarse en la sociedad —me había dicho—. Los chavales que nacieron a partir de entonces aprenden a manejar un teclado de ordenador o un teléfono móvil casi al mismo tiempo que a caminar. Pero sus padres y sus abuelos han tenido que adaptarse a estas nuevas tecnologías poco a poco, porque actualmente si no estás en la red, no existes. Y muchos están incorporándose ahora, aprendiendo a usar el WhatsApp, Facebook, el email… Inmigrantes digitales.

Yo asentí, me sonaba de sobra: todos tenemos casos muy parecidos… Mi madre no es una nativa digital. No nació ni vivió tan dependiente de la tecnología como lo hizo mi generación, y más aún las siguientes. Pero como muchas mujeres de su edad, al final terminó claudicando. Primero entró el teléfono móvil. Y a mí me pareció bien. Me gustaba saber que podía tener la oportunidad de escuchar su voz, si lo necesitaba, aunque no estuviese en casa.

Después llegaron los sms. Al principio le costó un poco porque no se aclaraba con las teclas, aunque un mensaje era más barato que una llamada, y eso siempre es una buena motivación para agudizar el ingenio.

Pero más tarde se empeñó en tener WhatsApp. Y eso ya no me hizo tanta gracia. Cuanto más leía sobre las vulnerabilidades de las nuevas tecnologías, más críticas me encontraba a ese sistema de comunicación. Al parecer, varios investigadores habían descubierto formas de romper la seguridad de WhatsApp para acceder a los mensajes de otros usuarios, y no me hacía ninguna gracia que alguien pudiese leer los WhatsApp de mi madre. Pero su argumento era irrefutable:

—Pues yo quiero WhatsApp. Todas mis amigas lo tienen y no voy a ser yo la única que se quede fuera. Si no me lo pones tú, ya encontraré a alguien…

Porque después del WhatsApp llegó el correo electrónico. Mi madre, como muchas madres, también quería tener su propio email, aunque solo fuese para saturarme el correo de *memes*, vídeos de gatitos o chistes. Los mismos que le reenviaban sus amigas. Mi madre desconocía que los ciberdelincuentes utilizan esas imágenes tiernas e irresistibles, invitándote a que las reenvíes a todos tus contactos, para transmitir sus virus de ordenador en ordenador, o para conseguir direcciones de email operativas. Y nosotros se las damos cada vez que reenviamos esos emails «tan monos» a todos nuestros contactos, y el ciberdelincuente recibe una copia con todas las direcciones de email actualizadas, para saber a quién debe dirigir su próximo ataque.

Igual que, haciendo gala de una insensibilidad que roza el sadismo, los *spammers* utilizan las grandes catástrofes para lanzar a la red sus campañas de *phishing* ocultas tras un email solidario. Tras ver en los informativos las dramáticas imágenes del Tsunami de 2004 o el terremoto de Japón, ¿quién se resistiría a reenviar un email que nos promete que las víctimas recibirán una donación, solo con que nosotros hagamos *clic* en un enlace, o por reenviarlo a todos nuestros amigos? A la hora de escribir estas líneas, en septiembre de 2015, tras la terrible crisis de los refugiados sirios que está dividiendo Europa, los ciberdelincuentes han encontrado un nuevo vector de ataque, y en mi buzón de correo comienzo a recibir el mismo spam de siempre, ahora disfrazado de refugiado sirio… Seguramente también tú has recibido alguno.

Es necesario que mi madre, y todas las madres, padres, abuelos y nietos comprendan los mecanismos de las estafas en internet, porque no existe un único modelo. El *phishing* no solo se transmite a través de los vídeos de animales o paisajes, o las campañas solidarias. Todo mensaje, por email, sms, WhatsApp o redes sociales que te invite a reenviar un contenido o a visitar una página desconocida puede encerrar una campaña de fraude en masa. Y caer en la trampa no solo nos perjudica a nosotros, sino que infectamos a todos nuestros amigos.

En el primer trimestre de 2015, la firma de antivirus Kaspersky registró 50,07 millones de reacciones de su sistema contra *phishing*, lo que supone un aumento de un millón frente al primer trimestre de 2014. Y los estafadores utilizaron noticias de gran difusión, como la muerte de Amy Winehouse, para excitar la curiosidad de la víctima incitándole a pinchar en el enlace infectado.[38] En el *phishing* vale todo. Utilizarán cualquier cosa que pueda motivarte.

Y después llegó el Facebook. Mi madre también quería entrar en las redes sociales. Y de nuevo la misma discusión absurda.

—Pero, mamá, ¿para qué quieres tú un Facebook?

—Porque todas mis amigas lo tienen…

Mi madre es buen ejemplo de esa generación de inmigrantes digitales, que llegan a las nuevas tecnologías con mejor intención que conocimientos. Y por ello se encuentran en el perfil de mayor riesgo de cara a los delitos cibernéticos.

Hoy un anciano de ochenta años y un niño de ocho saben que tienen que mirar a ambos lados al cruzar la calle, que no deben internarse en plena noche (ni tampoco de día) en barrios de dudosa reputación y que si no quieren que les roben sus bienes más preciados, deben guardarlos bajo llave… Pero no sospechan que en internet también existen lugares de mala reputación. Que deben leer a un lado y otro antes de darle al *clic*. Y que para que no les roben sus vidas digitales, deben guardarlas bajo contraseñas seguras.

Estoy seguro de que muchos de ellos saben más por viejos que por diablos, y que han desarrollado el instinto que otorga la experiencia de una larga vida, para detectar la expresión corporal y la comunicación no verbal cuando alguien les cuenta una mentira. Pero en las redes sociales no existe esa posibilidad. Ni siquiera a través de la

webcam, que ralentiza el numero de *frames* por segundo de la imagen, impidiendo valorar toda forma de expresión no verbal. Y el 29% de los incidentes de seguridad informática están relacionados con nuestro uso de las redes sociales.

Hay cosas, no muchas, que cualquier persona no familiarizada con la tecnología puede entender que son buenas o malas.

Simplemente con echar un vistazo a la dirección que aparece en el navegador de nuestra pantalla (la URL), cuando somos redireccionados a nuestro banco desde el email que acabamos de recibir de nuestra sucursal evitaría el 98% de las estafas por *phishing*. Pero no lo hacemos. Yo no lo hacía. Sin embargo, el consejo: «Mamá, mira la dirección del navegador cuando entres en el banco y comprueba que es la correcta» es fácil de entender para cualquiera. Igual que es comprensible, para cualquier inmigrante digital, que es importante utilizar contraseñas fuertes para proteger tus cuentas de email o sociales. No es buena idea utilizar la contraseña 1234, ni *Password*, ni obviedades por el estilo, porque los ciberdelincuentes saben que son las más utilizadas. Yo descubriría una forma genial de establecer contraseñas sólidas y seguras unos meses más tarde, y de la mano del jefe de Angelucho en la sede del Grupo de Delitos Informáticos de la UCO, el capitán César Lorenzana, otro de mis guías en este viaje.

Pero mientras, ¿cómo podría explicarle a mi madre que, a veces, algo tan natural como visitar la página web de un famoso, puede contagiarnos un virus? A ella le encanta la actriz Marta Torné. A mí también, desde la primera vez que la vi en *Vitamina N* de City TV. Estuvo enganchada a la serie *El Internado*. En la primavera de 2007, mi madre no tenía acceso a internet, pero de tenerlo podría haberse convertido en una de las víctimas contagiadas por MPack, el virus que afectó a 11.000 webs en todo el mundo, mayoritariamente alojadas en el mismo proveedor de espacio para dichas web *(hosting):* Aruba. MPack era un *malware* (software malintencionado) que cualquiera podía comprar por 700 dólares en el mercado negro, para luego infectar miles de páginas, como la de Marta Torné. Quien visitaba esas páginas, con su navegador desactualizado, quedaba infectado.

Según un cálculo del brillante Fernando de la Cuadra: «El dinero obtenido en un año por el *malware* supera con creces el PIB de muchos países. Y en billetes de 500 euros, da para alfombrar España entera». Una parte de ese dinero proviene de los bancos, que constantemente sufren robos millonarios, aunque prefieran ocultarlo para evitar la estampida de clientes. Otra, del espionaje industrial, militar y político. Pero una parte importante del millonario negocio del *malware* está originada en el tráfico de vidas, en los robos que sufrimos a diario los simples usuarios. Solo que si un periodista veterano, como yo, que lleva años utilizando internet a diario, no ejecutaba las actualizaciones, no cambiaba periódicamente las contraseñas, ni comprobaba el navegador hasta hace bien poco, ¿cómo pretender que alguien recién llegado a la red, como era el caso de mi madre, lo hiciera?

Por lo que me contaba Israel Córdoba, unos años atrás Angelucho, autor de

x1red+segura, se había encontrado con el mismo problema:

—Él es guardia civil —me contó—. Está destinado en el Grupo de Delitos Telemáticos de la UCO, y además tiene un blog sobre seguridad informática destinado a hacer más accesible a los usuarios las medidas de precaución básicas para una navegación segura. A Ángel le preocupa mucho la vulnerabilidad de los chavales más jóvenes cuando comienzan a navegar por la red, porque la red encierra muchos peligros. Pero también le preocupan mucho los inmigrantes digitales que se han encontrado ahora con las nuevas tecnologías. Estaba muy preocupado por los riesgos a los que podría enfrentarse su padre al comenzar a moverse por la red, así que abrió un blog: www.elblogdeangelucho.com, donde se esfuerza por hacer accesible a nivel de usuario toda la información básica sobre seguridad informática que necesita un internauta para moverse mínimamente seguro por la red. A nosotros —se refería a su empresa, Aiuken Solutions— nos pareció una idea genial, así que decidimos respaldarle económicamente para que lo más relevante de su blog pudiese publicarse en forma de libro.

Tal vez esta sea la lectura más recomendada para alguien que desee iniciarse, desde cero, en la seguridad de su vida digital. Para mí lo fue. Tras haberme gastado un dineral en libros técnicos sobre hacking y seguridad informática de los que no entendía absolutamente nada, el libro de Angelucho supuso un soplo de aire fresco. Estaba redactado para legos en la materia, y en un idioma accesible. Pero su esfuerzo no se quedó ahí: el 17 de mayo de 2013 la utopía trascendió las páginas y los bits para materializarse con la celebración de las primeras jornadas X1Red+Segura que tuvieron lugar en Madrid.

Angelucho consiguió reunir a algunos de los primeros espadas de la comunidad hacker y del mundo de la seguridad informática —personajes tan emblemáticos e influyentes como el propio Israel Córdoba, Chema Alonso, Román Ramírez, Juan Garrido, Juan Antonio Calles, Pablo González, Lorenzo Martínez o la entrañable Blanca Tulleuda, impecable ilustradora del espíritu de X1Red+Segura—. De forma absolutamente altruista, todos ellos regalan sus profundos conocimientos a los usuarios que nos arrojamos como kamikazes a las autopistas de la red, sin abrocharnos el cinturón, sin airbag, sin haber pasado la ITV, y conduciendo demasiado rápido, las más de las veces, en plena noche y con los faros apagados.

Cuando oí hablar de ellos supe que tenía delante algo que era mucho más que un libro y que un blog en internet. Era una de esas utopías por las que merece la pena luchar. Debía conocerlos más de cerca…

X1Red+Segura

En noviembre de 2005, la II Cumbre Mundial de la Sociedad de la Información celebrada en Túnez aprobó proponer a la Asamblea General de Naciones Unidas la designación del 17 de mayo como Día Mundial de las Telecomunicaciones y de la Sociedad de la Información. En el artículo 121 del documento de conclusiones de dicha cumbre se afirma que:

> Es necesario contribuir a que se conozca mejor internet para que se convierta en un recurso mundial verdaderamente accesible al público. Hacemos un llamamiento para que la AGNU declare el 17 de mayo Día Mundial de la Sociedad de la Información, que se celebrará anualmente y servirá para dar a conocer mejor la importancia que tiene este recurso mundial en las cuestiones que se tratan en la Cumbre, en especial, las posibilidades que puede ofrecer el uso de las TIC a las sociedades y economías, y las diferentes formas de colmar la brecha digital.

Y el 17 de mayo de 2014, coincidiendo con el Día Internacional de Internet, las II Jornadas de X1Red+Segura volvieron pisando fuerte. La inauguración corrió a cargo de don Arsenio Fernández de Mesa, director general de la Guardia Civil, y la primera conferencia fue impartida por el comandante Óscar de la Cruz, jefe del Grupo de Delitos Telemáticos de la Benemérita, que ya había participado en las primeras jornadas y al que volvería a encontrarme en las terceras, un año después. El apoyo de la Guardia Civil a estas actividades era incuestionable.

X1Red+Segura consiguió, año a año, hacerse un sitio en las conferencias de la comunidad hacker española más influyentes: CoreTeam, Navaja Negra, RootedCON, CyberCamp, No cON Name, Hackron, ConectaCon… Pero, desde mi humilde experiencia, algo la diferencia de todas las demás: el ambiente que se respira en X1Red+Segura es más cercano, más entrañable, más familiar, que el frenético vaivén de hackers, informáticos, consultores de seguridad, exposiciones de vulnerabilidades, publicación de *papers*, o los talleres de *exploit, pentesting*, ingeniería inversa o forense que se vive en las grandes convenciones como RootedCON o CyberCamp, mucho más multitudinarias.

En el primer libro de su *República,* y citando a su maestro Sócrates, Platón sentenció: «El inteligente es sabio, el sabio es bueno». Yo siempre he pensado, como Hemingway, que la gente buena es más feliz, y también más inteligente. Porque la bondad es por naturaleza, y a largo plazo, la opción más inteligente, mientras que la maldad funciona a corto plazo, y es por naturaleza estúpida.

Supongo que por esa razón los cerebros mejor amueblados del hacking ético español acuden a la cita, siempre de forma desinteresada, en cuanto Angelucho los invita. Ninguno deja escapar la oportunidad de echar una mano a crear una red más segura para los usuarios más vulnerables. Esos que no usábamos antivirus, ni actualizábamos el sistema, ni protegíamos nuestro tráfico con VPN… Ignorantes digitales como yo cuando comencé esta investigación.

Alrededor de Angelucho no solo me encontré algunos de los mejores expertos del país en seguridad informática, sino una gran familia. Y personajes, tan cercanos y entrañables, como Longinos Recuero Ortega (@LonginosRecuero), un exempleado de Correos que descubrió internet tarde, y se ha convertido en un ciberabuelo ejemplar. O David Insonusvita (@insonusvita), un héroe digital que pone banda sonora a X1Red+Segura con su prosa. Las rimas duras y directas de su disco *Algo diferente*, fueron dulcificadas para una serie de raps que acompañan desde su fundación las jornadas. Es necesario también mencionar a Josep Albors, director de Comunicación de Ontiner.Com y responsable, entre otras funciones, de las charlas de concienciación en centros escolares. Está en X1Red+Segura casi desde el principio, como conferenciante, patrocinador y organizador, junto con Fernando de la Cuadra. Y sobre todo a Juan Antonio Calles, editor de Flu Project, y emprendedor. Fundó la empresa Zink Security tras su paso como responsable del departamento de Hacking Ético de Everis, y actualmente trabaja como Senior Manager - Cyber Security en KPMG. Yo he asistido a sus conferencias y talleres en otros eventos, y puedo dar fe de sus asombrosos conocimientos.

Hay que tener las cosas muy claras para hacer fácil lo difícil. Y que lo lograban quedaba claro en las conferencias de sus jornadas. Los ponentes sabían que no estaban hablando para otros hackers, sino para usuarios que no necesitaban comprender los principios técnicos de un ataque de DoS, ni de la explotación de una *botnet*, ni del funcionamiento de una vulnerabilidad de día cero. Lo que necesitábamos era aprender a proteger nuestra red wifi, a limpiar los navegadores, a evitar los virus y troyanos, a actualizar las aplicaciones de nuestro equipo… Y sobre todo a navegar con sentido común. Y eso mismo ocurría en los talleres, más allá de las conferencias: talleres verdaderamente fascinantes para padres, para educadores, para niños, para «ciberabuelos», para discapacitados (muy capaces), para empresarios, para internautas de base… Todos los espectros sociales entran en su órbita.

También en 2014 prestigiosas empresas del sector, como Aiuken o Buguroo, volvieron a patrocinar las conferencias. Y también ese año Israel Córdoba participó en una de ellas con el sugerente título de: «Lo que pasa en las Vegas… en internet también».

En ella trataba de concienciar a los usuarios de que todo lo que sube a la red permanece en la red. Para siempre. Aquella foto con los compañeros del insti, abrazados a las litronas de calimocho, celebrando el final de curso. Aquel vídeo, haciendo un calvo, dedicado al jefe tirano. Aquel tuit replicando un chiste subido de tono, y de cuestionable buen gusto… Israel intentaba concienciar a los usuarios, especialmente a los más jóvenes, de que cinco o diez años más tarde, cuando el responsable de recursos humanos de la empresa en la que buscamos trabajo analice nuestro perfil digital, sin duda buscará ese tipo de «manchas» en nuestro historial de Facebook o Twitter, y algo tan ingenuo como absurdo podrá convertirse en la causa

de que perdamos ese empleo.

Hay ejemplos de sobra. Sin ir más lejos, un año más tarde a Guillermo Zapata le costarían su concejalía en el Ayuntamiento de Madrid unos chistes publicados en su Twitter cuatro años antes.

Y Zapata no fue el primero ni el último que perdió un trabajo por una estupidez subida a una red social. En diciembre de 2013 Justine Sacco tuiteó, justo mientras embarcaba en Nueva York en su vuelo rumbo a Sudáfrica: «Me voy a África. Espero no pillar el sida. Es broma ¡Soy blanca!». La broma le costó el puesto como directora de comunicación de InterActiveCorp (IAC), compañía que gestiona la comunicación de portales como Ask o Vimeo. En cuanto el avión tomó tierra, ya estaba despedida. [39]

En su primer día de trabajo Kaitlyn Wells colgó un comentario en su perfil de Facebook: «Empiezo un nuevo trabajo pero la verdad es que odio trabajar en guarderías… Odio estar rodeada de niños». Duró veinticuatro horas. A la mañana siguiente fue despedida. Sus jefes habían visitado su Facebook.[40]

Lindsey Stone se hizo una foto haciendo una peineta y simulando que gritaba junto al cartel «Silencio y respeto» del histórico cementerio militar de Arlington (Virginia, EE.UU.) y la subió a su Facebook. No solo perdió su trabajo en la ONG de ayuda a adultos con dificultades de aprendizaje donde trabajaba, sino que tuvo que mudarse de casa.[41]

En Halloween de 2013 a Alicia Ann Lynch le pareció una buena idea disfrazarse de víctima del atentado de Boston, hacerse una foto y subirla a Twitter. Además de perder su trabajo tuvo que sufrir un feroz acoso en la red.[42]

Son solo algunos de los casos recogidos por el periodista norteamericano Jon Ronson en su libro *So You´ve Been Publicity Shamed*, en el que recopila los testimonios de personas cuya vida quedó destruida a raíz de un estúpido comentario en internet, y sirve al mismo propósito que la conferencia de Israel Córdoba. Un mensaje clarísimo. Piensa dos veces lo que vas a colgar en tu red social, porque no estará solo a la vista de tus amigos. Y lo estará para siempre.

Esa charla sacudió a los oyentes. Y es que ese es el espíritu de X1Red+Segura: alertar a los usuarios sin conocimientos técnicos de todos los riesgos que entraña la red, como tú o yo, como nuestros abuelos, padres o nuestros hijos más pequeños. Ese pozo sin fondo de conocimiento, ocio e información que, como todos los pozos oscuros, es mejor explorar armado con una linterna y una radio para pedir auxilio en caso de extraviarnos.

De X1Red+Segura me llevé el decálogo básico para una navegación segura e inmediatamente se lo hice leer a mi madre y a todos mis amigos. Lo redactó Angelucho hace tiempo, pero sigue estando del todo vigente.[43]

DIEZ MANDAMIENTOS PARA UNA NAVEGACIÓN SEGURA:

1. Utiliza un antivirus de confianza, no de los que se descargan de cualquier página web (los hay

incluso gratuitos y muy efectivos), y sobre todo ten en cuenta la importancia de tenerlo actualizado, los virus van apareciendo y los antivirus necesitan estas actualizaciones para desempeñar su función.

2. Mantén actualizados los sistemas operativos de tus ordenadores así como los programas más sensibles de infección o propicios para facilitar la entrada a tus equipos por nuevas vulnerabilidades detectadas y que no han sido actualizadas.
3. No bajes la guardia y pienses que al tener instalado un antivirus o actualizado el sistema operativo estás exento de ser víctima de cualquier ataque. Los virus realmente son peligrosos en su «nacimiento» cuando todavía no han sido detectadas las «puertas falsas» por donde entran en nuestros equipos (vulnerabilidades aún desconocidas), ni el *malware* catalogado por las compañías de seguridad informática. A esto se le denomina ataque del día cero (0Day).
4. Si tus conocimientos no son demasiado apropiados para poder apreciar un ataque por algún tipo de *malware,* deberías utilizar una cuenta de usuario con permisos restringidos, evitando usar la cuenta de administrador que utilizamos por defecto en nuestros ordenadores; de esa manera evitarás que estos virus modifiquen o manipulen tu ordenador.
5. Elige contraseñas seguras y distintas para cada uno de los servicios de internet que utilices.
6. Usa el sentido común y no hagas *clic* en cualquier «cosa» que veas en la red.
7. Desconfía de los enlaces o descargas que aparecen en páginas web de poca confianza o correos electrónicos enviados por desconocidos.
8. Nunca abras mensajes de usuarios desconocidos o que no se hayan solicitado, elimínalos directamente y no contestes en ningún caso a estos mensajes.
9. No hagas operaciones bancarias desde ordenadores que no sean de tu confianza, como los de los cibercafés, o utilizando conexiones wifis que no controles. Lo ideal sería utilizar un ordenador específico para «operaciones sensibles» en la red y no mezclar la navegación de ocio.
10. Sé muy cauteloso con la información que decides compartir en la red, y con quién la compartes, porque internet es como Las Vegas: lo que se sube a internet queda en internet. Por supuesto, solo se debe aceptar como amigo a gente conocida, tanto en los clientes de mensajería instantánea como en redes sociales.

Mientras escuchaba las conferencias y tomaba notas como un poseído, me preguntaba cómo era posible que una iniciativa tan fantástica, útil, urgente y necesaria, no recibiese más apoyo del Ayuntamiento, la Comunidad de Madrid o el Gobierno de España. En un momento histórico en que toda nuestra vida circula por la red, en que los niños crecen utilizando videojuegos, teléfonos móviles y tablets, en que nuestros padres y abuelos se ven forzados a descubrir el WhatsApp, el correo electrónico y Facebook, nos hemos convertido en la generación más informada de la historia… pero también en la más vulnerable.

Este decálogo de una navegación segura, redactado por el guardia civil del GDT de la UCO, no es un chaleco antibalas que te garantice sobrevivir a un proyectil de teflón, pero te protegerá del 9 mm, que es el más habitual.

Por desgracia, cuando te enfrentas a tipos con un perfil como el de MarkoSS88 necesitas mucho más que eso. Aunque yo ni siquiera lo sospechaba todavía…

ABRIL-AGOSTO DE 2014
PROPAGANDA FASCISTA EN LA RED

«Estamos convencidos de que la gente necesita y requiere esta fe. Por lo tanto hemos llevado a cabo la lucha contra el movimiento ateo, y esto no solo con unas pocas declaraciones teóricas: lo hemos aplastado.»

Adolf Hitler, discurso en Berlín, 24 de octubre de 1933

Buenas tardes, Salas, te escribo porque me acaba de decir la chica que ya ha recibido los libros: *El palestino, Diario de un skin* y *El año que trafiqué con mujeres,* mañana mismo voy a recogerlos y a empezar a leer. Muchas gracias.

Aquel breve email de MarkoSS88 era una buena noticia. Había enviado el paquete con los libros a través de un servicio de mensajería, pero no tenía garantías de que la dirección que me había dado fuese real. Y por precaución, Markos no me había dado los apellidos de su amiga, así que el paquete iba a nombre de «Srta. Stefy».

La identidad de su amiga tuve que averiguarla yo: Estefanía C. era una joven vinculada a UltraSSur, con perfiles activos en Twitter, Facebook, y demás, directamente relacionados con otros viejos camaradas de la comunidad NS. Por suerte, es una de esas chicas que vuelcan toda su vida en la red, para que cualquiera, como yo, pueda investigarla… En las fotos de su perfil aparece menuda, casi frágil, con un rostro angelical, que nadie imaginaría infectado por la ideología ultra. Estefanía perdió a su madre siendo solo una niña, y ahora vivía sola con su padre en aquella dirección, así que el paquete probablemente llegaría a su destino. Pero eso tampoco me garantizaba que Markos me respondiese. Contesté su email de inmediato:

Es muy importante, Markos, que tengas algo claro. Lo que vas a leer es mi experiencia personal…

Lo que ocurrió a continuación fue una sorpresa incluso para mí. En realidad, yo no sabía nada de MarkoSS88. Solo presté atención a sus mensajes cuando amenazó a los alumnos de la URJC por mi culpa. Así que entré a visitar su blog y descubrí una entrada íntegramente dedicada a una de las muchas identidades que me atribuían en la red. Una de las muchas que llevaban meses replicándose en la red y cuyo origen conocía bien.

No hacía mucho, en enero, una lectora me envió un email para avisarme de que un tal Sebastián Yanguas hablaba de mí en un foro y había enlazado un artículo delirante extraído de un blog de puteros, en el que se me

identificaba, siguiendo las teorías del Chino Carías, con un agente de los servicios de Inteligencia, que además había «traicionado a su género» al condenar la prostitución, y a todos los hombres que la consumen:

> Salas es apenas un pseudonimo de un sujeto oculto que por lo que se sabe es un agente de los servicios de inteligencia, relacionado con los secuestros y desapariciones de mujeres y niños de manera forzada, cuya misión es a través de libros difamatorios encubrir las verdaderas causas de sus desapariciones, y culpar de todo a los hombres normales que pagan por sexo. Es un terrorista, farsante y traidor de su propio sexo, y por mas que sea un agente secreto su final sera de terror. Porque la traición se paga con sangre.[44] *(sic)*

Sebastián Yanguas cogía el relevo del argumento en el foro, aumentando la apuesta con una serie de afirmaciones tan audaces y contundentes, que cualquiera podría suponer que manejaba una información privilegiada. Lo inquietante no era la sarta de estupideces que soltaban los foreros, sino que el avatar que Sebastián Yanguas utilizaba era el símbolo de ETA, y después del revuelo que había generado en los medios nacionales la publicación de mis imágenes de Arturo Cubillas, el presunto jefe de ETA en Venezuela, el tema era como para preocuparse.

Al poco, el 13 de febrero, Yanguas se coló en mi Facebook para dejar en mi muro un enlace a un delirante y extenso artículo titulado: «La verdadera identidad de Antonio Salas y sus vínculos con los servicios secretos».

No contento con eso, se permitía dirigirme un mensaje a través de Facebook, uniéndose a la condena de muerte de los tupamaros. Este es, literal, el primer mensaje que recibí del tipo que se identificaba con el logotipo de ETA:

> Hola Antonio.

Un sujeto llamado Mario Velezques te menciono en su articulo. Dijo que sos un agente de servicios secretos, pero ademas que sos un terrorista que esta relacionado con los secuestros y desapariciones de mujeres y niños, cuya desaparición la justificas con la escusa de la trata de personas. Y que la vez culpas a todos los hombres inocentes que pagan pro sexo de su desaparición, cuanto tu mismo es el causante.

Por lo tanto te condeno a muerte por terrorismo y traición a tu propio sexo…

Le di bastantes vueltas, lo hablé con David Madrid y el resto de policías, y al final —y contra su consejo—, terminé escribiendo a Yanguas para convencerlo de su error. No solo sobre mi identidad, que es lo de menos, sino sobre su escepticismo en torno a la trata de mujeres y a su defensa de la prostitución como un trabajo lícito, y así comenzó un intercambio de emails con el admirador de ETA. Pero todo fue absolutamente inútil. No daré publicidad a su blog, pero diré que Yanguas aseguraba que no existía «ni una mujer traficada», que «todas practican la prostitución de forma libre y voluntaria» y que las chicas que aparecían en mi reportaje «son actrices».

Las afirmaciones de Yanguas sobre mi identidad, y las motivaciones de mi trabajo, comenzaron a extenderse por la red, como un reguero de pólvora. Y pronto otros puteros, simpatizantes de ETA, o simples internautas, comenzaron a replicar en sus respectivos muros de Facebook o Twitter sus absurdos argumentos. De esta forma yo podía asistir, perplejo, al torrente de estúpidas conjeturas que los usuarios hacían sobre mi supuesta relación con los servicios secretos, mi «identidad real» y mi implicación en el negocio de la prostitución, con profusión de fotos y vídeos del «verdadero Antonio Salas», para justificar la campaña «no compres sus libros, aquí los tienes gratis».

Al margen de la malévola intención, si realmente yo fuese el agente secreto que denunciaba Yanguas, o como afirmaba el Chino Carías en un intento de desacreditar mi trabajo ante las cámaras de la CNN, o cualquiera de las otras identidades falsas que me han atribuido ellos y otros tantos… ¿Cambiaría en algo el peso de las evidencias? ¿Dejarían los ultras de Hammerskin de ser nazis? ¿Rebajaría la contundencia de las confesiones que había hecho el Chino ante mi cámara, reconociendo asesinatos y torturas? ¿Desaparecerían las niñas mexicanas que pude comprar a Mario Torres? ¿ETA nunca habría estado en Venezuela?

De hecho, debería estar agradecido a gente como el Chino Carías, Markos o Yanguas, por «desenmascarar mi identidad real» en la red, aunque cada uno escoja una distinta. Sus desvaríos me han permitido continuar todos estos años trabajando como periodista encubierto. Sebastián Yanguas y MarkoSS88 aparecieron en mi vida prácticamente a la vez. Los dos me habían condenado a muerte. Los dos afirmaban haber descubierto mi «identidad real». Los dos dedicaron horas y horas de sus vidas a acosarme, insultarme y difamarme en la red. Y con los dos intenté dialogar, durante

meses, para convencerlos de su error. No tardé demasiado en concluir que Sebastián Yanguas era un trol, un usuario que publica mensajes provocadores con la intención de molestar y provocar una respuesta emocional en otros usuarios. Lo de Markos no lo tenía tan claro.

Aparte de otra supuesta «identidad real de Antonio Salas», en su blog me encontré con que MarkoSS88 había liderado la redacción de un libro dirigido a los «jóvenes cachorros» del movimiento nazi hispanohablante, para instruirlos en el pensamiento NS.

> … tengo uno en conjunto con unos camaradas, el cual puse a la venta bajo mi nombre con su permiso para recaudar dinero para la asociación NSSC, el de blog, destinado a proyectos para familias que no tienen apenas ni para comer, fue un trabajo muy difícil y había mucho que hacer en poco tiempo, recoge la ideología NS desde tiempos muy pasados, *¿Qué es el Nacional Socialismo? Un trabajo de dedicación y entrega;* lo subimos a la biblioteca virtual también porque me negaba a que se pagara por un libro cuando tenemos unos 150 libros subidos *online,* no era justo.

MarkoSS88 ya no solo era un nick anónimo en internet. En su perfil de Facebook aparecían muchas fotos suyas y su nombre completo: Marcos Santos Navarro.

Ya no se trataba solo de un nazi que había llegado a amenazar a los organizadores de un evento universitario, solo por haberme invitado al mismo. Ni siquiera era simplemente el bloguero responsable de uno de los miles de *sites* que pueblan la comunidad neonazi en la red. Markos se presentaba como un ideólogo. Un formador. El responsable de un libro doctrinal —con ISBN: 9781291686098— dirigido a los jóvenes y adolescentes que llegaban al movimiento NS, y que además tenía inquietudes sociales, en tanto que destinaba los ingresos del libro «a proyectos para familias que no tienen apenas ni para comer». Su gesto, donar los derechos del libro a un centro social, me pareció encomiable.

De hecho, en sus emails, MarkoSS88 me dejaba creer que era uno de los impulsores del proyecto de los Hogares Sociales Patriotas, que acapararon la atención de la prensa nacional ese año. Tanto en su muro de Facebook como en su blog en varias ocasiones habló de las «casas okupas nazis».

Y es que en agosto de 2014 un grupo de jóvenes nacionalistas decidió aplicar la estrategia de sus odiados enemigos de la izquierda, okupando un edificio antiguo para convertirlo en un centro social. La técnica de la «okupación» hasta ese momento era exclusiva de los grupos antisistema, anarquistas y antifascistas, y por primera vez un colectivo de extrema derecha hacía lo mismo en España.

El Hogar Social Ramiro Ledesma se estableció en un antiguo edificio

abandonado que había sido propiedad de la presunta mafia china de Gao Ping, en el cruce de las calles Juan de Olías con Lérida, en pleno barrio de Tetuán. Un barrio repleto de emigración latina y magrebí, que conozco bien porque siguiendo Lérida, y a solo cinco calles, en Anastasio Herrero 7, se erige la gran mezquita de Abu Bakr que en su día frecuentaba Mustafá Setmarian, y en la que yo pasé tantos viernes, mientras intentaba recomponer la historia de Setmarian antes de viajar a Siria tras sus pasos… De hecho, *El Palestino* arranca justo en esa mezquita.

El Hogar Social Ramiro Ledesma, vinculado al Movimiento Social Republicano, no prestaba ayuda a los «moros» de la mezquita, pero al menos de sus ventanas ondeaban banderas palestinas, en solidaridad con las víctimas de la ocupación israelí… Una de las paradojas de los grupos de extrema derecha.

Puedo imaginar la situación, si un palestino se hubiese presentado en el centro social en busca de algo que comer…

—Tengo hambre, necesito ayuda.

—Moromierda, esto es para los españoles, vuélvete a tu país.

—Camarada, ¿no ves que es palestino? Su país está ocupado por las hordas sionistas opresoras.

—Tienes razón, camarada, putos judíos. Bueno, moromierda, pues muérete por ahí sin hacer mucho ruido. Eso sí, nos solidarizamos profundamente con tu causa: ¡Palestina libre! El siguiente…

La apertura del primer centro «okupa» de extrema derecha en España levantó gran alarma social. Y a pesar de que los vecinos españoles que se beneficiaban de las ayudas estaban encantados, la presión mediática terminó por volverse en su contra. Cristina Cifuentes decidió el desalojo inmediato del Hogar Social Ramiro Ledesma a pesar de que a pocos metros existía otro centro social «okupa» de extrema izquierda, que no fue desalojado. Aun así, los «patriotas solidarios» no cejaron en su empeño, y tomaron un nuevo edificio, unas antiguas oficinas del Ministerio de Trabajo en la calle Bretón Hierro, de donde también serían desalojados, para trasladarse a un nuevo lugar…

> Sobre la casa okupa [me escribía Markos] nos encontramos denuncias falsas de agresión, kilos de comidas que se quedaron dentro de HSM, la policía no permitió que esos kilos se recuperaran. Por otra parte, decir que no todos los que estaban en esa casa eran nazis, es verdad que solo se daba refugio y comida a personas españolas mostrando el DNI, pero en ningún momento se les comentaba que era un reparto de comida solo para los de nuestra ideología. HSM, como muchos de los hogares sociales que ayudan a españoles, se creó por el hecho de que había hogares y comedores sociales únicamente para inmigrantes, debido a eso, se crearon estos hogares sociales, que muchos de ellos los están cerrando y desalojando por ser «racista». No entiendo por qué nuestros hogares sí, y solo los que ayudan a inmigrantes no, o todos o ninguno; nosotros empezamos a hacer una página por Facebook «Hoy por ellos mañana por ti» para que la gente conociera puntos y grupos de gente que podrían ofrecer

ayudas o para que colaboren con ellos y ayuden a las familias.

Puede que algún lector se sienta sorprendido por el trabajo social de los neonazis… No es mi caso. Durante mi infiltración, y ese fue uno de los descubrimientos más estimulantes, conocí a los activistas skinhead movilizados contra las corridas de toros, o que organizaban conciertos de música «patriótica» contra las drogas, o que trabajaban como voluntarios en asilos de ancianos (ancianos españoles, claro), o que viajaron a las playas de Galicia para recoger el chapapote tras el desastre del *Prestige…* Porque, no me cansaré de repetirlo, incluso las personas más violentas, agresivas y peligrosas hacen lo que hacen porque creen que es lo correcto. Y eso suele implicar la solidaridad con quienes consideran iguales.

A pesar de ello, Markos no reculaba ni un milímetro en sus argumentos a favor del uso de la violencia o el racismo.

> Si nosotros no tenemos problemas en ayudar a los demás, a inmigrantes, a gente de fuera, vamos, pero primero los de aquí, y cuando sobre, a los demás, claro. Si es que la gente está confundida, no pegamos a inmigrantes todos los días ni los acosamos, a ver… a latin, a DDP, a ñetas… a esas bandas claro que sí y yo te digo directamente que voy a por ellos, no van a aterrorizar a los míos, nuestro problema con inmigrantes viene a que el gobierno deja que sus culturas se impongan a las nuestras o que porque trabaja por menos dinero sea contratado antes que un español. Si se quedaran en su país, nosotros no iríamos a atacarlos.

No, la afirmación de Markos no me pillaba por sorpresa, pero confería mayor interés a mi objetivo. Si era capaz de convencer a aquel violento y agresivo NS, un ideólogo capaz de escribir un libro y de adoctrinar a los jóvenes cachorros del movimiento, el efecto podía ser contagioso entre sus seguidores. Estaba seguro de que si Markos lo dejaba, otros jóvenes skins seguirían su ejemplo. Así que me congratulé de mi decisión. Había merecido la pena cada minuto invertido, y cada libro que le había enviado. Ahora me tocaba a mí buscar el suyo y contribuir con su compra a esos proyectos solidarios. Nazis, pero solidarios.

No fue difícil. El libro *¿Qué es el Nacional Socialismo? Un trabajo de dedicación y entrega,* firmado por MarkoSS88, se encuentra en diferentes plataformas de venta *online* como dropbox.com, lulu.com o books.google. Así que me hice con un ejemplar dispuesto a leerlo. Quería comprender mejor a Markos para tratar de convencerlo de que el camino del odio nunca es un camino. Pero la lectura iba a resultar áspera…

Diez capítulos repartidos en 161 páginas que probablemente causarían sorpresa, incluso irritación, en cualquier lector mínimamente familiarizado con la historia, pero que resultan redundantes a todo estudioso conocedor del hitlerismo esotérico, y su tendenciosa, sesgada y subjetiva forma de reescribir esa historia.

Esto era bueno. Yo conocía perfectamente esa línea del ideario nacionalsocialista, e incluso había entrevistado para *Diario de un skin* al diplomático y escritor chileno Miguel Serrano, una de las plumas más influyentes en la propaganda del hitlerismo. Tenía argumentos para establecer el debate con Markos, en mi firme propósito por alejarlo del NS. Así que decidí escribirle para iniciar el ataque ahora que entendía mejor su pensamiento. Sabía que para él, como para muchos jóvenes skin, Adolf Hitler no era solo un referente militar, filosófico o político. Era una especie de Mesías. Y Markos pretendía que otros jóvenes hispanoparlantes, a los que él mismo se refería como «mis cachorros», aceptasen esa devoción al Führer como el referente en sus vidas. En el fondo, Markos hacía exactamente lo mismo que los grupos que considera sus enemigos naturales: antifascistas, latinos, yihadistas… utilizar la red como un altavoz para su propaganda.

Yo intentaría que abriese los ojos, y que se los hiciese abrir a sus cachorros. Me sentía con ánimo y con argumentos. Pero algo iba mal. De pronto, después de varios meses de un intercambio fluido de correos, Markos no respondía a mis emails. Ni tampoco a los mensajes en Facebook.

Tampoco actualizaba su blog.

De repente, MarkoSS88 había desaparecido…

Capítulo 5
El yihad informático

«Un caballero no puede pegar a una mujer… ni siquiera con una flor.»

Proverbio árabe

«El mejor de los hombres es aquel que hace más bien a sus semejantes.»

Profeta Muhammad (saas), hadiz citado por Ibn Hazm

en el epílogo de *El collar de la paloma*

El día que Boko Haram descubrió internet

El 17 de mayo de 2014 los titulares de prensa no se hicieron eco del magnífico evento organizado por X1Red+Segura. Y apenas recordaron que celebrábamos el Día Mundial de Internet. En París, el presidente francés François Holland había convocado una cumbre con sus homólogos de Nigeria, Níger, Chad, Togo y Benin, además del ministro británico de Exteriores, William Hague; el presidente del Consejo Europeo, Herman van Rompuy, y la subsecretaria adjunta de Asuntos Políticos de Estados Unidos, Wendy Sherman.

El objeto de aquella reunión internacional era tomar medidas urgentes y enérgicas contra Boko Haram, la última piara de psicópatas que había descubierto el poder de internet… El titular de *El País:* «Nigeria y sus cuatro países vecinos declaran la guerra a Boko Haram», refleja perfectamente lo que ocurrió aquel sábado en la capital francesa.[45]

Se había cumplido un mes del secuestro de doscientas niñas en un colegio femenino de Chibok, una pequeña población de Borno, al nordeste en Nigeria, y una campaña internacional de apoyo a las víctimas intentaba presionar al Gobierno nigeriano para que se pusiese las pilas con el caso. El Gobierno liderado por el presidente Goodluck Jonathan se vio impotente para solucionar el drama que había conmocionado a la opinión pública internacional, y pidió ayuda para poner freno a la organización de crimen organizado Boko Haram. (En la lengua hausa, una de las 520 que se hablan en el país, *Boko Haram* se traduce como «la pretenciosidad es anatema»; en los medios occidentales ha sido traducido de manera tendenciosa como «la educación occidental es pecado».)

El secuestro de las niñas de Chibok realmente conmocionó a la opinión pública internacional cuando, a principios de mayo de 2014, el líder de Boko Haram, Abubakar Shekau (alias Darul Tawhid), mandó un mensaje al mundo a través de la red. En un vídeo en el que aparecía rodeado de las doscientas pequeñas secuestradas, vestidas con el tradicional *khimar,* anunciaba que todas se habían convertido al islam, y que serían entregadas como esposas a sus combatientes o vendidas como esclavas sexuales.

Shekau, que acababa de descubrir el poder de la propaganda en internet, aseguraba hablar por boca del profeta Muhammad. Una blasfemia comparable a las vertidas por el líder del Ku Klux Klan Frazier Glenn Miller, cuando violaba, masacraba o quemaba vivos a negros y judíos, «en el nombre de la Sagrada Biblia».[46] Estoy seguro de que hasta el lector más obtuso coincidirá conmigo en que ni Frazier Glenn Miller, ni ninguno de los «Magos Imperiales» del KKK, ni de ninguna otra organización violenta que se autoproclaman cristianos tienen la menor legitimidad para representar a la religión cristiana. Pues este mismo argumento puede y debe aplicarse a todos los terroristas, como Abubakar Shekau, que toman el nombre

de Allah en vano. Tan en vano como Miller pronunciaba el nombre de Jesús.

El vídeo de las niñas de Chibok ataviadas con *khimar* se convirtió en *trending topic* en pocos minutos, extendiéndose por las redes sociales como un virus. En solo unas horas todo el planeta conocía el rostro de Abubakar Shekau. Aquel miserable delincuente, paleto y desalmado, que afirmaba hablar en nombre del profeta del islam, había conseguido lo que quería: ser tan famoso y temido como Ben Laden. Y todos nosotros, los usuarios de la red, fuimos en cierta manera sus cómplices cada vez que retuiteamos los vídeos con sus delirantes discursos; cada vez que comentamos las noticias con sus crímenes en nuestro perfil; cada vez que obsequiamos un «me gusta» a cada referencia sobre su organización en Facebook.

Boko Haram había descubierto que una imagen impactante vale más que mil balas. Porque con todos sus atentados anteriores no había conseguido el protagonismo mediático internacional que obtuvo con aquellos instantes de vídeo, rodeado por las doscientas niñas de Chibok. Ahora ya lo sabían. En la era de la tecnología, el terrorismo no puede nutrirse solo con sangre. Necesitan algo más. Necesitan que les demos vida en internet. Nos necesitan a nosotros. Boko Haram lo descubrió entonces, pero antes del siguiente Ramadán otro nuevo monstruo sin precedentes en la historia surgiría en la red. Un engendro tan blasfemo como Boko Haram pero con recursos, experiencia y voluntad infinitamente superiores. Y dispuestos a utilizar la red, en el nombre de Allah, como jamás se había utilizado antes.

Ramadán de 1435 en El Príncipe

El noveno mes musulmán del año 1435, Ramadán, se inició el 28 de junio de 2014 en nuestro calendario occidental. Durante treinta días, más de 1.500 millones de musulmanes de todo el mundo, casi 2 millones en España, dedican una especial atención a las cuestiones espirituales, y como una prueba de fe y caridad, comparable a la penitencia o la Cuaresma de los cristianos, se mantiene el ayuno entre la salida y la puesta del sol. Los occidentales no somos muy consciente de lo que significa pasar hambre y sed, y el islam nos ofrece la posibilidad de concienciarnos, durante el noveno mes del año lunar, de lo que sienten los que nada tienen. Aunque evidentemente es una penitencia con trampa, ya que tras la puesta del sol basta con abrir el frigorífico para saciar nuestra sed y apetito, y los que de verdad viven en la pobreza no pueden disfrutar de ese privilegio.

Ramadán es una fiesta familiar. Una celebración para vivir con los vecinos, amigos y hermanos. Pero mi familia no es musulmana, así que desde hace años vivo el Ramadán a mi manera. Solo. Intentando adaptarme a las circunstancias. Durante estos años, cuando una reunión con tal o cual hacker, consultor de seguridad, o funcionario de las unidades de delitos tecnológicos de nuestras policías coincidía en pleno Ramadán, la situación era siempre la misma: nos citamos en una cafetería o un restaurante, el camarero se acerca a la mesa para tomar nota, mis interlocutores examinan la carta y piden la comanda, y después me miran con expresión de perplejidad cuando yo digo que no voy a tomar nada.

—¿Cómo que nada? Algo tendrás que comer…

Normalmente basta con una mentira piadosa.

—No, qué va, es que tengo el estómago revuelto y no me apetece nada… Quizá más tarde…

En estos casos he aprendido que es mejor zanjar así la cuestión, que tener que dar explicaciones sobre qué es el Ramadán y por qué no como ni bebo nada en esos días. Y estoy seguro de que algunos personajes relevantes de la comunidad hacker española —como Román Ramírez, David Pérez o Lucas— sonreirán al leer estas líneas, porque recordarán nuestro primer encuentro, y mi extraño comportamiento inicial. Esta es la explicación. Por lo general me limito a pedir una botella de agua, preferentemente en envase plástico, que no tocaré durante la reunión, y que terminará apilada en el maletero del coche, o en la maleta de la moto, con docenas de botellas similares. Desde hace años se repite la misma escena. Termino el Ramadán con el maletero lleno de botellines.

Acababa de concertar una de esas reuniones durante el Ramadán de 2014 cuando leí un siniestro titular en la prensa internacional. El 29 de junio de ese año, el portavoz del Estado Islámico de Irak y el Levante, Abu Mohamed al-Adnani, declaró la intención del grupo de crear un califato que se extendiera por todo el mundo musulmán, al tiempo que nombraba a Abu Bakr al-Baghdadi su máxima autoridad,

autoproclamado «Ibrahim, imán y califa de todos los musulmanes». *Habemus Papam.*

¿De dónde procedía esta inmensa expansión del Estado Islámico? ¿Cómo estaba logrando fortalecerse paso tras paso? ¿Y qué papel jugaba internet en el proceso?

Mi helicóptero despegó desde el helipuerto de Algeciras a primera hora de la mañana. Escogí el mejor asiento, estratégicamente situado cerca de la ventanilla. Quería grabar todo el viaje y tenía la esperanza de poder realizar unos planos aéreos de mi objetivo: el barrio de El Príncipe, antes de aterrizar en Ceuta.

Empecé a grabar en el despegue. No quería perder ni un plano. El día era despejado y las condiciones de vuelo inmejorables, así que era optimista.

Durante todo el trayecto sobre el estrecho de Gibraltar pude tomar unas imágenes estupendas. El piloto del helicóptero mantenía una altitud de crucero perfecta para disfrutar de unas vistas excelentes. Y mientras sobrevolábamos los abundantes cargueros y ferris que transitan diariamente el estrecho que comunica el Mediterráneo con el Atlántico, sentía que si forzaba el zoom de la cámara, casi podría identificar a la tripulación de cada barco. Sin embargo, durante aquel vuelo no pude evitar recordar a Susy, a Edith, a Loveth, y a tantas y tantas mujeres traficadas que conocí durante mi investigación de la trata de blancas, y que habían cruzado aquellas aguas hacinadas en una patera, jugándose la vida a bordo de un infecto cayuco, después de haber pasado el infierno de atravesar a pie medio continente africano en busca del sueño europeo. En unas circunstancias muy diferentes, y en una dirección contraria, al viaje que yo estaba realizando.

No hubo suerte. En cuanto avistamos Ceuta me di cuenta de que la advertencia que me había hecho el inspector Ángel era tan precisa como siempre: «No te hagas ilusiones, Ceuta suele amanecer totalmente cubierta por la niebla, así que desde el helicóptero probablemente no podrás grabar nada».

Ceuta, como Melilla, son un ejemplo de convivencia en armonía entre cristianos y musulmanes. Y más en Ramadán. Al volante del primer taxi que tomé iba un español, cristiano, que sin embargo hacía el ayuno del Ramadán como sus amigos musulmanes. Me fascinó.

—No, no, yo no soy musulmán, soy católico, apostólico y romano. Pero, mire usted, tengo muchos compañeros musulmanes, y cuando me explicaron lo del ayuno, la verdad es que me pareció una cosa buena. Empecé hace ya años por curiosidad, y por respeto hacia ellos. En este oficio nos pasamos mucho tiempo en la parada, y me parecía un poco… no sé cómo decirle… No me parecía bien estar bebiendo o comiendo delante de ellos, mientras me miraban sin comer ni beber nada. Así que decidí que pasaría con ellos el ayuno. Yo soy devoto de la Virgen del Rocío, no se confunda, y no voy a la mezquita ni ná, pero sí hago el ayuno. Y además de perder unos kilillos, que siempre viene bien, lo importante es cómo te cambia la cabeza. Ea, que dejé de fumar y todo. Porque no hay mejor cosa pá la fuerza de voluntad que hacer el ayuno… Yo se lo recomiendo a todo el mundo…

Tengo que reconocer que la anécdota me pareció entrañable. Que el primer taxi que tomaba estuviese conducido por un católico devoto de la Virgen del Rocío, que sin embargo hacía el ayuno del Ramadán musulmán, se me antojó un regalo de la Providencia. No se me ocurriría una forma más gráfica y elocuente de ilustrar la integración pacífica y armónica del islam y el cristianismo en el norte de África.

Me alojé en el mismo hotel que utilizaban los actores de la serie *El Príncipe,* de Telecinco. Y compartí chófer con el actor Juanma Lara, el subinspector Quílez en la ficción.

Ceuta, como Melilla, están llenas de policías… y de confidentes. Antes de subirme al helicóptero ya tenía un contacto. Uno de los colaboradores de los servicios de Información españoles en la comunidad musulmana del norte de África. Uno de muchos. Acostumbrado a tratar con funcionarios cristianos, que valoraban económicamente sus informaciones, cuando un común amigo le pidió que hablase conmigo, creo que no entendió bien quién era yo. Supongo que la descripción que le hicieron —«Un periodista español musulmán que ha estado en muchos países de Oriente Medio, y que habla bien de vosotros»— despertó su curiosidad. En El Príncipe, y en la comunidad hispanomusulmana del norte de África en general, no están acostumbrados a que la prensa hable bien de ellos.

Es fácil hacer una búsqueda en Google y comparar los titulares asociados al barrio de El Príncipe en los últimos años. Yihadismo, narcotráfico, inmigración ilegal… Pero El Príncipe que yo conocí, de la mano de Hakim, era muy diferente.

Los barrios de El Príncipe (Felipe y Alfonso) no me parecieron más conflictivos que Las Tres Mil Viviendas (Sevilla), las Barranquillas (Madrid), Penamoa (A Coruña), Palma Palmilla (Málaga), Cabanyal (Valencia), Mil Viviendas (Alicante), la Mina (Barcelona) o Campano (Cartagena). Lo único que diferencia la barriada ceutí, vendida en los medios de comunicación como la más peligrosa de Europa, de los otros barrios de la península considerados especialmente conflictivos es que en El Príncipe hay una mayor tasa de musulmanes. Y supongo que en los tiempos que corren eso inspira más miedo. Sin embargo, yo no tuve ningún problema. Una vez más, viajar a los lugares, en vez de conocerlos a través de Google, es la mejor vacuna contra los prejuicios.

El Príncipe en un fascinante hormiguero de callejuelas, subterráneos, plazas y «casas colgantes», que no tiene nada que envidiar, en su atractivo turístico, a los cascos antiguos de Cuenca, Toledo, Barcelona o Compostela. Desde luego, no vi brigadas de Al Qaeda patrullando las callejuelas del barrio, ni comandos del ISIS secuestrando infieles. Ni siquiera vi ningún tipo de violencia contra los cristianos, al contrario…

Según me reveló Hakim, a pesar de la terrible propaganda que los medios peninsulares lanzaban contra El Príncipe, satanizándolo como un nido de terroristas y criminales, algunas empresas de turismo como la ceutí Aerobús SKN, o la gaditana Viajes Eurocherry, habían comenzado a establecer circuitos turísticos en Ceuta que

incluían la visita guiada a El Príncipe. «Y no vienen con escoltas armados», bromeaba Hakim con cierta amargura. Primera sorpresa.

—Es una pena que no estuvieses aquí hace dos meses, para ver tú mismo la procesión de Semana Santa en El Príncipe. Desde hace por lo menos cuarenta años la imagen del Cristo de Medinaceli sale de aquí, y va en procesión hasta la sede de la hermandad de los Nazarenos, en la avenida de España, pasando por la puerta de la Mezquita de El Príncipe. Y cuando pasa por el Centro Penitenciario de Los Rosales, se libera un preso. Aquí se juntan miles de personas. Vecinos cristianos y musulmanes del barrio, la mayoría musulmanes, participan en la procesión, porque aquí se le tiene mucho cariño a este Cristo y a la Virgen de los Dolores, que también está ahí dentro… ¿A ti te parece que eso sería posible si esto fuese un foco de *mujahidin*?[47]

www.20minutos.es/noticia/360607/0/procesion/medinaceli/ceuta/

20 minutos | Portada | Nacional | Internacional | Economía | Tu ciudad | Deportes | Tecnología | Artes | Gente y TV

CEUTA

Cristianos y musulmanes participarán en el traslado del Señor de Ceuta

El Medinaceli pasa ante la mezquita del Príncipe. (J.S.)

- La talla del Medinaceli es trasladada desde la iglesia ubicada en la barriada del Príncipe.
- La población del barrio, de mayoría musulmana, participa.
- Es uno de los actos de Semana Santa más emotivos.
- CONSULTA AQUÍ MÁS NOTICIAS DE CEUTA.

C.E., 17.03.2008

Supongo que mi cara de asombro fue suficiente respuesta. No tenía ni la menor idea de que justo allí, en El Príncipe, tildado por la prensa como el mayor foco de integrismo islamista de España, musulmanes y cristianos daban una lección de convivencia y respeto religioso, compartiendo juntos la procesión de Semana Santa. Cuando Hakim me preguntó por qué los periodistas de la península no contaban este tipo de cosas, y se limitaban a dibujar una imagen tan oscura y siniestra del barrio, no supe qué responder.

Las calles de El Príncipe están llenas de pintadas y grafitis, con mensajes más o menos elocuentes. Pero nadie se había atrevido a profanar la fachada del templo cristiano. Un comportamiento mucho más respetuoso del que he visto en otros países.

Más tarde, Hakim me mostraría la gran sinagoga judía de Ceuta, que cuenta ya

con su propio espacio en la red: comunidadisraelitadeceuta.es. Y que unos meses después celebraría la primera exposición pública de la centenaria Torá que conserva en su altar. Y también el incipiente oratorio hinduista Mandhir de Durga Mata, que en aquel momento estaba ampliando sus instalaciones para convertirse, al año siguiente, en el gran Templo Hindú de Ceuta. Asimismo con un espacio web.[48] Judíos e hinduistas ceutíes también habían comprendido que, en pleno siglo XXI, Dios no solo predica en los templos. También lo hace en la red. La intención de Hakim era demostrarme que si existía un lugar en España donde el islam podía convivir pacíficamente con otras religiones, en la red y fuera de ella, era Ceuta y su Príncipe.

Durante los días que pasé en Ceuta descubrí que mis compañeros de la prensa no habían exagerado al referir los problemas de marginación, narcotráfico, paro juvenil y exclusión social que existen en El Príncipe. Pero la mayoría había obviado que existían más cosas. Cosas y personas buenas. Como NawaloBayra, de la Asociación de Vecinos; como el franciscano Luis Miguel Martell, responsable de la iglesia de San Ildefonso; como el abogado Mohamed Mustafá Madani o como los voluntarios y trabajadores del Centro Equal, o de la UTS. Ellos son la primera línea de lucha contra el yihadismo en El Príncipe. Y no empuñan *tasers*, ni porras, ni escudos antidisturbios. Empuñan palabras, argumentos, coherencia. Armas mucho más eficientes contra el virus que se extiende por Occidente, incluyendo Ceuta.

—Aquí la gente tiene muchos problemas para salir adelante. Por culpa de los periodistas, el barrio se está aislando cada vez más del resto de Ceuta. Nos miran como si todos fuésemos terroristas…

—No todo es culpa de la prensa, Hakim. Acuérdate de Rachid Hassein Mohamed. Él fue el primero en ir a hacer el yihad con armas. Eso no se lo inventaron.

—Un asesino. Es verdad. Abu Musab mató a más de cien personas. Todos musulmanes. Yo lo conocía, era taxista aquí, en la ciudad, y no era un buen musulmán. Le gustaban las discotecas, las turistas… Estaba todo el día hablando del Real Madrid y del Barça. Le gustaba más el fútbol que ir a la mezquita. Nadie podía imaginar… Pero no fue el primero.

—¿Hubo otros antes?

—Claro. Ahora ya nadie se acuerda de Hamido. A él lo secuestraron los americanos, lo llevaron a Guantánamo, lo torturaron. Y después lo soltaron porque era inocente. Pero ¿quién le devuelve lo que le quitaron?

Ahmed Abderrahaman Ahmed, alias «Hamido», fue bautizado por la prensa como «el talibán español». En verano de 2001 viajó a Afganistán con la intención de estudiar el Corán. El 11-S le pilló allí. Capturado en la frontera con Pakistán cuando intentaba escapar de un país en guerra, fue «vendido» a las tropas de ocupación, que pagaban una buena recompensa por «terrorista». Fue trasladado a Guantánamo, donde permaneció hasta que, en febrero de 2004, el juez Baltasar Garzón consiguió su extradición a España. El Tribunal Supremo lo absolvió de todos los cargos.

—A Hamido le arruinaron la vida, y después nos lo devolvieron con una

palmadita en la espalda y un «lo siento, nos hemos equivocado». Lo mismo que ocurre constantemente en El Príncipe. Tú mira cuántas detenciones por terrorismo yihadista se han hecho en El Príncipe. O en el resto de España. Y compara ese número con el de las sentencias judiciales que se han dictado por verdadero terrorismo. Es un escándalo. Pero nadie dice nada de esto.

Hakim tenía razón. Al menos en parte. Durante la infiltración de *El Palestino* yo llegué a tener una buena amistad con algunos de los supuestos terroristas árabes más «peligrosos» según la prensa. Como el palestino Ibrahim Abayat, o el iraquí Abu Sufian, considerado por la prensa «el hombre de Al Zarqaui» en España. Viví su lenta agonía, desde su detención en la mezquita malagueña de La Unión en 2005, hasta su juicio, al que asistí como público, en 2010. El «jefe de Al Qaeda» en Al Andalus fue absuelto, después de un martirio legal de cinco años, que otros muchos supuestos terroristas han vivido antes y después de él.[49]

Pero entre casos como el de Abu Sufian y casos como el de Rachid Hassein Mohamed, algo había cambiado: la captación de *mujahidin* se había trasladado desde las mezquitas a la red…

Debatimos mucho sobre los problemas de criminalidad que han crecido en Ceuta de forma directamente proporcional al paro. Sobre todo el tráfico de hachís y de seres humanos en el Estrecho —«Pero eso tampoco tiene nada que ver con el islam. Un buen musulmán jamás participaría en eso», subrayaba Hakim indignado—, y también sobre el mito de la pobreza como el principal elemento de captación yihadista. Y con buen criterio, Hakim argumentaba que es falso. Que personas, como el taxista Rachid Hassein Mohamed, tenían un buen trabajo, casa, familia y estaban integrados en la sociedad occidental. Y lo cierto es que la inmensa mayoría de terroristas que yo he conocido en persona pertenecían a familias de clase media o incluso acomodada. Reducirlo todo a un problema económico, en mi opinión, es muy simplista. Y así fue como llegamos a un nuevo hilo para la investigación que tenía entre manos:

—La culpa no es de los imames —me confirmó Hakim—. La culpa es de internet. Todas las mezquitas de Ceuta están controladas por la Policía y el CNI. Aquí nadie intenta captarlos para ir a Siria a matar a otros musulmanes. El gran demonio es internet…

Hakim señaló inequívocamente una serie de foros, webs y blogs como el gran problema del yihadismo en Ceuta. Pero antes de abandonar la ciudad insistió en que tenía que ver algo más. Y me condujo hasta la plaza de los Reyes, en pleno centro de la ciudad.

Desde el 5 de mayo anterior, más de un centenar de refugiados sirios, que habían llegado a Ceuta huyendo de la guerra, habían improvisado un campamento frente al edificio de la Delegación de Gobierno, suplicando asilo.

—Deberías contar esto —me dijo—, dicen que un puñado de ceutíes se van a Siria a hacer la guerra, pero lo cierto es que cientos de sirios vienen a Ceuta escapando de ella.

El Ramadán de 2014 fue duro, aunque no tanto como lo sería el de 2015. Al coincidir con los meses de más calor los días eran largos y asfixiantes, y en aquellas tiendas improvisadas con lonas, pedazos de plástico y mantas, docenas de familias sirias sobrellevaban como podían su desamparo, gracias a la solidaridad de los españoles. Tanto musulmanes como cristianos. Ellos habían sufrido en sus carnes la crueldad del Estado Islámico y los demás actores de un juego geopolítico que había desplazado el tablero desde Afganistán y Pakistán a Irak y Siria.

Por la noche, en un cibercafé cercano al hotel, seguí las indicaciones de Hakim para buscar al Diablo en la red. No fue difícil. Basta seguir los *hashtags* apropiados en Twitter para descubrir los perfiles de cientos de terroristas del ISIS, que constantemente invitan a los jóvenes musulmanes de Occidente a viajar a Siria para unirse a su aberrante causa. Una vez identificados los usuarios de esos perfiles, es fácil localizarlos también en Facebook y en otras redes sociales, y asistir perplejo al espectáculo de horror que su delirio siembra en uno de los países más bellos y hospitalarios que yo he conocido. Allí está su diabólica obra, asomándose a la pantalla de tu ordenador. Y su mensaje recurrente: ven a Siria, únete al ISIS.

El Diablo en tu teléfono móvil

En 2003, Manuel Torres Soriano presentó su tesis doctoral en la Universidad de Granada, y se publicó en 2007. Bajo el título *La dimensión propagandística del terrorismo yihadista global,* Torres Soriano había hecho una meticulosa investigación académica, una de las muchas que se han realizado, sobre el factor propagandístico en la extensión del terrorismo yihadista. Su estudio es fascinante.

> En nuestra investigación —escribe Torres Soriano— nos hemos decantado por el llamado Movimiento Yihadista Global (GJM en adelante), denominación que trata de englobar la complejidad de una organización terrorista como Al Qaeda, la cual ha evolucionado desde sus iniciados hasta mutar en una realidad completamente distinta a la de una organización terrorista convencional. Estas siglas han sido útiles para simplificar y hacer operativa una realidad compleja compuesta por grupos y redes que comparten una misma visión de la región y la legitimidad del uso del terrorismo.[50]

Con este universo de estudio, Torres se pregunta cuál es el papel que desempeña la propaganda en la consecución de los objetivos del Movimiento Yihadista Global. Esa es la clave de su estudio, y eso es lo que me interesó cuando su tesis cayó en mis manos. Para responder a esa pregunta, consulta infinidad de fuentes, siguiendo los pasos que hemos seguido muchos investigadores, antes y después de él. Torres menciona medios como la CNN, BBC o Al Jazeera. Organizaciones como el Centre de Noticies per a la Difusió de les Ciencias Criminológiques, Global Research in International Affaire (GLORIA) Center, SITE Institute o The Jamestown Foundation's, entre otras.[51] Sin embargo, y en base a mi experiencia personal en la fase de formación teórica de *El Palestino,* más que las opiniones de los expertos teóricos, son de valor las fuentes directas. Siempre es mejor trabajar sobre el terreno, pero a falta de eso Torres Soriano accedió a una serie de comunicados emitidos directamente por las organizaciones terroristas, que en mi opinión reflejan mejor que cualquier estudio teórico las características de dicha organización. Más de cuatrocientos comunicados oficiales emitidos por Al Qaeda y todas sus organizaciones satélite.

Como buen académico (objetivo, empírico, científico), Torres Soriano es consciente, y así lo subraya en su tesis, de que el término *terrorismo* no ha alcanzado un consenso universal. Y esa reflexión no es baladí. Ninguno de los «terroristas» a los que conocí durante mi investigación —no importa que pertenecieses a ETA, las FARC, Hamas, las Brigadas de los Mártires de Al Aqsa, el ELN, el IRA, los grupos bolivarianos, Hizbullah o Al Qaeda—, ninguno, repito, aceptaba la etiqueta de «terrorista». En su léxico, dicho término quedaba para referirse a los estados de Israel, España, Estados Unidos… Peor aún, incluso entre los mismos estados europeos o americanos no existe unanimidad de criterio para definir quién es o no es terrorista. Y mientras organizaciones como Hamas o Hizbullah, son partidos políticos legales en sus respectivos países, tras obtener el poder en unas elecciones

democráticas, en algunos listados de grupos terroristas se les equipara a Al Qaeda o el ISIS.

Aclarado esto, Torres Soriano entra a calzón quitado en el análisis de la ingente documentación reunida para su tesis. Y analiza la función de la propaganda terrorista:

1. Mantener la cohesión interna y acrecentar la moral y motivaciones del grupo.
2. La captación de nuevos adeptos.
3. Aterrorizar a la población enemiga y minar la confianza que esta deposita en sus gobernantes.
4. Generar simpatías y apoyo entre su base social.[52]

Y al referirse a la propaganda —y ahí vamos—, se refiere también a la publicidad mediática que alcanzarán sus acciones. Lo que implica un «estudio de mercado» previo a la matanza, solo asumible por mentes enfermas, psicópatas y crueles, capaces de gestionar la rentabilidad del terror con la misma frialdad que se estudian las prestaciones de un electrodoméstico (característica esta de toda forma de terrorismo, no exclusivamente yihadista). De hecho, el mismo Torres cita el caso de Timothy McVeigh, el terrorista católico que escogió el aniversario del asalto al complejo de la milicia cristiana de los Davidianos de Wacco por la ATF y el FBI, para detonar casi 2.000 kilos de explosivos en un edificio gubernamental de Oklahoma lleno de trabajadores. Murieron 168 personas y más de 600 quedaron mutiladas, tullidas o heridas de diversa consideración. Pero lo más espeluznante es que tras su detención McVeigh declaró que «había elegido el edificio federal Murrah para su ataque, porque estaba repleto de espacios abiertos que permitirían los mejores enfoques para fotos y televisión». La tesis doctoral de Manuel Torres Soriano está llena de ejemplos que ilustran el poder de la propaganda en un conflicto armado. Por una y otra parte.

El impacto que supuso en la opinión pública norteamericana las imágenes de los diez soldados muertos y cinco capturados en Nasiriya el 23 de marzo de 2003, hábilmente utilizada con fines propagandísticos por la resistencia iraquí, fue más brutal que un bombardeo. Hasta el punto de que la Inteligencia norteamericana «montó una operación ficticia, también televisada, para el rescate de una de sus soldados capturados: la soldado Jessica Lynch. La cual se encontraba realmente en un hospital iraquí abandonado por los combatientes enemigos».[53]

En otras palabras, que el Servicio de Operaciones Psicológicas del Ejército norteamericano creó un montaje, una película de un falso rescate heroico, para paliar el daño psicológico que había causado en los Estados Unidos la propaganda de la resistencia al exhibir a sus soldados muertos y prisioneros en las principales cadenas de televisión árabes. Las falsas imágenes de su rescate dieron lugar, ese mismo año, a una película: *Salvar a la soldado Lynch*, dirigida por Peter Markle y con Laura Regan en el papel de la soldado falsamente rescatada. Contrarrestando así, al estilo Hollywood, la propaganda terrorista. Como ya habían hecho antes con el Black Hawk derribado en Mogadiscio. Otro error militar que subsanó con una buena dosis de

propaganda cinematográfica. La mejor forma de reescribir la historia.

En España vivimos un trauma similar cuando se emitieron las imágenes de los siete agentes del CNI asesinados en Irak el 29 de noviembre de ese mismo año. Pero nuestro Gobierno no montó un falso documental con imágenes del rescate del superviviente, ni subvencionó una película sobre el tema.

Durante las 480 páginas de la magnífica tesis doctoral de Manuel Torres, asistimos a la evolución de la propaganda yihadista. De pequeños fanzines impresos, y videocasetes que debían enviarse por correo a los medios de comunicación, a las primeras apariciones en internet, que cada vez va cobrando mayor protagonismo.

Poco a poco, las primeras revistas yihadistas, que también podían descargarse en internet, como *La Voz de la Yihad, Campo de entrenamiento Al Battar* o la destinada a las yihadistas mujeres *Al Khansaa,* combinaron sus contenidos con vídeos efectistas y atroces. Y todo porque habían descubierto el efecto mediático del horror, y del eco que despertaba el enfermizo morbo de los seres humanos, con las decapitaciones televisadas.

El vídeo que titularon «El degollamiento del periodista-espía, el judío Daniel Pearl», fue el punto de partida de una atroz tendencia que continúa en nuestros días. Lo subieron a internet, y desde allí se reprodujo en diferentes canales de televisión. La terrible historia de Daniel Pearl, que Angelina Jolie llevó al cine en la película *Un corazón invencible* (2007), y la espectacular propaganda que generó a Al Qaeda en todo el mundo, marcó el camino.

En febrero de 2000, había aparecido la primera página web oficiosa de Al Qaeda en internet: maalemajihad.com (hitos del yihad), alojada en un servidor chino. Maalemajihad fue la página precursora de la famosa Al Neda, posterior web oficial de Al Qaeda. Al menos hasta que en 2002 los terroristas perdieron el dominio, que «fue adquirido por un ciudadano norteamericano que trataba de ese modo de realizar su particular contribución a la lucha contra el terrorismo».[54] Tampoco eso consiguió frenar mucho tiempo la presencia de Al Qaeda en la red. Después, en abril de 2003 llegaría Al Faroq, y más tarde muchas más web, blogs y foros. A partir de ese año la propaganda yihadista comienza su tránsito definitivo a internet.

> El GJM cree firmemente que el ciberespacio les ha permitido sortear las barreras impuestas por los enemigos del islam para que pueda producirse una directa y masiva comunicación con la *umma*. Los yihadistas creen ciegamente en la capacidad transformadora de su mensaje, de ahí que la principal barrera que detectan sea los esfuerzos llevados a cabo por los regímenes «apóstatas» y la conspiración «cruzado-sionista»para impedir que los musulmanes sean conscientes de sus verdaderas obligaciones como creyentes. Para el GJM el ciberespacio ha permitido romper los límites impuestos por los aparatos represivos del Estado y ha acabado con el monopolio de la propaganda oficial.

Una de las organizaciones que Torres incluye en su estudio, Al Qaeda en la Tierra de los Dos Ríos, tendría un protagonismo fundamental en los años posteriores, pero por desgracia la revolución digital de la propaganda en internet, gestionada por el Ejército Islámico, se inició cuando la tesis de Torres ya estaba concluida.

Allí, en la organización liderada por un viejo conocido mío, Abu Musab Al Zarqaui, que tantos quebraderos de cabeza me dio cuando busqué a su familia en la ciudad jordana de Zarqa, fue el inspirador de ese monstruo abominable al que Hakim se refería como «el Diablo en internet»: el Ejército Islámico.

Ya sabía cómo el Diablo utilizaba la red, en la captación y propaganda. Un año después descubriría cómo luchar contra él en su propio terreno: internet.

OCTUBRE DE 2014
DESAPARECIDO

«Sigo el camino que me marca la Providencia con la precisión y seguridad de un sonámbulo.»

Adolf Hitler, discurso en Renania, 1936

Octubre es un mes triste. El día 5 mi compañero, el cámara de Telecinco José Couso, habría cumplido cuarenta y nueve años. Pero el 8 de abril de 2003 un tanque norteamericano decidió dar una lección a la prensa que cubría la ocupación de Irak bombardeando el hotel Palestina de Bagdad, donde estaban los periodistas, y se llevó su vida. Hasta hoy nadie ha sido procesado por ese asesinato. Es bueno que eso no se olvide…

Cinco días después de esa onomática, el 10 de octubre de 2014, recibí un mensaje en mi correo de Facebook. No provenía de ninguno de mis contactos. Ni siquiera de alguien con quien tuviese un «amigo» de Facebook en común. La remitente, a la que llamaré Marga, había decidido comunicarse conmigo, angustiada por la desaparición de MarkoSS88.

Buenas, Antonio. Mi nombre es M… soy amiga de Markos. Me pongo en contacto contigo porque sé que hablas con él, me lo ha dicho. Te escribo porque estoy preocupada por él. Anda la Policía buscándole y no sé nada de él. Tengo miedo de que le haya pasado algo y no sé con quién contactar. Por favor, si lees esto, contéstame. Gracias.

A pesar de su juventud, Marga resultó ser una veterana del movimiento NS, muy cercana a UltraSSur y exmilitante de AN:

Yo me considero de ideas nacionalsocialistas… Yo antes era muy parecida a Markos. Reconozco que llegué a la violencia, pero me di cuenta de que no me iba a llevar a nada, aunque mi ideología sigue siendo la misma… Yo cambié mi visión y dejé la violencia gracias a una persona que me ayudó y aparte me cambió mucho el ser madre y digamos haber tenido una vida dura pero salí de ello y es lo que quiero que haga Markos. Él es joven y yo ya tengo treinta y cuatro años y he pasado por todo…

Durante años, Marga militó en grupos ultras, y a pesar de que en mi caso eso lógicamente disparaba las alarmas, mi intuición me decía que su preocupación por Markos era sincera y profunda. Tan profunda y sincera como para decidirse a escribir al periodista más odiado por los skinhead neonazis españoles.

Naturalmente, le contesté. Yo también estaba inquieto por la desaparición de Markos, y por el hecho de que no contestase a mis mensajes. En un principio creí que la presión de sus camaradas de UltraSSur, por hablar con

Tiger88, le había hecho cortar nuestra comunicación. Pero no era así.

Le dije a Marga que Markos y yo llevábamos meses intercambiando emails, pero que hacía tiempo que no respondía mis mensajes. Marga insistió.

> Es que ayer estaba con miedo y no sé qué hacer. Quiero contactar con su abogado y no sé quién es. Hemos ido a la nacional pero nada. Él me jura que no ha hecho nada, pero ya le pegaron una paliza hace unas semanas y tengo miedo.
>
> Sí, ya me contó lo tuyo y él, y yo le dije que le importara un carajo lo que le digan sus colegas. Como le dije si le hablas, será porque habéis llegado a un entendimiento. Yo desde luego se lo hice ver. Y sé que él mira mucho por ellos y no se da cuenta de que si le tienen que dejar de lado lo harán. No hago más que decirle que mire por él, que es buen tío, y no desperdicie su vida.

La angustia de sus mensajes resultó contagiosa. Durante los días siguientes Marga y otras «camaradas» por un lado, y yo por otro, intentamos localizar a Markos en hospitales, comisarías de Policía y cuarteles de la Guardia Civil. A pesar de que buenos amigos del Cuerpo Nacional de Policía y la Benemérita movieron cielo y tierra, no existía ninguna detención de nadie llamado «Marcos Santos Navarro» en sus respectivas bases de datos. En los hospitales de Madrid tampoco figuraba el ingreso de nadie con ese nombre. Ni siguiera de algún joven con tatuajes que pudiesen delatar su pertenencia a movimientos neonazis.

Markos se había esfumado en el aire y ni sus camaradas de confianza sabían dónde encontrarle… Era como si hubiese protagonizado un «suicidio digital».

Capítulo 6
Los guardianes de la reputación *online*

«Necesitamos un foro mundial y un financiamiento global comprometido con el desarrollo de normas de seguridad para hacer cumplir nuestro derecho a la intimidad, no a través de la ley, sino a través de la ciencia y la tecnología.»

Edward Snowden

El Celebgate

El 31 de agosto de 2014 llegó la primera andanada y rápidamente se convirtió en la comidilla de la red. Para deleite de pajilleros y onanistas, casi medio millar de fotos privadas de actrices, cantantes, presentadoras y otras *celebrities*, desnudas o en actitud sexual, fueron colgadas en el *website* 4chan.

4chan es un tablón de imágenes ideado originalmente por el adolescente norteamericano Christopher Poole, para el intercambio de contenidos sobre manga y anime, operativo desde el 1 de octubre de 2003. Sin embargo, con el paso del tiempo sus foros y su sistema de publicación anónima facilitaron que se convirtiese en punto de encuentro de hacktivistas (y algún que otro trol). De los foros de 4chan surgieron campañas y «ataques» frikis y absurdos, que se han hecho un hueco en la historia de internet como los memorables Rickrolling o los memes de Pedobear y Lolcat. Pero también cosas mucho más serias, como Anónymous.

El Proyecto Chanology fue la primera gran acción de Anónymous. El 21 de enero de 2008, y como protesta por un vídeo de Tom Cruise que la Iglesia de la Cienciología intentaba retirar de internet, bajo amenaza de denuncia, un grupo de jóvenes anónimos y aburridos, que frecuentaban los foros de 4chan, se coordinaron para realizar una serie de ataques a las web de la Cienciología, y a toda su infraestructura tecnológica. Lo que comenzó como una broma con vocación de irritante, puro espíritu trol, dio lugar a algo más serio. Había nacido uno de los fenómenos de hacktivismo más heterogéneo, inclasificable y fascinante.

Sin embargo, en los foros de 4chan no todo eran hacktivistas y trols. Otro perfil de internauta buscaba la capacidad de anonimato que encontraba en la web para intercambiar otro tipo de material gráfico menos amable… De hecho, una parte importante del éxito de 4chan en la red se debió a sus foros sobre Lolicon y Shota, subgéneros de cómic manga que se caracterizan por la representación de niñas y jóvenes infantilizados representados en actitud marcadamente sexual, y que abrían el debate de si puede considerarse estos géneros como una forma de pedofilia. Yo opino que sí.

El 31 de agosto de 2014, como decía, 4chan volvía a ser noticia al recibir la primera descarga de imágenes sexuales robadas a un centenar de celebridades. Curiosamente casi todas mujeres: jóvenes actrices, presentadoras, cantantes, deportistas… No es difícil imaginar al atacante, un varón, solitario, pajillero, con el cerebro acomodado entre los testículos, lo que convertiría su trastorno obsesivo compulsivo en una enfermedad venérea. Porque, desgraciadamente, muchos hombres piensan con la polla.

Jennifer Lawrence, Kate Upton, Mary Elizabeth Winstead, Jessica Brown Findlay, Kaley Cuoco, Kirsten Dunst, etcétera, descubrieron con horror que aquellas fotos que se habían hecho desnudas, en un momento de intimidad o complicidad, para un novio, amante o pareja, circulaban ahora por la red, replicándose como un virus, a

través de las redes sociales. Y alguna, como la gimnasta olímpica McKayla Maroney, se las hizo siendo todavía menor de edad, lo que implica un agravante a la difusión de esas imágenes robadas.

¿Cómo te sentirías tú si aquellas fotos o vídeos que hiciste, en la intimidad de tu dormitorio o cuarto de baño, destinado solo y exclusivamente a tu amante, novio, pareja… fuese de pronto subido a la red y puesto a la vista de todos? ¿Humillada, vejada… violada? La actriz Jennifer Lawrence, una de las víctimas más afectadas por el Celebgate, lo explicó muy bien: «Las personas que vieron las fotos también han perpetuado un delito sexual. Deberían sentir vergüenza. Incluso gente que estimo venía y me decía: ¡Oh, sí, vi las fotos! Yo no quería molestarme pero pensaba: Yo nunca te autoricé a mirarme desnuda». Lawrence se hizo aquellas fotos para su novio, que estaba en otra ciudad, y eran parte de una relación tan íntima entre ambos como si estuviesen haciendo el amor. Y a nadie le gusta que le miren clandestinamente mientras está haciendo el amor con su pareja.

¿Y tú, hombre, que sonríes con ironía al leer estas líneas, cómo reaccionarías si fuesen las fotos de tu hija, o las de tu hermana, o las de tu esposa, las que se difundiesen por la red para que tus amigos, vecinos o compañeros, se masturbasen con ellas? Porque, siento decírtelo, tu hija, tu esposa y tu hermana probablemente también se han hecho fotos similares…

Supuestamente los autores del robo dirigieron un ataque a las cuentas de iCloud de las víctimas, para reventar sus contraseñas y acceder a sus archivos en la nube de Apple, y las fotos se replicaron inmediatamente en miles de sitios. Ahí siguen. Cualquiera puede encontrarlas buscando un poco, a pesar de que muchas de las víctimas demandaron a Google por ello.

No importa cuánto dinero tengan. Cuántos Oscar, Grammy o Globos de Oro hayan ganado. Si las contraseñas de sus cuentas de internet no eran seguras, sus secretos estaban al alcance de cualquiera… y por eso los perdieron.

El hacktivismo no tiene nada que ver con esto. Los ciberdelincuentes que compararon esta mierda con lo que han hecho Assange o Snowden sencillamente los están ofendiendo. Y a nosotros nos están llamando estúpidos.

Pero los robos de imágenes privadas y su difusión por internet era solo una parte del problema al que se enfrentaron las *celebrities* atacadas. El otro eran los *fakes*.

Existen cientos de páginas en internet en las que se exhiben imágenes de contenido pornográfico, sustituyendo el rostro de las actrices porno por los de actrices, cantantes o presentadoras famosas. Algunos son unas chapuzas, pero otros están verdaderamente bien hechos y resulta muy difícil distinguirlos de una imagen real. Y ese es el problema.

El Celebgate generó un efecto colateral no deseado. De repente, las imágenes (totalmente falsas) de famosas manteniendo todo tipo de perversiones sexuales ganaron credibilidad. ¿Se trataba de un *fake* o de una imagen real robada de su cuenta de correo? Y como internet es como la carretera, donde nos envalentonamos para

tocar el claxon, cagarnos en la puta madre de otro conductor o mandarle un corte de mangas, eso sí, sin bajarnos del coche, los internautas explotaron esa confusión, generando todo tipo de contenidos y comentarios desagradables.

En España, por supuesto, existen también webs especializadas en *fakes* de famosas. Durante el rodaje de las películas basadas en mis libros *Diario de un skin* y *El año que trafiqué con mujeres,* tuve la oportunidad de conocer y charlar con las actrices de los respectivos repartos: Macarena Gómez, Juana Acosta, Raquel Meroño, Jennifer Rope… Y recuerdo que varias de ellas mostraban su preocupación por este problema. Sin embargo, en España, la primera en personarse en una comisaría de Policía para poner una denuncia explícita, hastiada de los miles de *fakes* pornográficos realizados con su cara, fue la actriz y presentadora Pilar Rubio.[55]

Gracias a eso algunas web especializadas en ese subproducto pornográfico especificaron que los *fakers* (creadores de *fakes*) podían subir cualquier *fake* anal, facial, zoófilo, etcétera, de cualquier actriz, presentadora, cantante, periodista, etcétera, española… pero no de Pilar Rubio. Después, otras siguieron sus pasos. Pese a ello los miles de *fakes* realizados antes de su denuncia continúan flotando en el océano de la red. Porque, como repetía Israel Córdoba, «todo sube a la red, pero nada desaparece del todo».

El Celebgate español, sin embargo, fue diferente. De hecho, no fue. A pesar de que algunos colegas periodistas intentaron amortizar el tirón mediático utilizando ese concepto en sus titulares.

Lo que ocurrió en España, y en otras partes del mundo, fue que las imágenes sexuales obtenidas al activar la cámara web de la víctima, mientras esta mantenía cibersexo *online,* afectaban a conocidos y mediáticos varones…

Al tronista de *Hombres, mujeres y viceversa* y concursante de *Mira quién salta,* Leo Cámara, o a los futbolistas Ronaldinho o Maxi López, los pillaron de esa manera. En 2011 (Ronaldinho) y 2012 (López) alguien les grabó a través de la webcam mientras tenían cibersexo y divulgó las imágenes en internet. Si hubiesen colocado un simple adhesivo sobre la cámara de su portátil, se habrían ahorrado el bochorno y la vergüenza. Una vez más, los consejos de X1Red+Segura se demostraban con casos prácticos.

OnBranding, guardianes de tu reputación digital

«Esto no les habría pasado, si hubiesen conocido a Selva…» La frase de Martín, otro de mis guías en este viaje, fue la mejor carta de presentación.

OnBranding es una consultoría de reputación *online* y ciberinvestigación, especializada en protección de marcas corporativas y personales en internet (gestión de crisis digital, reputación *online*, retirada de contenido en internet, posicionamiento y desposicionamiento de contenido en *social media*, así como en promoción de apps móviles…). Vamos, que abarcan todo lo que puede afectar a nuestra reputación digital. Otra de las piezas del puzle de nuestra vida en la red.

Sus oficinas están ubicadas en la barcelonesa Rambla de Catalunya, casi haciendo esquina con Diputació. Una de mis zonas favoritas en la ciudad. Repleta de librerías de viejo. Muy cerquita del antiguo Teatro Barcelona, que entre 1925 y 1983 acogió los estrenos de García Lorca, Asquerino o Marsillach, el edificio que acoge OnBranding también tiene mucha historia, aunque la empresa liderada por Selva no tiene nada de obsoleto ni anticuado. Por el contrario, se mantiene al día de las últimas novedades en seguridad informática, porque entre sus clientes se encuentran, me consta, importantes empresas, multinacionales y… algunas estrellas mediáticas de la televisión en España.

Selva María Orejón es la fundadora y directora ejecutiva de OnBranding. Brillante, enérgica, y con una capacidad de trabajo y voracidad de conocimiento inabarcable, es además una profesora didáctica y comunicativa. Lo sé porque tuve la oportunidad de asistir como alumno a alguno de sus talleres sobre reputación digital y ciberinvestigación. Nos habíamos conocido previamente en casa de Martín, pero fue en esos talleres donde aprecié su potencial.

Pese a mi insistencia periodística, Selva es una profesional responsable y en ningún momento aceptó mostrarme ejemplos reales extraídos de los casos que lleva su empresa. Sin embargo, me lo puso fácil… «No te costará demasiado si sabes buscar, muchos están publicados en la red.»

Licenciada en Ciencias de la Comunicación en la Universidad Ramon Llull, especializada en gestión de crisis, estrategia de reputación y comunicación *online*, Selva no deja de estudiar. Cuando la conocí cursaba Applied Cryptography y técnico avanzado en ciberseguridad para Inteligencia.

—Celebgate parece un ejemplo obvio de ataque dirigido, pero ¿quédiferencias hay para vosotros entre un ataque aleatorio y uno dirigido?

—La naturaleza de la motivación del ataque es lo que marca la diferencia entre ambos. Siempre hablamos de cuatro motivaciones básicas que mueven a un agresor o una red organizada a idear y perpetrar un ataque: un motivo económico; un motivo emocional personal o profesional (desamor, despecho profesional); un motivo activista (político, filosófico…) o un motivo psicopatológico. Y luego están los motivos combinados, por ejemplo, un motivo 2 combinado con un motivo 1 y un

motivo 4 es muy típico a la par que muy peligroso.

»Cuando alguien pone un componente personal/profesional en el ataque, es ya un ataque dirigido. En cambio, un ataque aleatorio es un ataque en red, un ataque que no se fija en la persona en sí, sino en si su perfil está dentro del perfil que interesa atacar, por ejemplo, su estatus profeso-social *(celebrity).* O bien, si buscan tener una red de ordenadores zombi, lo que buscarán es que las víctimas "ordenadores" estén desprotegidas. De todos modos, como bien dice uno de mis mejores colegas profesionales, en cualquier ataque tenemos un componente de ataque dirigido, porque de un modo u otro te han escogido como víctima.

En enero de 2014, Argentina vivió su propio Celebgate. Un ciberdelincuente que se ocultaba bajo el nombre de Camus Hacker consiguió mantener en tensión a los famosos del país latinoamericano, tras hacer públicas numerosas fotografías y vídeos íntimos de actrices, cantantes, deportistas y presentadores de televisión. Pero, a diferencia de lo ocurrido en el Celebgate, Camus afirmaba que no había robado imágenes que las propias víctimas se habían hecho, sino que había conseguido sus direcciones de email, activando remotamente las webcam de sus ordenadores personales para fotografiarlos en la intimidad de sus casas. Lo cierto es que, durante semanas, los famosos argentinos vivieron una auténtica psicosis de pánico cada vez que se sentaban ante su ordenador. Al fin, y gracias a la investigación de auténticos hackers, el joven Emmanuel Ioselli fue identificado como Camus Hacker y procesado, y sus supuestas habilidades técnicas cuestionadas. Sin embargo, lo cierto es que Camus Hacker consiguió reunir cientos de miles de seguidores en Twitter, gracias a la publicación dosificada de infinidad de fotos íntimas de las *celebrities* argentinas en su cuenta.

—Imagina que os llega el caso de una importante presentadora de televisión, un actor famoso, o un político relevante, que quiere eliminar una serie de contenidos en la red que atentan contra su imagen… ¿Qué haríais? —le pregunté a Selva.

—Cada caso es diferente y es un mundo en sí, pero como norma principal, si no es un caso de crisis, trabajamos en evaluar los argumentos legales con el fin de ejercer su derecho al honor, su derecho al olvido y pedir la retirada. Se pide la retirada a las plataformas y a los lugares donde está replicado el contenido y a los propios buscadores (no solo Google, también Bing, Yahoo y Ask). Hay clientes que están en pleno proceso judicial y que aún no hemos podido retirar su contenido por dónde está albergado. Entonces debemos iniciar simultáneamente la creación de una identidad paralela, desposicionar el contenido generando contenido positivo relativo a una serie de palabras clave, para que cuando se busque por dicho cliente aparezcan los resultados que nosotros queremos y no lo que un tercero dice de este famoso.

»Para que nos entendamos: esto no es un lavado de cara, una limpieza de imagen o un barrer la basura del famoso en cuestión. Esto es analizar qué imagen estás proyectando y qué imagen quieres proyectar. Igual que en la vida *offline,* si alguien habla mal de ti, tú tienes la opción y casi la obligación de aclarar lo sucedido y dar tu

versión de los hechos.

»Existe lo que llamamos una comunicación activa y una comunicación pasiva. Si tú no dices nada en activo, los demás estarán hablando por ti y en el mejor de los casos, tú lo sabrás. Bien, en internet de entrada debes saber qué estás proyectando, quién está generando el contenido, quién lo replica y quién lo está difundiendo. Una vez contamos con esta información, ponemos el protocolo en marcha y empezamos a marcar los objetivos, la estrategia y la táctica que se ha de usar, así como las acciones concretas que necesitamos.

Recordé la desaparición de MarkoSS88 que nos tenía preocupados. Algunas personas, en un momento determinado de su vida, deciden desaparecer de manera voluntaria de la red borrando toda su vida digital.

—La última solución, si todo falla, es el suicidio digital… —comenté.

—Depende —replicó Selva—. No es «si todo falla». A veces nos han pedido desaparecer de internet sin que se haya intentado nada antes. Quiero decir que, en ocasiones, el propio objetivo del cliente es desaparecer con la identidad que tenía y reaparecer con otra nueva. Un claro ejemplo son las personas víctimas de violencia de género, personas que han estado en prisión, personas que han tenido un pasado vinculado a una historia de la que no se sienten orgullosos ni las beneficia, o bien personas que necesitan hacer un borrón y cuenta nueva, por seguridad. Y nunca mejor dicho, cuentas nuevas de todo. Limpieza de todas las cachés, inventar una identidad nueva relacionada con una misma identidad pero otra carrera profesional, otra ubicación… Una vez, no voy a indicar quién, una persona nos pidió desaparecer de internet en España y reaparecer con otra carrera profesional en cinco países de Latinoamérica. En otro momento, un personaje público nos pidió que le suicidáramos digitalmente hablando y lo hiciéramos aparecer relacionado a otro perfil profesional del todo opuesto al anterior.

Aunque Selva no quería decírmelo, yo sabía por otras fuentes que uno de esos clientes no deseados era uno de los líderes históricos de la extrema derecha en España, y uno de los personajes que pude conocer en persona durante la infiltración de *Diario de un skin*. En la era de internet, hasta los nazis quieren limpiar su pasado. Y como OnBranding declinó el servicio, el tipo contrató a otra empresa.

—Ahora, aun cuando morimos físicamente, nuestra vida digital continúa en la red —continué—. Quedan redes sociales abiertas, cuentas que están ingresando dinero de juegos *online,* etcétera. ¿Cómo se enfrenta una familia anónima a esta situación? ¿Y qué ocurre cuando el fallecido es alguien célebre como Álvaro Bultó o Santiago Trancho? Creo que conoces ambos casos…

—Bueno, esta es una buena fase de la vida digital de una persona… Digo una buena fase porque profesionalmente así lo considero. Pero evidentemente es un drama para una familia que no tenga conocimiento de redes sociales, y menos si no sabe usar los mecanismos que estas mismas dejan a nuestro alcance. Por ejemplo, si hablamos de Facebook, podemos cerrar la cuenta del perfil del fallecido y esta

desaparecerá de la red social y ya no aparecerá en los resultados de los buscadores. La plataforma social ya no dejará que sus contactos envíen sugerencias o recordatorios relacionados con esa persona, situación absolutamente molesta. Y ¿qué pasa con toda la información contenida en la cuenta, ya sean fotos, enlaces, conversaciones, etcétera? Pues que será retirada; en cambio, el contenido que ese perfil ha dejado en perfiles de terceros (comentarios en un muro, los eventos a los que ha asistido pero que organizan otros, los mensajes privados con otros usuarios, y demás) seguirá visibles. Cuando la cuenta se cierre ya no se podrá reactivar y tampoco se podrá recuperar el contenido de la misma. Se puede pedir a través de… Dame un segundo.

Selva abrió su ordenador, buscó su perfil en Facebook y no paró hasta encontrar el enlace que quería apuntarme:

https://m.facebook.com/help/contact/228813257197480.

—Yo, personalmente —prosiguió—, recomiendo que además se pida una actualización de caché de los principales buscadores (Google, Bing, Yahoo y Ask) para que la información sobre la cuenta cerrada ya no aparezca como resultado de búsqueda asociada a la identidad del fallecido. También puedes dejarle la cuenta en legado a uno de tus contactos, de modo que pueda tener la responsabilidad de tu cuenta cuando fallezcas. Se hace a través de otro enlace. Espera.

De nuevo, Selva tecleó con la agilidad y rapidez que da la experiencia, manejando el ratón del ordenador con la pericia del domador acostumbrado a dominar a las fieras del ciberespacio con su látigo.

—Este es: https://m.facebook.com/home.php#!/settings/security/?legacy_contact. En el caso de ser famoso, como bien comentabas, también lo puedes pedir con un memóriam o bien cuenta conmemorativa, se solicita a través de aquí: https://m.facebook.com/help/103897939701143?ref=m-search#!/help/150486848354038?ref=m-search.

Recordé entonces el caso de uno de los actores que participaron en una de las películas de ficción que se han realizado sobre mis libros. A través del director supe que había sufrido un chantaje a raíz de unas imágenes comprometidas que habían robado de su ordenador, y que había preferido pagar al cracker antes de poner denuncia. Quise conocer la opinión de Selva al respecto. ¿Por qué los famosos no quieren denunciar cuando les pasa algo así? Lo pensó durante unos segundos.

—Gran pregunta —dijo por fin—. La mayor parte de mis clientes famosos no quieren denunciar por miedo a dos cuestiones básicas: bien porque temen que la información se filtre, o bien porque no confían en que se pueda hacer algo y les preocupan las represalias. Ante esta primera voluntad, lo mejor es hacerles entender, en el caso de que yo también lo crea así, que un acto delictivo en el que hay una extorsión sumada de por medio se debe denunciar. Como es lógico, cliente, OnBranding y cuerpo policial competente trabajan de forma conjunta para escoger la mejor intervención. No siempre el silencio es la mejor opción, y tampoco una

respuesta rápida.

Por suerte, cada vez más *celebrities* y personajes públicos se conciencian de que es preferible denunciar. En noviembre de 2011, la Policía Nacional detenía a un tuitero e imputaba a otros tres por las amenazas de muerte que venía recibiendo el periodista deportivo Juanma Castaño desde meses atrás. Cada vez que el periodista se sentaba ante las cámaras de Cuatro, o ante los micrófonos de la COPE, recibía en su cuenta de Twitter mensajes como: «Vete preparando tu ataúd, mierda seca. Cada vez te queda menos. Voy a por ti y a por los tuyos». Tras vivir unos meses de angustia, el periodista decidió poner en conocimiento del Cuerpo Nacional de Policía su situación.

Ese mismo mes de noviembre, la humorista y presentadora Eva Hache respiraba tranquila cuando la Brigada de Investigación Tecnológica del CNP detenía también, en Marbella, al tuitero que llevaba meses atemorizándola en la red social con mensajes como: «Te odio a muerte te odio con toda mi alma si te cruzas con mi vete corriendo», «Putaaaaaaaaaa muereteeeeeeeeeeeeeeeee» o «Voy al teatro y te apuñalo delante de todo el mundo». Yo he recibido muchos mensajes similares, de personas como MarkoSS88, y puedo dar fe de que es muy desagradable. Por mucho que tus amigos y la Policía te repitan que no te preocupes, que solo son bravatas… yo sí puedo comprender la angustia que debía de experimentar mi admirada Eva Hache cada noche. Al quedarse sola. Al entrar en el ascensor. Al meter el coche en el parking. Al abrir el ordenador…

En mayo de 2012 fue la presentadora de Televisión Española María Escario, la que sufrió la persecución en las redes sociales. En su caso con el agravante de que, tras recuperarse de un terrible ictus cerebral, comenzó a recibir mensajes como: «La pena es que no te matara el ictus… Volveremos a intentarlo». Pero si existe un caso paradigmático es el de su compañera, la también presentadora de TVE Lara Siscar. Su *ciberbullying* comenzó en Facebook, en 2009. Pero no denunció. El acoso llegó al extremo de decidir cerrar su cuenta de Facebook en 2011. Se pasó a Twitter, y los acosadores también. Continuó recibiendo «mensajes amenazadores, vejatorios y denigrantes», pero no denunció. Al menos hasta 2015, cuando, hastiada de aquella situación, la puso en conocimiento de la Policía. En abril de ese año, la BIT seguía el rastro de los acosadores y los ponía a disposición judicial. Solo un imbécil puede creer a estas alturas que puede amenazar e insultar desde la red, y pretender que no le pillen. Aunque los dos individuos detenidos por el acoso a Lara Siscar habían llegado a crear hasta treinta perfiles falsos en varias redes sociales, para ocultar su rastro, obviamente fracasaron.

Otros rostros conocidos del cine o la televisión —como la periodista deportiva Ana Cobos, el humorista Andreu Buenafuente o la presentadora y actriz Paz Padilla,

entre otros— han pasado por el mismo trago. Fuera de España, el panorama no es mucho más halagüeño: actores, cantantes, presentadores, periodistas, escritores, políticos… Cualquier persona que adquiera un mínimo de popularidad será objeto del acoso en las redes sociales. Quizá por ello, algunos de los más enérgicos luchadores contra el acoso en la red son rostros conocidos, que han vivido en sus propias carnes, y en sus propias cuentas, el más despiadado *ciberbullying*, como Monica Lewinsky, Curt Schilling o Ashley Judd.

Pero OnBranding, como otras empresas del sector, no solo lleva la reputación digital de celebridades y famosos. Empresas, políticos y particulares requieren también sus servicios como ciberinvestigadores, lo que les ha permitido reunir, en los últimos años, una dilatada experiencia y una voz autorizada en todo lo referente a las amenazas que podemos encontrar en la red como simples usuarios. Y un archivo repleto de casos, que ilustran, mejor que cualquier discurso teórico, sobre los riesgos de una navegación irresponsable. Un torrente de experiencias e información de un valor incalculable para mí en este momento de mi viaje. Y más valioso aún en el futuro, cuando les pedí consejo ante una amenaza concreta…

—Sabemos que la geolocalización se puede incluir en tus fotos o mensajes si no la anulas —le comenté—, pero te he oído decir que existen otras formas de dar tu posición geográfica cuando un atacante quiere elaborar un patrón de comportamiento.

—Bueno, la geolocalización la puedes tener en muchos más lugares, no solo una red o un email. De hecho, cuando queremos localizar la ubicación de una persona (en el momento en el que tiene lugar esa comunicación) usamos balizas, es decir, una «muesca» o una miga de pan que indica por ejemplo la IP, y esa IP corresponde a un lugar que está geolocalizado. Hecha la ley, hecha la trampa, y por tanto si esa persona o ese dispositivo está navegando con una VPN y está saliendo desde Estados Unidos o desde otro lugar «cualquiera», entonces no tendrás la ubicación física real. La idea es por ejemplo balizar varias de las comunicaciones de una misma persona, también puedes usar técnicas de *fingerprinting* para extraer no solo la IP sino también más informaciones como pueda ser qué navegador utiliza, qué cliente de correo, cuándo abre el documento, la foto, si su sistema operativo tiene alguna versión que pueda contener una vulnerabilidad… Y así poder explotar esa vulnerabilidad. Es decir, la geolocalización realizada con balizas no sería una geolocalización de forma voluntaria, sino siendo «víctimas» de una investigación u observación sin saberlo.

»En cambio una geolocalización puede realizarse voluntariamente mediante el uso de redes sociales; en muchas ocasiones, uno mismo no es consciente de estar compartiendo la localización, como por ejemplo muchos usuarios de Twitter, que por defecto la comparten sin saberlo. Existen apps para localizarte, comparar esas localizaciones y ver cuántas veces ese perfil ha indicado estar en un mismo lugar y por tanto, se puede sacar un patrón de comportamiento. Estas apps son especialmente útiles para casos de *hackerazzi*. —Uso de técnicas de hacking en manos de paparazzi —. Por ejemplo, en el caso de los famosos es especialmente sensible: no solo pueden

estar compartiendo la información de dónde están a tiempo real (por ejemplo si asisten a un bolo, o están en una concentración en un hotel, en una cafetería, restaurante…). Cuando esto ocurre en tierras extranjeras, son más proclives a usar redes abiertas o redes de los lugares de concentración, y ahí se dan más casos de posibles ataques por localización y por acceso ilícito a dispositivo a través de la red a la que se conectan.

»Para que se pueda entender mejor: un famoso se concentra con varios compañeros suyos, por ejemplo futbolistas, y puede ser víctima por varios motivos de los cuatro que hemos indicado; pongamos que el motivo del ataque sea conseguir dinero. En muchos de los ataques que hemos analizado, se sufre después una extorsión: conseguir dinero a cambio de no hacer públicas las informaciones que se han conseguido; pedirles más información (imágenes, contactos…) o bien única y exclusivamente el agresor puede querer "cargarse su reputación" haciendo públicas esas imágenes, como en el caso del Celebgate, o bien por ego, para conseguir el reconocimiento de su comunidad.

Aquel concepto, la geolocalización, tendría un protagonismo crucial más tarde en la identificación de MarkoSS88, pero yo todavía no podía imaginarlo.

—¿A qué llamáis extimidad?

—La extimidad es un concepto que utilizamos para referirnos a lo contrario de intimidad; según el psiquiatra Serge Tisseron, es la exposición de los aspectos más íntimos de una persona: las imágenes de su cuerpo, su estado de ánimo, sus pensamientos, etcétera. En las redes sociales, la persona no se muestra para compartir algo con los demás, sino que usa a los otros como un espejo para reafirmarse. Es decir, puro *show-OFF.* Por lo tanto, nos encontramos con casos donde clientes han sido víctimas de la necesidad de exhibirse y exhibir a su círculo y así construir y seguir construyendo un personaje que sea más aceptado que la propia persona.

»Se dan muchos casos con menores, donde ni ellos mismos han podido decidir si quieren o no estar en las redes sociales, ni en qué redes se les va a mostrar ni cómo. Se puede generar un imaginario sobre ellos que ni beneficia a los menores, por supuesto, ni a los mayores. Únicamente «atiborra» una imagen que se quiere transmitir. En muchas ocasiones, y sin entrar en detalles por respeto a las víctimas, los menores o las parejas de adultos son sobreexpuestos en círculos de no confianza y sufren las consecuencias de no ser tratados con respeto.

—Te llega un encargo de una empresa que está siendo atacada por otra empresa de la competencia… ¿Cuál es el protocolo de OnBranding?

—Lo primero de todo es iniciar el PAS (prevenir, avisar y socorrer).

»Fase P. PREVENIR, es decir, contener, evitar mayores daños. Tenemos un protocolo propio de la fase inicial, que es para evaluar el daño, y el posible origen del mismo, en esta fase se ponen las herramientas de monitorización a funcionar.

»Fase A. AVISAR, fase 2, es la que está protocolizada para que los responsables de seguridad y reputación de la empresa se pongan en contacto con las autoridades

competentes, el juzgado de guardia, las plataformas sociales, los buscadores… Dependiendo del caso que tengamos entre manos. Pero damos pie a que también los Cuerpos de Seguridad inicien o acompañen nuestra investigación privada, denuncia y proceso policial-judicial.

»Fase S. SOCORRER, fase 3, aquí ya ponemos en marcha a los profesionales de cada campo, se inician los trabajos de reparación, securización y creación de identidades, borrado y eliminación de contenido o bien desposicionamiento.

—Hay gente que usa fotos de otras personas en internet, ¿cómo podemos descubrir si alguien es quien dice ser? He oído que han aumentado los casos de suplantación de identidad.

—Efectivamente. Además, rara es la semana que no tenemos algún caso. Ahora estamos llevando uno que además de usurpación, después se suplanta la identidad y se cometen estafas y robos en su nombre. Por supuesto, la identidad no solo te la da una imagen, ni muchas imágenes, también el uso de datos privados robados, o URL de perfiles usurpadas y usadas de forma ilícita. Pero sí, es cierto que no es tan fácil como parece detectar las información de identidad suplantada. Es decir, si tú te das de alta alertas con ciertas palabras clave relacionadas con tu identidad, ya sea tu DNI, tu nombre completo, tu apodo, tu número de teléfono, tu email, tu TIP… Cuando se detecte en la red abierta (sin estar cerrada por usuario y contraseña, por ejemplo si se publicase dentro de un foro) una publicación que usase dichas palabras clave, al menos tú ya sabrías dónde ir a buscarlo.

»Pero ¿qué ocurre cuando lo que están usando es una foto de tu DNI, tu foto de cara, la foto de tu coche…? Si más o menos se sabe cómo indexan los buscadores, sabremos que rastrean texto, no imágenes; por tanto, si no se ha etiquetado con alguna de las palabras clave que hemos descrito antes, o las encuentras con un buscador de imágenes, o no puedes dar tan fácilmente con ellas, a no ser que se haga una búsqueda relacionada, una búsqueda manual y dedicando horas, muchas horas. Cabe decir que existen buscadores de imágenes a tiempo real, pero son muy embrionarios, funcionan si tienen una base de datos previa con la que contrastar.

Cuando los casos reales superan a la ficción

En uno de los talleres sobre reputación digital organizados por OnBranding al que tuve la oportunidad de asistir, me llamaron la atención algunos de los casos más llamativos a los que había tenido que enfrentarse Selva. Podría habernos ocurrido a cualquiera. Porque, a pesar de su cuestionable legalidad, en ocasiones para hacer un ingreso en un banco, o un pago con tarjeta de crédito, o como en este caso para alquilar un coche, nos piden nuestro Documento Nacional de Identidad. Y lo damos, sin imaginar, como le ocurrió a una clienta de Selva, que ahí comienza nuestro martirio…

—Ostras, sí —soltó ella cuando le recordé ese caso—: una pareja va a alquilar un coche a una compañía de alquiler de vehículos. La recepcionista les pide el DNI y la tarjeta de crédito, los coge, y de repente uno de los miembros de la pareja se da cuenta de que están haciendo la foto con un iPhone porque la fotocopiadora no les funcionaba. Bien, el iPhone estaba conectado a la wifi del establecimiento. Wifi única y abierta a los clientes sin contraseña, por amabilidad y por dar un servicio añadido mientras esperan. Alguien accedió a la wifi de esa empresa de alquiler de vehículos, que además siempre es la misma, no la cambian y llevan días sin arreglar la fotocopiadora. El cracker que accede a la red esnifa el tráfico de datos, roba las fotos de DNI y de tarjeta de crédito y el robo está servido…

Este aspecto de la vida digital, la suplantación de identidad, es uno de los mayores problemas a que se enfrentan los usuarios. Solo en Facebook, se calcula que existen unos 83 millones de perfiles falsos y por lo menos un 1,5% de ellos —más de 1.200.000— se utilizan para engañar a otros usuarios. Por su parte, Instagram reconoció en 2014 que 10 millones de sus 300 millones de usuarios eran perfiles falsos. Pero ¿cómo detectarlos?

Según los expertos hay varias medidas que podemos tomar para intentar dilucidar si ese desconocido que nos pide amistad es uno de esos perfiles fraudulentos. No es muy complicado encontrarlas (aquí[56] tienes un enlace a Softonic o a WikiHow, por ejemplo). Allá van algunas pistas:

1. Sus fotos de perfil: los perfiles falsos suelen tener pocas fotos (porque conseguirlas es un trabajo), no etiquetadas y de baja calidad. Y si no, suben fotos de «ellos mismos» en plan sexy o de lo más perfectas, cuando no directamente la de un famoso. Por puro sentido común (qué se le va a hacer), no va a llegar un chico clavadito a Brad Pitt ni una chica clavadita a Jennifer Lawrence de la nada para solicitarte que seas «su amigo».
2. Sus «amigos»: ¿qué tipo de gente tiene ya en su perfil?, ¿y cuántos? No es normal tener quinientos amigos y encima repartidos por todo el mundo. Mira su perfil: lo habitual en uno falso es que se rellenen con datos de lo más estándar. ¿Te pega que alguien tan aburrido tenga amigos para dar y tomar? Y si no es aburrido, ¿de dónde saca tiempo para todo lo que hace?, ¿de verdad necesita ponerse a buscar nuevos «amigos» en su Facebook?
3. Sus datos de perfil: ¿cuadran con las fotos?, ¿su biografía tiene sentido? Investiga: por ejemplo, ¿te pega que un tipo con veinticinco años sea profesor de universidad o piloto?, ¿o que salga en manga corta en una foto del mes de julio si te dice que trabaja en Ciudad del Cabo, Hemisferio Sur?

Cuestiónalo, trabaja tu faceta crítica.

4. Tipo de perfil: ¿no para de exhibirse y desde el primer momento se nota que intenta ligar contigo? No te iría mal tener cuidado: algunos confunden las redes sociales con páginas de contactos, y no es buena idea dejar esa puerta abierta…
5. «Dice que conoce a un amigo mío»: confírmalo. Antes de aceptar su solicitud, pregúntale al menos quién es ese amigo y por qué se ha puesto en contacto contigo. Sentido común: si se te acerca por la calle alguien a quien no conoces, te promete que es amigo de un amigo tuyo (aunque no te dice de quién) y te pide que le invites a algo en tu casa, ¿lo harías?

Esta cuestión de los perfiles fraudulentos es importante, porque muchos de los ataques informáticos se inician precisamente en lugares como Facebook, Badoo, Twitter o Tuenti. Y eso mismo me confirmó, Selva: (…)

—Tengo muchos casos de extorsión que comienzan en las redes sociales, pero los que más me están llegando son los de sextorsión. Exparejas, examantes, exparejas de tu pareja actual, exsocios, socios enfadados, exempleados, empleados descontentos… Cualquiera con una motivación personal, económica, política o por enfermedad mental, y no bromeo, con un acceso ilícito a tu dispositivo y a tus comunicaciones, puede revelar tus secretos más íntimos y chantajearte y extorsionarte, con tal de que él se beneficie y tú hagas lo que él quiere. Siempre digo que el desamor y el dinero son los grandes pilares de los casos que llevo, y no te digo nada cuando al desamor se suma un problema de dinero y detrás está una persona con ciertos problemas mentales… Eso es imparable, porque los límites legales no son una barrera válida para ellos, les da igual.

—Ponme un ejemplo. En una de tus conferencias te oí comentar un caso que me impresionó porque se interrelacionaban diferentes redes sociales, de las que usa todo el mundo: Linkedin, Facebook, Badoo… ¿Sabes a cuál me refiero?

—Claro, y cada vez que recuerdo este caso se me contrae el estómago. Da vértigo pensar que ocurre cada día y que aún hay personas que van a seguir cayendo en estas trampas. Sin entrar en detalles, por confidencialidad y por respeto, la víctima pertenece a una buena empresa, en el sentido amplio de la palabra. Empresa de renombre, buena categoría profesional y en la que prima la confianza de los clientes en sus trabajadores y marca. Bien, esta persona está pasando por una mala etapa matrimonial y entra en Badoo para «airearse» de su situación claustrofóbica. Primer error: entrar con la misma identidad de email que en otras redes. Si alguien de tus contactos importa tus direcciones, se ejecuta un *match* y saben que estás dado de alta.

»Segundo error —prosigue Selva—: tras hablar largo y tendido durante cinco días con un auténtico desconocido que además no sabes si existe ni sus motivaciones reales, caes en la pseudoconfianza y le abres tu corazón y tu mente de par en par y además cuentas informaciones privadas reales como dónde vives, dónde trabajas… La parte contraria se va haciendo una composición de lugar y resulta que es un agresor, así que a va querer sacar algo de ti. Ya sabe que eres confiado, que te abres rápido, que por lo que cuentas tienes x tipo de vida, y pasa a la acción. De esta primera fase de tanteo y selección de víctima, pasan a la de atención, donde estarán

siempre disponibles para ti, serán el perfecto camaleón: seré quien tú quieres que sea cuando quieras y siempre que lo desees. Te diré lo que quieres escuchar y ¡zas!

»Tercera fase: fidelización de la confianza y ataque. El agresor le pide un Skype para poder hablar con más tranquilidad, con imagen, que siempre es más cómodo y la comunicación es más completa. La víctima se conecta con el vídeo incluido. Nuevo error. Resulta que la cuenta de Skype está asociada a su identidad real. El agresor va tomando nota. La víctima conecta la cámara y ¡oh, casualidad!, el agresor no puede porque no le funciona… La conversación sube de tono, la víctima se desnuda, inician una conversación erótica y lo que no sabe la víctima es que está siendo grabada. Como en Skype tiene su identidad real, sin que lo sepa ya le están haciendo una página, no un perfil, una página en Facebook con la privacidad abierta y con la URL personalizada con su nombre real, porque lo ha sacado de Facebook. El contenido de la página es el vídeo íntegro de Skype, así como el vídeo fragmentado en *frames*, fotos y más fotos de lo que ha ocurrido. De modo que sin que la víctima lo sepa, también han accedido a su perfil de Facebook, a su perfil de Linkedin. Han copiado la lista de contactos, vuelven a Badoo, su red de origen y le dicen: "O me pagas 1.500 euros, o todos tus contactos", y pegan el listado de contactos de ambas redes, "sabrán que: 1) estás siendo infiel a tu pareja; y 2) estés teniendo conversaciones por Skype y tienes estos vídeos e imágenes y las verán".

Según me contó Selva, la reacción de la víctima fue de pánico total, porque las amenazas y la extorsión venía acompañadas de llamadas desde diferentes países, diferentes voces, le llegaban mensajes con fotos del colegio de su hijo pequeño, como si hubiesen estado allí —en realidad, eran sacadas de Google Street View—, pero ¿cómo sabían dónde estudiaba el hijo? Porque en Facebook usaba Instagram connect, de modo que con la privacidad abierta se podía saber dónde había estado tomándose los últimos cafés a las nueve y media de la mañana, y con qué madres estaba.

—Tampoco quiero dar detalles de las consecuencias personales y profesionales —continuó—, pero no se pagó, se denunció: la persona no tenía recursos para afrontar una investigación, y no se dio con la red de crimen organizado. Un infierno.

El sangrante caso de esa mujer no es una excepción. Por desgracia, cada vez más miserables y desaprensivos, envalentonados por el supuesto anonimato de la tecnología, se deciden a materializar sus fantasías de poder y control, lanzando sus redes al océano de internet, y lo terrible es que siempre pescan algún incauto. Las unidades especializadas en Policía Nacional y Guardia Civil cada vez tienen más recursos, más formación y más experiencia. Y al final la mayoría de estos crackers de todo a cien termina con sus huesos en una celda. Pero la agonía, el miedo y la angustia que sufren las víctimas durante todo el proceso no puede compensarlas nadie. Por eso es tan importante conocer este tipo de ejemplos para fomentar nuestro uso responsable de la red.

—Veo que con frecuencia hay un componente emocional en la motivación del ataque. ¿Son las redes de ligue donde más información se consigue?

—Depende de qué tipo de información pero si yo quisiese hacer un ataque dirigido, desde luego buscaría si esa persona tiene presencia en redes de ligue, porque muy probablemente si la estudias bien (trabajo, aficiones, geolocalización, familia, miedos, pasiones…), puedas hacerte un perfil a imagen y semejanza de lo que busca; bajarle las defensas y conseguir que explique lo que te interesa. Después ya veremos cómo explotar sus vulnerabilidades psicológicas y técnicas.

—Pero entiendo que el problema no es solo de uno. Yo he accedido a mucha información de un objetivo, durante mis investigaciones, a través del perfil de su hijo, hermano, padre…

—En efecto, de los últimos casos que hemos llevado, hemos tenido que hacer una auditoría de privacidad a los familiares, a la pareja y a los responsables de la seguridad física de la víctima. A uno le parece mentira que uno de los escoltas de un presidente de una compañía esté en Badoo y geolocalizado mientras trabaja. Esto lo hago extensivo a miembros de Cuerpos de Seguridad del Estado, solo hace falta hacer una prueba. Pon en Google, *site:* Badoo.com y la palabra *mossos esquadra* o *policía* o *Cnp* o *ertzaina* o *ccffssee*. Vas a alucinar con la de personas que deberían estar protegiendo su identidad y que en cambio la usan primero como «la erótica del poder».

—Creo que individuos de dudosa reputación han intentado contratar vuestros servicios… ¿Os piden cosas ilegales con mucha frecuencia?

—Demasiado habitual es recibir emails o llamadas, a veces directamente visitas al despacho, donde te piden por ejemplo que hagas espionaje industrial, o bien que saques información de un terminal que resulta que no es de quien dice ser. O bien que hackees una web porque habla mal de ellos. O que hagas una campaña de desprestigio… Ante cualquiera de estas peticiones, mi respuesta es una gran sonrisa, enviarles un enlace del artículo del Código Penal que indica qué delito constituye lo que me están pidiendo y poco más. En ocasiones el desconocimiento es lo que los empuja a enviar estos mensajes.

Salí de OnBranding con la sensación de que durante toda mi vida como periodista había invertido mucho tiempo y dinero intentando obtener, a través de los medios convencionales, una información que habría podido conseguir mucho más rápidamente de haber sabido cómo buscarla en internet. Pero también con la convicción de que ahora estaba más capacitado para proteger mi vida digital.

De entrada, Selva me dio un listado de herramientas básicas para una navegación más segura, que estaba decidido a usar desde ese mismo instante:

1. Hotspot Shield: para navegación con VPN.
2. Latch: una app móvil para proteger tus cuentas y servicios *online* cuando no estés conectado, 100% gratuita.
3. LastPass: un gestor de contraseñas.
4. Brand Rain: para monitorización de tu propio nombre, datos relacionales, etcétera.
5. eGarante: una certificación de comunicaciones digitales («Básico tenerlo, y en tu caso sobre todo», me indicaba).

6. Adblock: que bloquea los anuncios.
7. Deep freeze: reinicia tu máquina desde cero cada vez que te conectas, así evitas que te hayan instalado algo en segundo plano sin que tú lo sepas.
8. TrueCaller: un detector de llamadas spam y detector de llamadas, que busca en toda la red si coincide con algún número ya identificado, webs, redes sociales…
9. WOT (Web Of Trust): te dice el grado de reputación, confiabilidad, estafa y *malware* de cada página.
10. SuicideMachine: elimina todas tus cuentas sociales en minutos.

Y también me dio unos cuantos consejos de lo más sensato, como por ejemplo que a veces un gesto tan sencillo como apagar el *router* cuando te vas a dormir, en lugar de dejar tu ordenador conectado a internet veinticuatro horas al día, siete días a la semana, te puede proteger de que, mientras duermes, alguien haya accedido a tu equipo y cuente con horas para saquear todo lo que quiera en tu disco duro.

O que algo tan simple como guardar tus fotos, vídeos y documentos en un disco duro externo, que puedes conectar al ordenador cuando los necesites y desconectarlo cuando no sean necesarios, te puede salvar la vida. Porque de ese modo, incluso si alguien accediese ilícitamente a tu equipo, solo encontraría tu historial de navegación, contraseñas, etcétera, pero no podría llevarse de la memoria lo que está a salvo, en un disco duro externo.

Sus consejos llegaron en el mejor momento, porque justo ahora iba a necesitar de todos los recursos de Selva y de mis amigos policías para enfrentarme a un nuevo reto. MarkoSS88 estaba a punto de confesarme algo que condicionaría totalmente esta investigación, y el próximo año de mi vida.

OCTUBRE DE 2014
LA CONFESIÓN

«Debo cumplir con mi misión histórica y la cumpliré porque la Divina Providencia me ha elegido para ello.»

Adolf Hitler, discurso del 12 de febrero de 1938

MarkoSS88 reapareció finalmente, de forma tan misteriosa como había desaparecido.

Para entonces, Marga y yo ya habíamos intercambiado docenas de mensajes, no solo especulando sobre el paradero de nuestro «amigo», sino discutiendo sobre el ideario NS. Marga había oído hablar mucho de mi libro a sus camaradas, y solo había visto la película y el documental pirateados en internet, así que estaba llena de prejuicios. Y supongo que para ella, discutir con Tiger88 sobre las ideas racistas, xenófobas y políticas del movimiento nazi supuso un reto. Para mí también. Por fortuna, mucho antes de debatir conmigo, Marga ya había madurado lo suficiente como para apartarse de la violencia y el odio implícitos en esa ideología. Yo solo la reafirmé en que su decisión había sido la más lúcida.

El primer mensaje que recibí de Markos tras su desaparición, resultó sorprendente.

… ayer en cuanto pude encender el móvil M. (Marga) me pasó lo que hablaste con ella. Sinceramente, gracias. Se han movido y preocupado por mí cuatro personas, entre ellos tú. Ayer no me lo podía ni creer, te preocupaste por mí, por un «puto nazi» que quiso matarte. Yo hay cosas que valoro mucho y me sentí fatal. Con lo de mis apellidos… la verdad es que no me siento identificado con una familia de hijos de puta y con unos padres como los que tengo, si se pueden llamar padres, que me han hecho pasar años muy jodidos, con mucha mierda, y decidí no usar mis apellidos, usar otros. No me siento identificado con ellos, mis apellidos únicamente los sabe mi familia aparte de policías, jueces… Claro, fuera del entorno familiar nadie los conoce, es que no quiero, me da rabia, ira, vergüenza llevar estos apellidos.

Markos acababa de confesarme que Santos Navarro no eran sus apellidos reales. Por eso no habíamos conseguido localizarle en ningún hospital ni comisaría durante su desaparición… Pero lo más duro llegaba ahora. La frase «que quiso matarte» era literal.

Y por otra parte decirte que yo estuve muy cerca de acabar contigo, el día ese que diste una charla en una universidad que había que coger entrada… Yo me quedé en lista de espera y fui y quise comprarle la entrada a algunos que me tomaron como loco. Si ese día hubiera tenido entrada, habría matado a alguien que no se lo merecía o al menos lo habría intentado, así que aunque vienen un poco tarde, te pido disculpas si alguna vez te has sentido acosado por mí o si te ha molestado algo. Date con un canto en los dientes que me he disculpado con dos personas, yo creo… Pero sé que me he equivocado y que la ira no me dejaba ver más allá de lo que yo

pensaba y te tenía entre ceja y ceja… Así que perdóname.

De pronto sentí vértigo. El primer mensaje de MarkoSS88 tras su reaparición era muy largo, de varias páginas, pero tuve que detenerme y volver a leer y releer aquel párrafo: «Yo estuve muy cerca de acabar contigo… Si ese día hubiese tenido una entrada, habría matado a alguien que no se lo merecía…».

Con arrepentimiento aparente, Markos me confesó, sin escatimar detalles, que el miércoles 5 de marzo de 2014 se había cambiado el *look* para no parecer un skinhead, había ocultado un cuchillo en la mochila, y había acudido a la Universidad Rey Juan Carlos con la firme intención de ejecutar a Tiger88. No solo eso. El día previo, 4 de marzo, y según su espontánea confesión, se había colado en el campus de Vicálvaro para estudiar los accesos al salón de actos, las vías de escape y demás. Había planificado sobre el terreno mi asesinato…

No. No era posible. De pronto resucitaron viejos fantasmas. Nadie se acostumbra a recibir tanto odio. Una cosa es encontrarte un tuit o un mensaje en tu correo, amenazándote de muerte, y otra que alguien te diga el día, la hora y el lugar donde intentó asesinarte. Solo en dos ocasiones anteriores había sentido esa sensación de desamparo, de un peligro inminente, de que había llegado mi hora…

Una fue en junio de 2009. Gracias a una amiga vinculada al movimiento skinhead NS había sabido que las novias de algunos de los imputados en el macrojuicio de Hammerskin-España habían abierto una cuenta para recaudar fondos con los que pagar a un sicario que evitase mi declaración en el juicio. Tuve que reunir todo el valor que pude para asistir aquella mañana a la Audiencia Provincial y sentarme en el estrado, consciente de que quizá a pocos metros un asesino a sueldo estaba esperando el momento oportuno para cerrarme la boca. Y a pesar de que el enorme operativo desplegado por la Guardia Civil y la Policía Nacional para facilitar mi transporte hasta la Audiencia y mi entrada en el edificio eran dignos de una película americana, nadie podía evitar que mi corazón galopase como un purasangre desbocado, intentando salirse de la caja torácica. Creo que solo los testigos protegidos que han tenido que tragarse su miedo para declarar en un juicio contra cualquier grupo criminal podrán comprender lo que se siente en esos momentos.

La segunda ocasión fue en noviembre de 2011. Mi «padrino» Ilich Ramírez, alias «Carlos el Chacal» era juzgado en París por varios atentados terroristas cometidos en 1982 y 1983, al detonar cargas explosivas en varios trenes franceses. Varios simpatizantes del Comité por la Repatriación de Ilich Ramírez habían viajado desde Venezuela para apoyar al Chacal en el juicio,

haciendo escala en España. De nuevo gracias a una fuente en los grupos bolivarianos supe que el Chino Carías había movilizado a sus contactos en España para intentar darme caza. Y sabía, tras haber convivido con ellos mucho tiempo, que no se andaban con bromas.

En ambas ocasiones viví semanas de auténtica paranoia que no deseo a nadie. Constantemente esperaba que al abrir la puerta de un ascensor, al girar una esquina o al meter el coche en un parking subterráneo un arma me apuntase directamente a la cara. Apenas podía dormir por las noches. Me movía por la calle con una sensación de angustia permanente. Con los nervios tensados como la cuerda de un violín, y atento a todas las caras y matrículas que me encontraba. Siempre malhumorado. Solo mis amigos más cercanos sufrieron aquellas semanas de permanente tensión, aunque nunca supieron el porqué de mi extraño comportamiento.

Ahora, en pleno 2014, MarkoSS88 había vuelto a resucitar aquellos demonios. Siempre intuí que el odio es contagioso, que pasa de generación en generación. Y siempre fui consciente de que para cualquier cachorro skinkead, para cualquier *prospect* de un MC 1%, para cualquier aspirante al yihad, agredir o matar a Antonio Salas supondría un reconocimiento notable en sus respectivos colectivos. Por eso quienes vivimos en esta situación nos volvemos extremadamente paranoicos.

Sin embargo, a medida que pasan los años intentas convencerte a ti mismo de que las cosas se han calmado. De que quizá no es preciso ser tan exigente con las medidas de seguridad. Quieres creer que tal vez puedes pasear tranquilamente por la calle sin sentirte observado. Que no es imprescindible conceder las entrevistas encapuchado o con la voz distorsionada. Que no hace falta completar dos veces la misma rotonda, o pasarte la vida en cibercafés, o cambiar de aspecto en los aeropuertos… Que podrás salir de casa un día sin protección, y entrar en los museos, las bibliotecas o los archivos sin tener que evitar los detectores de metales. Que podrás relajar la tensión constante… Aquel email de Markos había tirado por el retrete todas esas esperanzas. La amenaza persistía. Concreta. Real. Cercana.

No esperé ni un segundo. Inmediatamente me puse en contacto con los organizadores de la Jornada sobre Inteligencia en la Universidad Rey Juan Carlos. Tenía la esperanza de que aquella confesión de Markos fuese un farol, aunque debía averiguar si realmente alguien con su nombre se había apuntado a las conferencias. Y la respuesta que me llegó de los organizadores no podía ser más descorazonadora.

> Ya lo tengo. No sé si serán sus datos reales, pero solo tenemos un Marcos en la lista. Marcos Santos Navarro – 65936296G – markos.markitos.sb@gmail.com. El DNI es falso porque la letra no coincide, pero el correo sí vale, porque recibió información, o eso creemos…

Al recibir la respuesta de la UEP, el suelo se abrió bajo mis pies y caí por un pozo oscuro, frío y profundo… Era verdad. Markos efectivamente se había matriculado en el curso, utilizando un nombre y un DNI falsos.

Insistí. Necesitaba saber si lo que contaba era cierto. Si de verdad había estado físicamente en el auditorio de la Universidad Rey Juan Carlos aquel 5 de marzo. Si había intentado entrar en la sala de conferencias para matarme, como me había confesado. De nuevo la respuesta de los organizadores fue la peor que podía recibir.

> El sistema de acreditación era un papel que te sellaban para poder obtener el certificado, porque a los alumnos se les daba créditos de libre elección. Hubo un chico que parecía alumno que se cabreó muchísimo porque no guardó el papel y la lió bastante y no le dejaban entrar. Puede que sea él. Se puso bastante agresivo cuando eso, y empezó a gritar a los que estaban controlando.

Y aún había más…

> … otra cosa a la que no dimos importancia, pero la comento por si sirviera de algo. Unos días después del seminario, cuando fuimos a la sala que tiene la asociación, nos habían pegado una pegatina de un grupo nazi que era de Coslada. La quitamos y pasamos del tema, pero ahora igual puede tener alguna relación…

De pronto todo encajaba. Sus amenazas a la organización en Twitter, sus comentarios sobre el odio irracional que sentía hacia Tiger88. Su insistencia en que ya había matado antes y que no le importaba volver a matar. En cuanto tuve fuerzas, le escribí un email desde lo más profundo de mis entrañas.

A partir de ese día, y aunque en ningún momento interrumpí mi cordialidad en el trato, y mi empeño en convencer a Markos para que abandonase el mundo NS, mi prioridad pasó a ser averiguar la verdadera identidad de MarkoSS88.

Marcos Santos Navarro, aunque ahora sabía que no era su nombre real, no se ocultaba. Una simple búsqueda en Facebook o Twitter permitía encontrar inmediatamente docenas de fotografías suyas. Pero mis conocimientos informáticos eran todavía muy limitados, y yo no era capaz de ir mucho más allá. Y entonces una legión de amigos, todos ellos funcionarios de las Fuerzas y Cuerpos de Seguridad del Estado, decidieron venir en mi ayuda, como una compañía del Séptimo de Caballería al rescate.

Yo no se lo pedí. Lo prometo. Se me hace difícil pedir ayuda. Pero esa semana teníamos una de las comidas tertulia organizadas por David Madrid, que ahora solía convocar en un restaurante de la ciudad, y no hacía falta ser un psicólogo titulado para darse cuenta de que algo iba mal. No era yo. Y mis amigos lo advirtieron enseguida. Menudos policías serían si no.

—¿Estás bien, Toni?

Solo tuve que tenderles la copia impresa con los emails de Markos para que todos entendiesen la razón de mi angustia. No tuve que añadir nada. Era una confesión en toda regla, se desnudaba: más allá de confesar el intento de asesinato, hablaba con pelos y señales de ese que habría cometido hacía años. Cuando mis amigos llegaban a la detallada descripción que Markos hacía del crimen que lo habría llevado a prisión, todos abrían mucho los ojos:

Ahora mismo lo visualizo como si fuera ayer. Lo recuerdo tan bien porque fue el que marcó mi etapa más dura, que vendría estando en la cárcel y después. Ocurrió en 2012, yo ya no vivía con mis padres, estaba viviendo con un camarada en un barrio de Hortaleza. Era tarde y salí del metro de camino a casa. Para llegar tenía que pasar una especie de descampado donde suelen aparcar coches y unas vallas que separan el camino de tierra de una zona de obras con ladrillos y matojos. (…)

Esa noche en la zona baja del descampado vi a tres tíos. Uno de ellos empezó a gritar en cuanto me vio, empezó a amenazarme, sacó la navaja y vino a por mí. Los otros dos le seguían detrás y ahora mismo no sé lo que llevaban, podía haber reculado y echar a correr, pero avancé hacia ellos. El primero intentó apuñalarme pero solamente me rozó. Me defendí como pude, acostumbrado a pelearme en la calle y tener técnica de pelea y defensa personal. Además, tenía la ventaja de que conocía eso como la palma de mi mano. Fui reculando, hasta que vi la oportunidad de desarmarle empujándole contra las vallas, y le golpeé con el codo en la cara, haciéndome con su navaja. Ahora yo jugaba con ventaja. Aparte de tener una ayuda, el otro chaval estaba aturdido, fui directo a por los otros dos. Me llevé golpes, claro, el primero que vino a por mí, y al que le había quitado la navaja, me atacó por detrás e intentó ahogarme. (…)

Me solté como pude, y en cuanto estuve cara a cara con él, le solté un gancho que conseguí que perdiera el equilibrio. Le cogí por el cuello inmovilizándole con la navaja. Le dije a los otros dos que se fueran, que se largaran o que le cortaba el cuello… lo hicieron. No sé cuánto tiempo nos quedamos así, hasta asegurarme de que tendría el tiempo suficiente para terminar sin problemas. Le di un golpe en la espalda para que cayera. Me guardé la navaja y lo primero que hice fue pegarle una patada en la boca. Seguí dándole golpes en la cabeza y no paré hasta que lo vi inmóvil. Después salí corriendo hacia el piso de mi camarada. Matar o morir.

Si esperas una muestra de arrepentimiento por ello, me temo que no la vas a tener. No es por hacerme el duro, ni el machote, ni el más malo, sino porque no me arrepiento en absoluto de hacerlo. Llámame asesino, criminal, animal, pero no me arrepiento ni de esta ni de las veces que he pegado a cualquier otra persona.

Mis amigos cuchicheaban entre ellos, señalaban párrafos con el dedo, pero su agitación se acrecentaba al llegar a la parte en que Markos detallaba cómo había planeado mi ejecución pública:

Soy una persona que antes de hacer algo, lo planea todo. El viernes anterior a esa semana encontré por casualidad un acto en la asociación de estudiantes de la Rey Juan Carlos, donde ponía quién iba a participar. Vi aquel nombre que tanto odiaba: «Antonio Salas». Tenía que inscribirme primero para tener una entrada y no lo dudé. El chasco me lo llevé cuando, al terminar la inscripción, me pone que había entrado en lista de espera. No tenía entrada, pero no me iba a quedar con los brazos cruzados. Avisé a todos mis camaradas. Nadie sabía que ibas a estar ese día en esa universidad. Mi idea era clara, iba a acabar con Antonio Salas, con Tiger88. Mis camaradas me dijeron que era una locura, que no merecía la pena, pero ya no había quien me sacara la idea de la cabeza. Me tiré el fin de semana planeando cómo hacerlo. Atando cabos sueltos. Me bajé el plano de la universidad de la RJC de Vicálvaro. El martes me acerqué a la universidad. La examiné de arriba abajo. Salón de actos en el interior de la biblioteca, y con sala de control, que me dio la clave. Sabía que al día siguiente Antonio Salas no iba a estar sentado enfrente de los presentes, sino que estaría detrás. Solo tenía que conseguir entrar a la conferencia, y una vez allí entrar a aquella sala.

Seguía en lista de espera, me había quedado sin entrada. El miércoles por la mañana me acerqué a eso de las ocho y media. Iba vestido con unos vaqueros, unas zapatillas, una especie de camisa y una mochila con papel de aluminio, por si las moscas. Llevaba una navaja. Nadie pensaría que yo fuera a otra cosa que no sea escuchar la conferencia. Nada más llegar intenté incluso comprar una entrada a cualquiera de los presentes. Todos pensaban que estaba loco. Yo insistía en que necesitaba los créditos que se daban, pero nada. Había muchos policías, y el colarme lo veía imposible. (…)

Había un enlace para seguir la conferencia. Me lo puse en el móvil con los cascos, al llegar tu parte, al saber que no había conseguido entrar, me levanté y arremetí contra una papelera. Esperé hasta una hora después de la conferencia, a ver si tenía la fortuna de encontrarte. Al no ver nada, me largué con un cabreo, y empecé con las amenazas vía Twitter hasta que vi tu correo. Sabía que el intentar abrir esa sala te daría ventaja. E incluso pensé que había un agente de policía por si acaso a algún loco se le ocurría esa idea. Podría haber acabado muerto yo, o podría haber acabado con el Tiger88 que había creado en mi mente. En ese momento estaba cegado de ira y rabia. Solo buscaba derramar sangre para sentirme a gusto conmigo mismo, para callar a mi cabeza.

Cuando Markos me escribió algo tan duro, le pregunté si seguía pensando igual. Le había hecho llegar mi libro a través de su camarada Estefanía y al leer *Diario de un skin* teóricamente se había dado cuenta de que su odio no estaba justificado:

Si ese día hubiera conseguido ponerte la navaja en el cuello, si hubiera llegado hasta el final, ¿qué habría sentido? En ese momento tranquilidad, ¿después? No lo sé, ¿que hubiera sido mi ruina? Sí, no habría vuelto a pisar la calle nunca más o a saber si ahí mismo un policía me hubiera abatido a tiros. ¿Mis camaradas? Los que saben la verdad pensarían que he sido un animal, que no lo debería haber hecho. Los que meten mierda a otros jóvenes dirían que les he quitado un peso de encima, un problema menos. Los que odian a Tiger88 como el que nos contaron pensarían que soy un héroe, pero todos ellos pensaría que sería una auténtica locura. Si al cabo de años me hubiera enterado, me habría arrepentido de condenar a una persona, de matar a una persona, inocente respecto a lo que tenía en la cabeza, pero si nunca me hubiera enterado, no me iba a arrepentir, eso también te lo digo.

Yo pertenezco a una familia humilde. Mi padre empezó a trabajar cuando era apenas un adolescente y no tuvo la oportunidad de completar sus estudios. Quizá por eso se esforzó tanto en que yo tuviese la formación que él no tuvo, y me inculcó desde muy niño la pasión por leer. Desde que me alcanza la memoria recuerdo a mi padre insistiéndome en un mensaje: «Sé lo que quieras, pero sé el mejor. Y seas lo que seas en la vida, por encima de todo sé buena persona. Si tus amigos están contigo por tu dinero, desaparecerán cuando se acabe, pero si están contigo porque te aprecian, los tendrás siempre».

Me falta mucho para llegar a ser buena persona, pero por alguna razón misteriosa la Providencia me ha obsequiado con el aprecio de quienes me rodean. No tengo palabras para agradecer la ingente cantidad de horas, esfuerzo y recursos que mis amigos invirtieron en identificar a MarkoSS88 desde aquella noche. No encuentro palabras en el diccionario para plasmar mi profunda gratitud. No tenían por qué hacerlo, nadie se lo pidió. Pero todos y cada uno de aquellos policías, desde sus respectivos conocimientos y

experiencia, dedicaron docenas y docenas de horas de su tiempo libre a rastrear las redes, a consultar los archivos, a interrogar fuentes, en busca de la verdadera identidad de Marcos Santos Navarro.

Sin embargo, todos le subestimamos. Su rastro nos obligaría a utilizar todo tipo de herramientas de hacking legal, a consultar a especialistas y a emplear a fondo la ingeniería social. Aunque cada nueva pista, cada nueva línea de trabajo, nos condujese, una y otra vez, a un callejón sin salida…

Pero cometió un primer error: no conocía mi tozudez. Yo no termino una investigación hasta que llego al final. Y ahora la investigación lo incluía a él.

Capítulo 7
Los *whitehats* de la Guardia Civil

«El Guardia Civil no debe ser temido sino de los malhechores, ni temible sino a los enemigos del orden. Procurará ser siempre un pronóstico feliz para el afligido, y que a su presentación, el que se creía cercado de asesinos se vea libre de ellos; el que tenía su casa presa de las llamas considere el incendio apagado; el que veía a su hijo arrastrado por la corriente de las aguas lo crea salvado; y por último, siempre debe velar por la propiedad y seguridad de todos.»

Duque de Ahumada, La Cartilla del Guardia Civil, artículo 6

En el GDT del capitán Lorenzana

Las nuevas instalaciones de la prestigiosa Unidad Central Operativa (UCO) de la Guardia Civil se encuentran en la calle Salinas del Rosio, muy cerca del aeropuerto de Barajas y un tiro de piedra del Club House de mis antiguos «compañeros» del MC, los Ángeles del Infierno. Sin embargo, el capitán me citó en el cercano Centro Comercial Plenilunio. Días atrás, Israel Córdoba me lo había presentado formalmente. Se conocían bien; de hecho, fue César Lorenzana quien bautizó a Israel como *business hacker*.

Durante la comida que compartimos los tres en un restaurante situado peligrosamente cerca del Club House del capítulo Madrid de los Ángeles del Infierno, charlamos sobre diferentes aspectos de la investigación policial del cibercrimen, y expresé mi interés por conocer por dentro las instalaciones del Grupo de Delitos Telemáticos de la UCO, el centro neurálgico de la lucha contra el cibercrimen por parte de la Benemérita. Pero tenía un problema. No quería identificarme en la entrada ni llamar la atención en el arco de metales. Y si tenía que atravesar el control de acceso al edificio, cargado de cámaras, grabadoras y demás «herramientas», iba a dar mucho el cante. Tampoco quería que quedase ningún registro de mi visita al edificio. Y el capitán supo comprender mis particulares circunstancias y obró en consecuencia.

Llegué al Plenilunio media hora antes de la prevista. Busqué un lugar discreto para dejar la moto y saqué la tablet para repasar por enésima vez la historia del Grupo de Delitos Telemáticos (GDT) de la Guardia Civil. La red está llena de referencias a los «pata negra» de la lucha contra el cibercrimen. En la página web oficial de la Guardia Civil, y con la característica redacción sobria e institucional del instituto armado, encontramos su historia oficial:

> El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos actos delictivos que se cometen a través de sistemas de telecomunicaciones y mediante las tecnologías de la información. En 1996, cuando las investigaciones sobre delitos informáticos empezaron a adquirir especial relevancia, se vio la necesidad de crear un Grupo específicamente destinado a perseguir esta clase de delincuencia constituido por agentes que unieran a su preparación en investigación criminal una buena formación informática.
>
> A mediados de 1999, dado que el campo de actuación se había ampliado a los fraudes en el sector de las telecomunicaciones, se adoptó una terminología más en consonancia con la realidad, pasando a llamarse Departamento de Delitos de Alta Tecnología (DDAT).[57]

Institucional. Formal. Aburrido… Para conocer mejor la actividad de los «hackers de la Guardia Civil» resulta más interesante explorar su dinámica presencia en las redes sociales. El GDT tiene más de 130.000 seguidores en Twitter y un número similar de «me gusta» en su página de Facebook.[58] Incluso, y junto con los demás grupos de la UCO, cuentan con su propio club de fans en http://clubdefansuco.es.

No es extraño. La incansable labor pública de sus principales caras visibles —el entonces capitán César Lorenzana y el cabo Javier Rodríguez— ha conseguido

ganarse el respeto y el cariño de la comunidad hacker. Solo hay que buscar un poco en portales como YouTube o iVoox para encontrar grabaciones de sus incontables participaciones en programas o eventos de hacking y seguridad informática. Así, año tras año, guardias civiles y hackers, durante tanto tiempo considerados adversarios a un lado y otro de la ley, hoy son compañeros de estudio. «Tradicionalmente nos habíamos visto como enemigos. Ellos nos perseguían. César me decía que no fuera malo y esas cosas, pero (ahora) estamos aquí colaborando y haciendo que tengamos comunidad de seguridad.» Con estas palabras Román Ramírez presentaba a Lorenzana y Rodríguez durante su intervención en la Rooted-2014,[59] reflejando perfectamente, y en apenas un par de frases, lo que ha sido la evolución del GDT dentro de la comunidad hacker. Una actitud muy inteligente, porque el GDT ha sabido canalizar el talento de muchos de esos nuevos exploradores de la red, para convertirlos en sus aliados contra el cibercrimen.

El claxon del coche del capitán Lorenzana me sacó de mis pensamientos, y del vídeo de su conferencia en la Rooted. Tiré el casco y la mochila en el asiento de atrás y me senté a su lado.

—Buenos días, César. Y gracias por recogerme.

—Es mejor así. Si no conoces el camino, llegar al edificio es un poco lioso. Y además, así entramos directamente por el parking.

Desde agosto de 2007, el capitán César Lorenzana González es el jefe de la Sección de Investigación del GDT de la UCO, además de ser su representante en las reuniones trimestrales de trabajo de Interpol, Europol, Counceil of Europe, G-8, etcétera. Sin embargo, su trabajo contra el delito no siempre se circunscribió a las redes informáticas. Al contrario. César se curtió como policía en las unidades de Inteligencia de la Guardia Civil, luchando contra ETA en el País Vasco y participando en numerosas operaciones contra la banda terrorista. Probablemente por eso le gusta dejar claro que, tras de la investigación tecnológica, llega el turno del trabajo policial convencional, que va más allá de lo que puede hacer un simple hacker.

Entramos en el edificio de la UCO por el sótano, tras pasar los controles del parking subterráneo, donde César mostró su acreditación y la del vehículo. Yo mantuve cara de póquer, intentando parecer «de la familia» y no un detenido, y accedimos sin preguntas ni interrogatorios a la base de operaciones de la unidad más legendaria y prestigiosa de la Guardia Civil.

Desde el parking subimos a la tercera planta. Saliendo del ascensor, a la derecha, se encuentran las instalaciones del GDT. A la izquierda, una enorme sala llena de ordenadores. El cerebro electrónico del grupo. Una veintena de funcionarios de «ciberpolicía» cuya jurisdicción va más allá de una demarcación territorial. Reconocí a algunos de los más respetados por la comunidad hacker, como Sergio, Fran, Javi o el alférez Mario Farnós. Y por supuesto, allí estaba Ángel Pablo Avilés, «Angelucho». A varios de ellos ya los conocía de eventos como X1Red+Segura. Yo sabía quiénes eran, pero ellos no sabían quién era yo. En los encuentros de hackers

siempre me presenté como Toni, un recién llegado al fascinante mundo de la seguridad informática sin nada destacable que contar. Uno más entre los miles de asistentes a esos eventos. Y prefería que así continuase.

—¿Quieres que te los presente?

—Gracias, pero mejor no. Cuanta menos gente sepa quién soy, mejor.

A la derecha de la sala de operaciones, un pequeño almacén, y a su lado el despacho que comparten el capitán Lorenzana y el comandante Óscar de la Cruz Yagüe, jefe del grupo. Allí nos parapetamos para poder charlar con un poco de tranquilidad.

—En la web dice que el grupo se fundó en 1996… ¿En serio? ¿Tan pronto?

—Sí. Lo fundó el teniente Anselmo del Moral.

En internet todavía puede localizarse alguna entrevista histórica de aquella época al teniente Del Moral, incuestionable visionario precursor del trabajo policial en la red.[60]

—¿Y cuántos sois?

—Aquí en la UCO, ahora mismo unos veintitrés o veinticuatro. Pero en cada provincia hay equipos de investigación territoriales, que suelen ser tres o cuatro por provincia.

—No me parece mucho, porque vuestra área de trabajo no será territorial… Internet es todo. ¿Cuál se supone que es el criterio para delimitar vuestra jurisdicción?

—A nivel judicial hay varios criterios a elegir. A nosotros se nos aplica el origen de la víctima. Si la víctima está en Madrid, se supone que es competencia de Madrid; se supone… porque si el autor está en Barcelona, a ver quién se lo queda… También es una historia muy curiosa esto de cómo se reparten las cosas.

Sobre la mesa del despacho, al lado de un montón de expedientes e informes, había una estatua de bronce de un guardia civil a caballo. Así patrullaban por montes y caminos en sus orígenes, a la caza de bandoleros. Ahora los agentes de la UCO patrullan la red en busca de cibercriminales, a través de programas informáticos. Y como ocurría en los caminos, a veces se topan con otros servicios que pujan por ser los primeros en detener al bandolero.

—En temas de terrorismo, crimen organizado… sé que a veces existe rivalidad, no ya entre distintos servicios, sino incluso dentro de la misma «casa», pero en esto…

—Bueno, si es terrorismo, tráfico de drogas o blanqueo de capitales es competencia exclusiva de la Audiencia Nacional. Cibercrimen… ah… jurisdicción ordinaria. Esto implica que tienes que ir a un juzgado, tú presentas el tema y él reparte.

—Corrígeme si me equivoco, pero básicamente vosotros tenéis cuatro áreas de trabajo, ¿no?

Antes de responder, el capitán Lorenzana tomó un dossier de uno de los cajones de su mesa y me lo entregó. Era el «Dossier de servicios y capacidades del GDT», un

documento interno de cinco páginas en el que se reportaba a la Jefatura las características, operaciones y capacidades del Grupo de Delitos Telemáticos de la UCO. En él se detallaban todos los servicios realizados por el grupo durante 2013 (con 4.150 actuaciones) y lo que llevábamos de 2014 (3.172 hasta ese instante).

La Carta de Servicios del GDT, a fecha de octubre de 2014, especificaba que dicho grupo asumía tareas de investigación, atención al ciudadano, formación y representación institucional. Pero también como Policía Administrativa, ciberseguridad (gestión de incidentes, I+D, auditorías, etcétera) y asesoramiento al Estado Mayor, Policía Judicial y demás.

—Lo que dice nuestra normativa que el GDT debe hacer es esto, pero con el paso del tiempo y como nos metemos en muchos charcos, andamos al 150% de rendimiento. Encima, con la estrategia de Ciberseguridad hay que participar en un montón de planes de trabajo… Durante mucho tiempo se planteó la necesidad de crecer, pero el cibercrimen no se veía como una prioridad, hasta 2013. Pero ahora que hay voluntad, nos pilló la crisis y no hay dinero.

—Sin embargo, aunque vosotros no podáis aumentar recursos, el cibercrimen sí aumenta…

—Yo no lo tengo muy claro. —El capitán me sorprendió con su respuesta—. No sé si el cibercrimen aumenta, o es que cada vez vemos más claro lo que hay. Poco a poco vamos viendo la foto completa de todo lo que está ocurriendo, porque hasta hace cinco años nadie hacía informes de esto.

—Te oí comentar una vez, y me pareció genial, que la pornografía infantil no existe…

—No, de hecho fuera de España no se le llama «pornografía», es abuso sexual infantil. Son violaciones de niños y bebés en toda regla. La pornografía tiene otras connotaciones.

Una vez más, no pude evitar el recuerdo de las cinco menores chiapatecas vírgenes que el narcotraficante Mario Torres me vendía, a 25.000 dólares cada una, para que las utilizase en mis ficticios burdeles.[61] Incluso aunque sus padres, humildes campesinos mexicanos, hubiesen accedido a la venta en la confianza de que sus hijas tuviesen un futuro mejor en Europa, aun pagando tan alto precio. Incluso aunque las niñas, de doce a catorce años, según Mario, aceptasen resignadas su suerte. Incluso aunque los puteros que requiriesen sus servicios insistiesen en que todas las partes habían asumido de manera voluntaria el pacto comercial… seguía siendo un delito. Con la llamada «pornografía infantil» ocurría lo mismo. Lorenzana tenía toda la razón.

Expulsé de mi mente la imagen de Torres estrechándome la mano para sellar el negocio mientras sonreía como un cerdo; esa imagen trae a mi imaginación reacciones inconfesables en una sede policial, y cambié de tema.

—¿Cuáles son vuestras mejores operaciones, o las que han tenido más repercusión?

—No es lo mismo. Una cosa son las que han tenido repercusión mediática y otra las que consideramos mejores. Te lo voy a enseñar…

Operaciones contra el cibercrimen

El capitán, con evidente y merecido orgullo, hizo desfilar ante mis ojos un sinfín de operaciones policiales desarrolladas por el GDT imposible de reproducir íntegramente. Algunas, de verdad espectaculares. Y lo que es más importante, un síntoma inequívoco de que Lorenzana y sus hombres patrullan la red sin descanso, a la caza de cibercriminales. Y los que se sienten seguros delinquiendo o atentando contra nuestra seguridad, detrás de un teclado, en la intimidad de sus casas, están equivocados. Esta es la prueba más evidente…

Me explicó cómo se había desarrollado la Operación Ronnie:

—Fue en 2003, el esclarecimiento del mayor ataque documentado de Denegación de Servicios Distribuidos (DDoS) a distintos servidores de internet, que afectó a más del 30% de los internautas españoles y a varios de los ISP de internet más importantes de España. —Los ataques DDoS o de denegación de servicio consisten en bombardear una web con miles de peticiones hasta colapsarla y hacerla caer de internet, y esa operación de la que hablaba Lorenzana fue un éxito rotundo—. Terminó con una condena contra S. G. «Ronnie», a dos años de prisión y una indemnización civil de 1.332.500 euros. La primera condena por un ataque DDoS en España.[62]

Hablamos de las operaciones Gala, Clon —«Difundía un troyano que podría haber afectado a más de 100.000 usuarios de internet en lengua castellana»—, Punto de Encuentro —«Una colaboración con policías de diecinueve países que logró desarticular una red internacional dedicada a la distribución de pornografía infantil a través de internet»—, Panzar, Cadena, Phesca, Azahar, Pampa, Global, Santiago…

—Esa fue la primera operación dirigida por el Servicio de Criminalidad Informática de la Fiscalía General del Estado, contra la distribución de pornografía infantil en la redes Edonkey y Ares del P2P —me dijo el capitán Lorenzana—. Para la ocasión se desarrolló un nuevo buscador, Nautilus, que ampliaba el campo de búsqueda a más redes.

Y había muchas más: Toco, Hispahack, Diablo y Basura, Faraón, Yanki, Piolín, Policarbonato, etcétera. Todas durante los primeros diez años de existencia del GDT. A partir de 2007, ya con la veteranía de una década cazando criminales en las redes, llegaron algunas de las más relevantes.

—En la Operación Mariposa se desmanteló la mayor red de ordenadores zombi a nivel mundial, en colaboración con el FBI americano, la policía eslovena y el sector privado. No solo conseguimos eliminar la red, sino identificar a sus administradores y los creadores del virus utilizado para infectar los ordenadores. Esa fue una de las operaciones más satisfactorias. Nos llamaban de fuera de España constantemente para pedirnos entrevistas, y aquí en España pasó desapercibida…

Sin duda, la Operación Mariposa ha sido uno de los mayores éxitos del GDT de la

Guardia Civil, que les valió un prestigio internacional, poco valorado en España. Pese a ello algunos medios nacionales, como el diario *El Mundo*, sí se hicieron eco.[63]

También estaban la Operación Santo —que logró identificar y detener a varias personas responsables de chantajear y amenazar al popular cantante español David Bisbal—,[64] y la Operación Calando —que en coordinación con agencias policiales de Reino Unido, Holanda, Estados Unidos, Brasil, Australia y Bélgica logró desarticular el foro de pedófilos www.boylover.net, uno de los más activos, e identificar a más de 30.000 usuarios—,[65] y otras como las operaciones Cordobés,[66] Pirulí,[67] Bamital, Magos…

—Esa fue curiosa: era una red organizada que utilizaba el timo del nigeriano para estafar sumas millonarias de dinero a empresarios extranjeros.[68] Logramos desarticularla. O la Operación Guardador, en la que se desarticuló una red de prostitución y corrupción de menores en la Comunidad de Madrid. Los adultos detenidos contactaban y captaban a sus víctimas a través de las redes sociales.[69]

El capitán Lorenzana me habló de una operación que llegaría a conocer bien, la Operación Onymous: una macrooperación contra la Deep Web, que se saldó con diecisiete detenidos en siete países (Reino Unido, Estados Unidos, España, Hungría, Suecia, Suiza e Irlanda) y el cierre de 410 dominios de servicios ocultos alojados en la red TOR en los que se ofrecía droga, armas, documentación falsa y hasta pornografía infantil. Entre ellos se encontraba el Silk Road 2.0, la web espejo que apareció en TOR tras la detención de Ross Ulbricht.[70]

De nuevo he de insistir. Hay muchas más: Telemensaje, Dragos, Bachiller, Espalda, Álamo, Smishing, etcétera. Sin duda el currículo y las referencias del GDT justifican la buena imagen de que goza la ciberpolicía española en el ámbito de la seguridad internacional.

—¿Y cómo hacéis para perseguir un delito —pregunté al capitán—, si todavía no está tipificado como tal? He escuchado al fiscal Jorge Bermúdez decir que este es uno de los grandes problemas de la ciberdelincuencia: que va más deprisa que la ley.

—Es muy complicado —coincidió—. Por ejemplo, cuando a un chaval le suplanta la identidad para abrir un perfil en Facebook o en Tuenti. Suplantar a alguien para abrir un Facebook no está tipificado como delito. Pero precisamente Jorge nos dio la solución: hackear la ley. La falsedad en documento mercantil sí es delito. Me explico. La suplantación de identidad en internet como tal no está regulado en el Código Penal, porque la usurpación de estado civil, que es el supuesto penal, habla de un acto jurídico formal, y publicar en Facebook no es jurídico y mucho menos formal. Pero al abrir una cuenta en un portal de servicios, que para ofrecer ese servicio me obliga a aceptar unas condiciones de uso que yo firmo… eso a efecto jurídico es un contrato. ¿Y qué estás haciendo? Firmando un contrato en nombre de otra persona. Eso es falsedad en documento mercantil… Entonces por ahí sí puedo meterle mano. Pero es una obra de ingeniería legislativa… Otra cosa por ejemplo, es

que te roben la cuenta de PayPal. Eso es como robarte la tarjeta de crédito. Eso es un fraude bancario y fraude económico. Es delito.

Es importante precisar que en el momento de producirse la entrevista, César Lorenzana todavía era capitán. Unos meses después ascendería a comandante. Y unos meses después, también, entraría en vigor la revisión del Código Penal que actualizaría los tipos penales aplicables a los delitos informáticos, tal y como publicó el Boletín Oficial del Estado.[71]

—Del tráfico de drogas tienes veinte o treinta artículos en el Código Penal, pero de delincuencia informática… Vamos usando cosas de artículos sueltos: 256, 197, 285, 530… El único delito informático como tal es la denegación de servicio, que ya está tipificado como tal, y el acceso no autorizado. Artículo 197.

—Imagino que la mayoría de usuarios creen que esto solo afecta a los bancos.

—No. En absoluto. Hay muchas formas de que alguien se haga con tu ordenador. Una son las RAT, que son herramientas de acceso remoto, *Remote Access Tool* en inglés. Yo controlo tu ordenador y puedo activar la cámara, activo el micro, registro tus pulsaciones, borro archivos… hago lo que quiera. Habitualmente lo que hacen es instalarte *keyloggers* o troyanos bancarios, que son bastante discretas. Una vez se instalan, están ahí durmiendo, monitorizando tu navegación, de tal manera que él tiene marcadas una serie de entidades financieras españolas. Cuando ve que tú en tu navegador estás accediendo a la web de uno de esos bancos, te roba las credenciales bancarias y accede a tu cuenta. Esto se diseñó originalmente para bancos, pero vale para PayPal, Hotmail, para todo. Otra forma de utilizar tu ordenador es incluirlo en una *botnet:* tu equipo pasa a formar parte de una red de ordenadores esclavos, es decir, hay una persona que tiene acceso a una red de un millón, dos millones, tres millones de ordenadores…

—¿Con esas cifras? ¿Tantos?

—Sí. De hecho, la más grande que se cazó, y donde participamos nosotros, la Operación Mariposa, eran unos 14 millones de IP únicas. Echando la cuenta eran unos 12 o 13 millones de ordenadores.

—Entiendo que eso se puede utilizar para un ataque de denegación de servicio, pero ¿para qué más pueden querer mi ordenador en una red zombi?

El capitán me hizo una seña con la cabeza para que me acercase. Rodeé la mesa del despacho y me situé detrás de él para tener una buena perspectiva del ordenador. Entonces abrió un PowerPoint que recogía una de sus presentaciones, en este caso en una reunión internacional de Policías europeas.

El documento suponía un viaje, profusamente ilustrado, a las entrañas del cibercrimen a través de todas sus etapas y en todas sus modalidades: *spamming*, *carding*, *phishing*, *herding*, espionaje industrial, etcétera. Fascinante.

Los ataques pueden realizarse por prestigio (y dinero), por venganza (y dinero), por satisfacción (y dinero) o por dinero (y más dinero). Lorenzana siempre insiste en este punto. Llama la atención de los usuarios de páginas que descargan películas o

libros piratas «gratis» sobre el hecho de que no hay nada de altruista, hacktivista o generosidad en esas páginas, sino de robo puro y duro, que supone grandes beneficios para el propietario de la web y perjuicios para los autores pirateados, como yo, con la colaboración necesaria de todos los usuarios. El fundador de Megaupload, por ejemplo, antes de ser detenido amasó una inmensa fortuna que lo convirtió en uno de los diez multimillonarios más ricos del mundo.

En una de las transparencias, que pasó de refilón, se mencionaban más de 12.000 ataques de denegación de servicio en una semana. Probablemente fueron más, ya que la mayoría no se denuncian. Me sorprendió lo elevado de la cifra, aunque me sorprendió más la estadística global del cibercrimen. Cada segundo, repito, *cada segundo* se producen 18 nuevas víctimas. 1,5 millones de víctimas al día. 567 millones de víctimas al año.

Aunque no nos demos cuenta. Aunque no seamos conscientes. Aunque nuestro ordenador continúe funcionando de maravilla. Incluso puede que mejor que antes (porque algunos virus funcionan como antivirus limpiando el ordenador y evitando que otros troyanos entren en un equipo que el cibercriminal quiere para él). Por la noche, mientras dormimos tan tranquilos, pensando que nuestro equipo solo está descargando ilegalmente programas, libros, películas o música del eMule, en realidad está formando parte de una red zombi *(botnet)*, que participa en un ataque a una entidad bancaria, está aumentando la reputación digital de un cliente de la mafia, o distribuyendo material a pedófilos… Desde que supe eso, apago el *router* cuando no lo utilizo, y el ordenador también. Y ya nunca lo dejo encendido por la noche.

Ante aquella avalancha de datos recordé de pronto las palabras de David R. Vidal cuando comencé esta investigación: «Tu ordenador está infectado, me apostaría el cuello». En opinión del agente Juan, la mayoría lo está, aunque no seamos conscientes de ello nunca. Al menos hasta que los agentes del GDT o la BIT del CNP llaman a nuestra puerta para ponernos los grilletes.

Cómo usa tu ordenador la industria del cibercrimen y cómo puedes ponérselo difícil

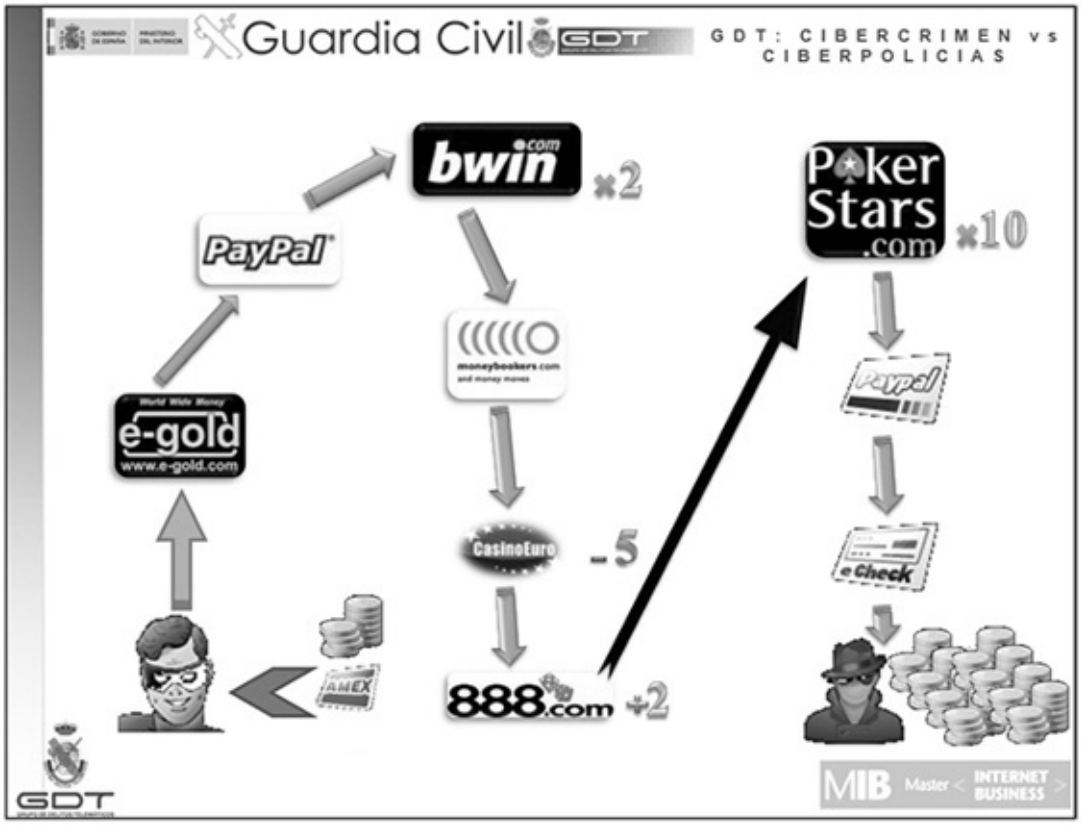
Por fin llegó al contenido que el capitán Lorenzana estaba buscando, y me explicó que los cibercriminales primero buscan cuentas de correo que estén operativas. Ese es uno de los muchos vectores de ataque para infectar nuestro ordenador. Un email que pide nuestra solidaridad para con las víctimas de una tragedia, una declaración de amor de una exuberante rusa, una supuesta herencia de un pariente lejano… Utilizan miles de técnicas. Pero no solo nos atacan por email. También lo hacen a través de Facebook o Twitter, de web previamente infectadas, de anuncios comerciales, etcétera.

Una vez introducido el «bicho» (virus), pueden controlar a distancia nuestro equipo, sin que nosotros seamos conscientes de que estamos «zombificados». Y lo peor es que el descubrimiento de un zombi no implica descubrir al máster, ni a otros zombis.[72]

—A partir de ese momento —me explicó el capitán—, el ciberdelincuente puede utilizar tu ordenador para muchas cosas: estafas, extorsión… incluso para el blanqueo de capitales. Cuando la gente piensa: «Pero quién me va a querer robar a mí el perfil de Facebook o de Tuenti», no piensa en esto.

Esta parte me pareció fascinante y más después de la charla que había tenido con Selva Orejón tiempo antes. Durante mi formación para la redacción de *Operación Princesa* realicé varios cursos sobre prevención del blanqueo de capitales, porque todos los investigadores saben que la mejor forma de lucha contra la corrupción o el crimen organizado es seguir el dinero. Pero en el ámbito del cibercrimen no es tan sencillo.

Apoyándose en una de las transparencias que utilizaba en las conferencias que impartía, Lorenzana me explicó varias de las estrategias de los ciberdelincuentes para borrar el rastro del dinero que nos han robado en la red. Toda una arquitectura.



El ciberdelincuente ha obtenido miles de euros con una campaña de fraude, pero el dinero aún está en la red, es rastreable. Así comienza a saltar de un soporte a otro, utilizando las comisiones de páginas como E-Gold, PayPal o Bwin para ir diluyendo el rastro. Utiliza las credenciales que ha robado a Pepito, Juanito o Antoñito para hacer esas transacciones, de tal forma que cuando la Policía siga el rastro, se encontrará con que ha sido Juanito quien envió un dinero a Antoñito, que había recibido de Pepito, mientras los tres duermen plácidamente con el ordenador encendido toda la noche, pensando que solo están descargando ilegalmente de Torrent el último disco de Alejandro Sanz, o el último libro de Vargas Llosa…

Después, usando esas mismas identidades robadas, el dinero pasa por casinos *online*, donde Antoñito (o sea yo) hace unas apuestas muy altas, para que Pepito (o sea tú) las gane, dejando un porcentaje al casino, pero sacando el dinero restante debidamente aseado.

Más tarde, una legión de «mulas» —esos incautos que han recibido un email en el que una prestigiosa empresa informática les ofrece el trabajo de su vida con una comisión estupenda a cambio de «solo» recibir una suma de dinero en su cuenta, sacarla y enviarla a otra dirección a través de MoneyGram, Western Union, o cualquier otra empresa similar— termina el recorrido. El dinero se transfiere a oficinas de otros países, donde lo retiran en efectivo. Y el único rastro que ha dejado es el nuestro. Cuando unas semanas después César Lorenzana llame a nuestra puerta, o a la tuya, pondremos cara de sorpresa, proclamaremos nuestra inocencia, argumentaremos que nosotros solo pirateamos películas, libros o música, pero las huellas «digitales» de nuestro equipo estarán por toda la escena del crimen…

—¿Y todo esto es aplicable al teléfono? Quiero decir, muchos chicos jóvenes ya están pasando de sus ordenadores y llevando toda su vida digital a través del móvil.

—Totalmente. El teléfono ya se utiliza para todo menos para hablar por teléfono, y la gente no es consciente de que es un ordenador. Tú pregunta cuánta gente tiene un antivirus en el ordenador y cuántos lo tienen en el móvil… Mucha gente tapa la cámara del ordenador, pero ¿cuánta tapa la del móvil?

De repente sentí una sensación incómoda. Nunca se me había ocurrido. Presumo de ser bastante razonable, y me preocupo mucho por tomar todas las medidas que nos aconsejan a los testigos protegidos, pero nadie me había hablado nunca de estas brechas digitales en nuestra seguridad. Estaba a punto de recibir un montón de consejos e información útil sobre el uso seguro de la red, que todos, testigos protegidos o no, deberíamos tener en cuenta.

—Toni, lo primero que tienes que aprender es a cifrar tus comunicaciones. Yo te recomiendo el PGP. Es un programa de encriptado que combina técnicas de criptografía métrica y asimétrica muy sólidas, y es gratis.

El PGP es un software de cifrado, firma y autenticación desarrollado por Phil Zimmermann en 1991, y el hecho de que veinticinco años más tarde profesionales de la seguridad como el capitán Lorenzana continúen utilizándolo acredita su eficiencia.

—Cualquier documento, cualquier imagen, al final no es más que una colección de 1 y 0. Hay funciones que sirven para comprobar la integridad del fichero, es decir, saber que no se ha modificado. Se trata de un algoritmo matemático que va cogiendo trozos del archivo, va haciendo una serie de operaciones matemáticas con ellos y al final te genera otro bloque numérico que es, por decirlo así, el resumen del archivo. De tal manera que solo cambiando un 1 o un 0 del archivo original, esto provoca que el resumen que yo tengo se modifique más de un 50%. Es decir, lo que generas no tiene nada que ver con lo que había de antemano…

El capitán me hizo una demostración. Un pequeño texto, de apenas un par de palabras, una vez sometido al PGP se convertía en un inmenso galimatías con cientos de caracteres entremezclados, absolutamente indescifrable.

—Tú te generas las claves de usuario y le dices: quiero cifrar esto… —mientras hablaba, Lorenzana me señalaba los pasos en la pantalla— y generas una contraseña segura, de veinte o treinta caracteres…

—¿Cómo que treinta caracteres? —no pude evitar interrumpirle—. Pero ¿cómo vas a recordar una contraseña de treinta caracteres? Es imposible.

—Qué va, es fácil. Por ejemplo, pones una frase tipo: «soypepitoyestoyescribiendounlibro» y ya tienes más de treinta. Y si cambias las oes por ceros, y las íes por unos, ya estás combinando caracteres alfanuméricos. Si además incluyes algún punto o coma, ya tienes una contraseña infinitamente más sólida: «s0ypep1to;yest01escr1b1end0unl1br0». Ahí tienes una contraseña muy sencilla de recordar y muchísimo más segura.

César tenía razón. A veces las soluciones más sencillas son las más eficientes,

pero nunca se me había ocurrido que fuese tan simple obtener una contraseña segura, combinando caracteres alfanuméricos, y fácil de recordar. Recordé una frase genial de Chris Pirillo que había leído en algún sitio: «Las contraseñas son como la ropa interior. No puedes dejar que nadie la vea, debes cambiarla regularmente y no debes compartirla con extraños». Imposible decirlo más claro.

Una de las formas más utilizada para romper una contraseña y acceder a una cuenta de correo, o a un perfil social ajeno, son los «ataques de fuerza bruta» o «ataques de diccionario». Los ciberdelincuentes utilizan programas informáticos que se conectan a la página y realizan millones de combinaciones basándose en diccionarios que incluyen todas las palabras en el idioma de la víctima, hasta que dan con la contraseña. Por eso es tan importante utilizar combinaciones de letras, números y signos. Así nuestra contraseña resistirá un «ataque de diccionario».

Durante los siguientes minutos, Lorenzana me explicó el funcionamiento del programa de cifrado, y otras medidas de seguridad básica para la navegación en la red. Sin embargo, me lo dejó muy claro:

—PGP significa *Pretty Good Privacy,* es decir, privacidad bastante buena. Bastante, no total. La seguridad total no existe en internet, y quien te diga lo contrario te miente… Ya venden procesadores, sobre todo con tarjetas gráficas que tienen una mayor velocidad de cálculo, capaces de probar 15 o 20 millones de contraseñas por segundo. Si el espectro que tengo que barrer son 45 millones de posibilidades, tardo 3 segundos en sacarla.

—¿Y las redes sociales? ¿Te he oído comentar alguna vez que Tuenti es la más segura?

—Desde mi punto de vista es la que más se preocupa por la privacidad del usuario. Por ejemplo, Tuenti no indexa perfiles en internet. O sea, tú no puedes saber si yo estoy en Tuenti…

El capitán Lorenzana abrió el buscador de Google y tecleó su nombre seguido de la palabra Facebook.

—¿Ves? Te salen los perfiles de Facebook. Si cambio esto, y pongo, por ejemplo, César Lorenzana Linkedin… Ahí lo tienes. Mi perfil de Linkedin. Pero si ahora borro Linkedin y pongo Tuenti… ¿Lo ves? Aparecen resultados con mi nombre, pero ninguno es mi perfil de Tuenti.

—¿Y tienes un perfil en Tuenti?

—Sí, claro. Pero Tuenti no indexa perfiles en internet. La comunidad está bloqueada y nada sale al exterior. Es decir tú no puedes saber si yo estoy en Tuenti a menos que tú también estés, y entonces ya estás sometido a la política de protección de la red. Además, hasta hace poco, la forma de acceder a Tuenti era por invitación, así que si hacías algo ya eras inmediatamente rastreable.

—Y siempre antivirus…

—Siempre. Pagado o gratuito, pero no pirata. No te garantiza la seguridad, pero ayuda. Es como el cinturón en el coche. Si tienes un accidente a 190, te vas a matar,

pero si es a 90 igual te salva… Si además llevas airbag, vas más protegido. Si además tienes airbag lateral, más protegido… El antivirus te protege de muchas cosas, pero no de todo.

El capitán señaló varios iconos en su pantalla del ordenador.

—Yo tengo varios, ¿ves? Uno que monitoriza los servicios y procesos que corren el sistema operativo (EMMET o WinMHR) y un cortafuegos personalizado que permite bloquear o aceptar cualquier intento de conexión del PC (Little Snitch o HandsOff).

Entonces me percaté de que la webcam de su portátil no estaba tapada con trozo de adhesivo o celo, como había visto en todos los demás hacker que había conocido. Y expresé mi sorpresa:

—Pero se te ha olvidado tapar la cam…

El capitán sonrió compasivamente. Estaba claro que mi comentario era una absoluta estupidez.

—No, no se me ha olvidado. Precisamente ayer estuve discutiendo sobre esto y a mí es que me da igual… En teoría, cuando la cámara se activa, se enciende este LED, y evitar que se active este LED es muy complicado porque ya va con el *firmware* de la cámara y una serie de cosas que no son fáciles de evitar. Así que si alguien se lo curra tanto que consigue hacerlo, se merece ver mi careto… Otra cosa es que yo tenga el ordenador en mi habitación, enfocando a mi cama.

Poco tiempo antes, Chema Alonso «el Maligno» había dedicado una entrada de su imprescindible blog al tema del LED de las webcam, desaconsejando fiarse demasiado de él.[73] A menos que, como el caso del capitán, no te importase que te viesen trabajando en tu despacho.

—A eso me refería. Supongo que habéis recibido denuncias de chicas a las que han grabado con sus propias webcam.

—Sí, claro. Mi ordenador tiene LED, pero otros no. Y los teléfonos móviles tampoco.

—¿También te pueden activar la cámara del teléfono?

—Naturalmente. El teléfono es un pequeño ordenador. Ni más ni menos.

Instintivamente volví a mirar mi propio teléfono, situado sobre la mesa del capitán, y sentí vértigo al pensar que alguien pudiese estar observando mis movimientos cada vez que miraba la pantalla para teclear un número o escribir un sms…

Continuamos repasando, una por una, todas las recomendaciones de seguridad que el GDT incluye en su página,[74] recomendables para todos los usuarios. Algunas ya las había visto en detalle con Israel o con Selva. Otras eran nuevas:

- Elija contraseñas seguras y diferentes para cada servicio de internet.
- Verifique regularmente los movimientos de su cuenta bancaria.
- Utilice un antivirus con licencia y actualizado, e instale un firewall.
- Desconfíe de los mensajes cortos y extraños que pueda recibir por redes sociales, sobre todo si

incluyen un enlace para acceder a otro contenido.

- No piense que es inmune al software malicioso porque utilice un determinado sistema operativo o un dispositivo portátil.
- No confíe ciegamente en las aplicaciones de seguridad instaladas, estas no reemplazan a la navegación responsable ni a la prudencia del usuario.
- Si dispone de un *router* inalámbrico para conectarse a internet, cambie las contraseñas por defecto y establezca una más segura.

—Vale, César —le dije al final—. Entiendo que esto te da una protección básica, pero solo si eres un pececillo en un banco de peces, y unas redes de arrastre están buscando por internet pillar ordenadores en masa para zombificarlos… En mi caso, soy consciente de que me he hecho muchos enemigos y puedo ser objeto de ataques personales dirigidos exclusivamente contra mí… Desde que empecé a gestionar la web de Carlos el Chacal, cogí la costumbre de acudir a cibercafés para hacer cualquier cosa en internet. ¿Eso es una buena protección?

—Evidentemente, si te mandan virus o troyanos, ahí se quedan. Es otra capa más. Todo eso de que el mejor antivirus eres tú, el sentido común, etcétera, te vale cuando buscan pillar credenciales, robar información aleatoriamente… pero cuando van a por ti, olvídate. Ni sentido común, ni antivirus. Tienes un problema serio, dependiendo de los conocimientos del técnico que vaya a por ti. Si tiene tiempo y dedicación… Pero espera, hay otra cosa que te puede ser útil. Mira, esto es un sistema operativo en un *pendrive*. Esto te lo llevas en el bolsillo y cuando enciendes el ordenador en el cíber o donde sea, lo arrancas desde este *pendrive* y no estás utilizando el ordenador, ni te puede entrar ningún bicho…

El capitán me enseñó a llevar un sistema operativo en un *pendrive*. A utilizar ordenadores virtuales en el ordenador anfitrión, y otras medidas de seguridad. César está infectado, no puede evitarlo. Infectado por otro tipo de virus. El mismo que detecté corriendo por las venas de otros profesionales de la seguridad informática, hackers y auditores de seguridad. Como Román, David, Chus, Israel… El virus de la pasión. Pueden tirarse horas y horas ante los ordenadores, o hablando de ellos, sin ser conscientes del paso del tiempo. Lo sé porque lo he vivido con ellos. Se les olvida comer, cenar, dormir… Esas máquinas, esos programas de software, de alguna manera se les incrustan en el cerebro, los seducen, los embriagan, los abstraen del mundo, les hacen perder totalmente la noción del tiempo. Algo que no siempre comprenden ni sus familias, ni nadie que no comparta su pasión por los ordenadores.

Después de varias horas en su despacho, de pronto nos dimos cuenta de que todos sus compañeros se habían marchado ya. Solo quedábamos nosotros.

Me sentí mal. César Lorenzana tiene una agenda muy apretada, y yo le había robado más tiempo del previsto. Sin embargo, no me hizo ningún reproche. Ahora que estábamos solos, incluso se brindó a hacerme un recorrido por las instalaciones. El capitán estaba orgulloso de su grupo, y yo, como periodista, tan agradecido como encantado con el tour.

Seguí al capitán Lorenzana por los diferentes despachos, cuartos de servidores,

archivos y demás del Grupo de Delitos Telemáticos de la UCO, hasta llegar al «cerebro» de la unidad. Una sala muy amplia en la que, a mi llegada, sus compañeros de grupo exploraban la red a la caza de los ciberdelincuentes. En una de las paredes, colgada bajo una metopa con el logotipo del GDT, una máscara de Guy Fawkes[75] y un pañuelo palestino. Supuse que incautados en alguna operación contra algún grupo hacktivista. Justo en el otro extremo de la sala, dos grandes monitores colgados de la pared en los que podían monitorizarse todos los ciberataques que se estaban produciendo en el mundo, en tiempo real, a través de páginas como hp.ipviking.com, que nos permiten ver los ataques por país emisor o receptor, tipo de ataque, distribución horaria y otras variables.

No hay ni un solo segundo de inactividad. Los ataques masivos, por ejemplo de denegación de servicio, resultan espectaculares. Y las líneas que salen desde China o Rusia hacia los Estados Unidos, o desde los Estados Unidos hacia Siria o Irak nos permiten imaginar operaciones de ciberespionaje contra el ISIS, envíos de troyanos, misiones secretas…

Pero más allá de la estética, el colorido y la vistosidad, esas páginas nos ayudan a hacernos una pequeña idea de las dimensiones épicas del problema al que se enfrentan los ciberpolicías.

Antes de abandonar el edificio aproveché para saludar a una buena amiga. La agente Luca, protagonista de *Operación Princesa*, todavía está destinada en esas mismas instalaciones, aunque en otro grupo.

Al regresar al Plenilunio, lo primero que hice fue abrir el portaherramientas de mi moto. Saqué el rollo de cinta aislante, corté un trozo pequeñito y lo pegué sobre la cámara del teléfono. El capitán me había contagiado la paranoia hacker.

A partir de ese día intenté utilizar el protocolo de cifrado PGP, pero me vi incapaz. Los pasos que debía seguir para cifrar un simple saludo me parecieron tan tediosos que pronto tiré la toalla… Falta de motivación.

Cometí exactamente el mismo error que el periodista Glenn Greenwald cuando Edward Snowden contactó por primera vez con él y le pidió que utilizase el PGP para revelarle una información de vital trascendencia. Greenwald no le creyó y dejó pasar la exclusiva, hasta que meses más tarde no tuvo más remedio que esforzarse y aprender a utilizar el protocolo de cifrado para no quedarse descolgado del bombazo periodístico del 2013.

A mí me ocurriría algo parecido. Unos meses más tarde surgiría la posibilidad de conocer a un veterano hacktivista, y presenciar cómo hackeaba un satélite… pero para eso tendría que aprender a utilizar el PGP. El hacktivista no estaba dispuesto a comunicarse conmigo de ninguna otra manera.

OCTUBRE-NOVIEMBRE DE 2014
MARKOSS88: UN PRESO POLÍTICO

> «¿Cómo puede explicarse que la Iglesia jamás excomulgara ni a Hitler ni a Himmler, que Pío XII nunca viera necesario —por no decir indispensable— condenar Auschwitz y Treblinka, que una gran proporción de los miembros de las SS fuesen creyentes y permaneciesen fieles a sus lazos cristianos hasta el fin, que hubiese asesinos que practicasen [el sacramento de] la confesión entre una masacre y otra y que todos ellos procediesen de familias cristianas y hubiesen recibido una educación cristiana?»
>
> Elie Wiesel, *A Jew Today*

Mi primer impulso para intentar averiguar más sobre MarkoSS88 fue acudir a los expertos en el movimiento neonazi, así que me puse en contacto con Esteban Ibarra, presidente del Movimiento contra la Intolerancia, y David Docal, director del CEIDIV.

El doctor Docal es un viejo amigo. En diciembre de 2010 tuve el honor de asistir a su defensa de tesis doctoral en la Universidad Rey Juan Carlos de Madrid: «Tribus urbanas y participación política». Y estoy en condiciones de afirmar que, junto con Esteban Ibarra, es la voz más autorizada en el país para opinar sobre el fenómeno de las bandas juveniles y tribus urbanas. Y muy especialmente, los movimientos ultras. Para entonces, David y otros amigos comunes acababan de poner en marcha su proyecto más ambicioso: el Centro de Estudios e Iniciativas sobre Discriminación y Violencia (CEIDIV). De hecho, el CEIDIV ha realizado investigaciones absolutamente novedosas y originales sobre los grupos violentos. Una de las más notables fue la compilación de los «símbolos del odio» utilizados por los grupos neonazis en España.

Los nazis españoles saben que la exhibición de símbolos tan evidentes como la esvástica está prohibida en casi toda Europa. Por eso en sus actos políticos, deportivos o culturales han aprendido a utilizar emblemas, logotipos y símbolos menos conocidos por el gran público, y que suelen pasar desapercibidos a las autoridades. Banderas, pancartas y camisetas con runas germánicas, cruces célticas, emblemas de las SS, etcétera, exhibidos impunemente en campos de fútbol, manifestaciones políticas o conciertos de «música patriótica».

Por esa razón los investigadores del CEIDIV rastrearon durante meses los «territorios ultras» en torno a los estadios, visitaron sus locales de reunión, controlaron sus publicaciones en internet… y realizaron la mayor compilación de símbolos usados por los grupos neonazis españoles, explicando el origen histórico y significado de cada uno de ellos, incluyendo

los acrónimos y guarismos más utilizados por la propaganda del odio. Ese estudio forma parte del manual *Odio en las calles: violencia urbana,* la mejor compilación publicada hasta la fecha sobre los grupos violentos en las ciudades españolas.[76]

—Nuestro objetivo —me explica Docal— es crear una asignatura troncal, de seis créditos ECTS, en carreras universitarias como Psicología, Sociología, Ciencias Políticas, Derecho, Magisterio y todas las que tratan las ciencias jurídicas y sociales. Hay que tener en cuenta que nuestro trabajo todavía es lento, ya que nos dedicamos a esto desinteresadamente, por vocación, y que recibimos a diario, a través de nuestro correo,[77] nuevas informaciones sobre las actuales tendencias en los grupos de odio.

—Hace más de diez años yo utilicé canales del IRC Hispano y chats para infiltrarme en grupos de extrema derecha y extrema izquierda… ¿Cómo ha evolucionado la presencia de los grupos violentos en la red en el siglo XXI?

—Las redes sociales se han convertido en el escaparate de la sociedad, y lo que a nosotros nos llama la atención es que no hay una franja de edad determinada para participar en determinados grupos en la red. Nos encontramos desde niños de catorce años hasta personas con sesenta, con acceso al discurso racista y violento. Antes, cuando tú estabas introduciéndote en el mundo nacionalsocialista, los chat de IRC eran el vehículo. Se amenazaban los grupos pero pocas de esas amenazas se llevaban a cabo. Actualmente Twitter, Facebook, Tuenti y la red social Ask se han convertido en el vehículo donde aficionados de equipos, o grupos contrarios por ideología, se amenazan, insultan y se citan para dirimir sus diferencias con violencia. Y ahora sí lo llevan a cabo.

Las palabras de David Docal resultaron proféticas. Poco tiempo después, el 30 de noviembre de 2014, Francisco Javier Romero Taboada, alias «Jimmy», un aficionado del Deportivo de La Coruña de cuarenta y tres años, falleció durante un enfrentamiento entre los ultras del Riazor Blues y el Frente Atlético, que se había convocado a través de internet. Jimmy estaba casado y tenía un hijo.

—En la red difunden los discursos del odio al diferente —prosigue Docal —, buscan fuentes de financiación, anuncian sus actividades, se retroalimentan de sus acciones, cuelgan vídeos de las agresiones que protagonizan; en definitiva, la red es una sociedad paralela. Lo que hay que hacer, insisto, es educar en valores.

Una vez más, las apreciaciones de Docal resultaron premonitorias. Al poco, en mayo de 2015, hacktivistas negacionistas del holocausto atacaron la web del campo de concentración de Mauthausen, sustituyendo las imágenes de las doscientas mil víctimas que murieron en él por fotos de abusos sexuales a menores (lo que otros llaman pornografía infantil). La

ministra austriaca de Interior, Johanna Mikl-Leitner, calificó el ataque como «enfermo, criminal y profundamente aborrecible». Yo creo que se quedó corta. Pero lo importante es que dicho ataque revelaba que el hacktivismo no se limita a la extrema izquierda: los cibernazis tienen la misma formación e idéntica motivación, y no se caracterizan por sus «valores democráticos».[78]

—Pero otro de los escenarios que a nosotros nos preocupa es la música que escuchan las personas que se identifican con grupos violentos, porque ahí está el discurso del odio que cala entre los más jóvenes. La música es el conductor de este mensaje del odio. Toni, tú lo sabes.

El director del CEIDIV aludía a un capítulo sobre la música del odio, incluido en mi libro *Diario de un skin,* en el que intentaba analizar, ya en 2003, el papel de la música «patriótica» en la transmisión de la ideología neonazi entre los más jóvenes.

—Te voy a ser sincero, David, pero por favor sé discreto —afronté al fin el tema que me había llevado a verle—. Estoy intentando averiguar todo lo posible sobre un cibernazi en concreto, un tal MarkoSS88… ¿Has oído hablar de él en vuestros análisis y rastreos por la red?

—Sí, claro —respondió—. Aunque es alguien al que se conoce únicamente por el nick. Nadie lo ha visto, nadie sabe cómo es. Es activo en las redes sociales relacionadas con los ultras violentos del fútbol español. Tenemos varias teorías sobre él, pero aún no tenemos una línea clara. Ven, te enseñaré algo…

David abrió su ordenador y me mostró el blog de MarkoSS88. Mientras buscaba una entrada en concreto me preguntó:

—¿Sabes quién es Leire Díez?

—No.

—Es una concejala socialista de Cantabria. Teniente de alcalde en Vega de Pas y muy activa en las redes. Twitter, Linkedin, ya sabes. Incluso tiene un blog personal: «Sin Perder el Norte».

—¿Y? No entiendo dónde quieres llegar.

—Ya lo tengo. —Por fin había localizado la entrada que estaba buscando en el blog de Markos. El post se titulaba: «No hay perdón, ni por su cargo ni por su retraso», y estaba subido el martes 10 de septiembre de 2013.

En su entrada, Markos arremetía contra la concejala socialista, dedicándole todo tipo de lindezas, y reproduciendo una discusión que ambos habían mantenido en su cuenta de Twitter (@leirediezpas) y que terminó con la amenaza de la teniente de alcalde de denunciar también a Markos si continuaba increpándola.

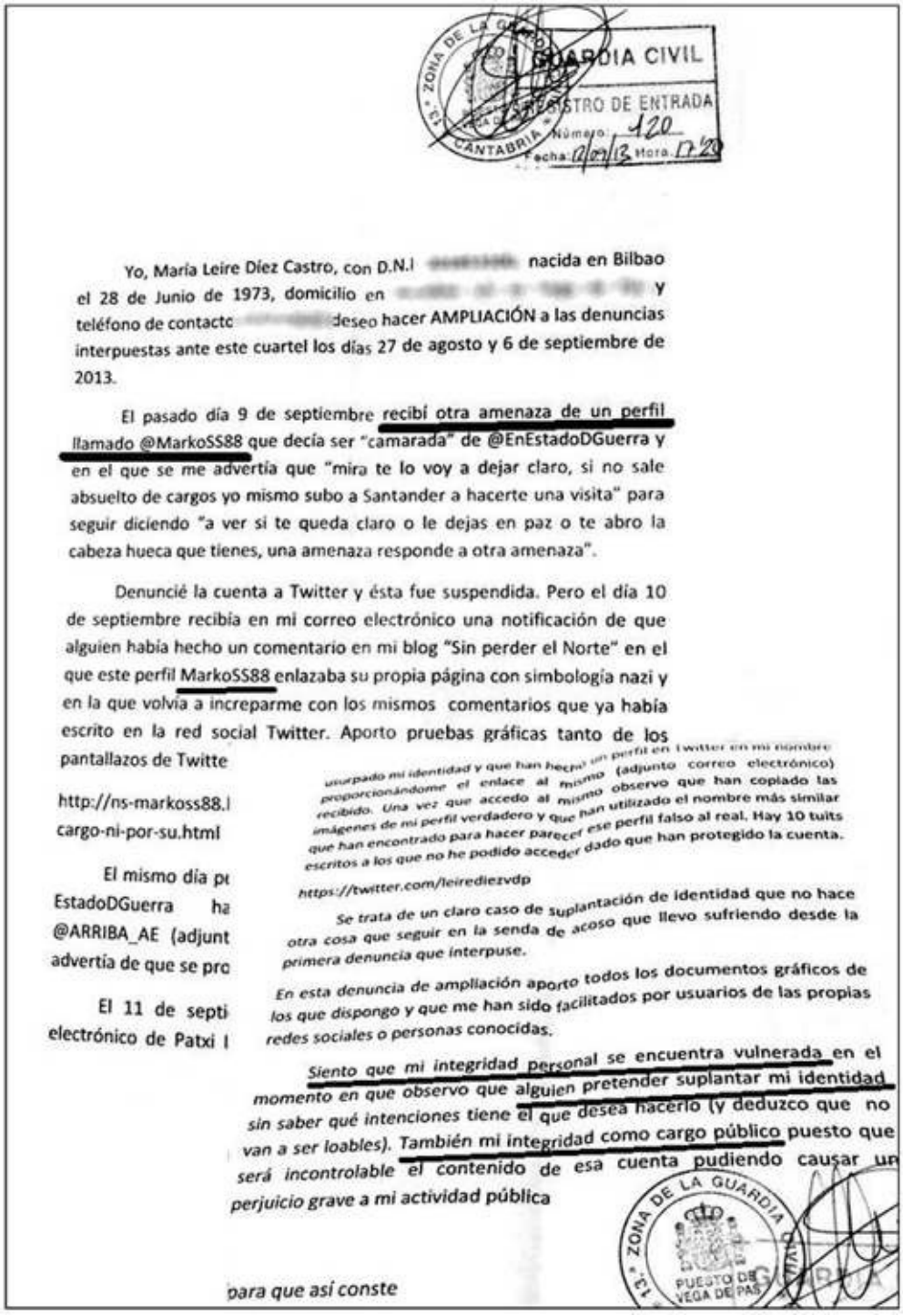
Leire Díez llevaba semanas sufriendo serias amenazas y comentarios soeces en su Twitter por parte de otros «camaradas» de Markos: le advertían que iba a recibir «un susto un día. Pas es pequeñito»; «Espero que tus

muertos estén en una cuneta para que sirvan de meadero, que es lo que se merecen por rojos»; «Lo que tengo es exceso de rojos. Si Franco y su compasión no se hubieran dejado a tantos sin ejecutar…»; «No veo que haya nada debatible con estos izmierdosos. Nada salvo el calibre que prefieren para su ejecución», etcétera. Y la concejala aguantó, estoicamente, hasta que ya no aguantó más, y puso una denuncia contra uno de ellos.[79]

Markos la abordó en su Twitter para amenazarla también por haberlo hecho, sin ningún tipo de contemplaciones (tuits que transcribo aquí literales):

> **@markoSS88** @leirediezpas mira te lo voy a dejar claro, si no sale absuelto de cargos yo mismo subo a Santander a hacerte una visita y esto no va con mi camarada. va entre tu y yo roja de mierda
>
> **@leirediezpas** @markoSS88 Jajajaja, sigues con la prudente cobardía. Muy bien. Algo has aprendido
>
> **@markoSS88** @leirediezpas ¿quieres que deje de lado la “cobardía” para que puedas denunciarme? vamos si me dices que si, nos vemos en los juzgados eso sí, yo las cumplo que te quede bien clarito.
>
> **@leirediezpas** @markoSS88 tú amenaza e insulta y te llevaré al mismo sitio que a tu amigo. Al mismo. Y como puedes observar, no amenazo. Hago
>
> **@markoSS88** @leirediezpas a ver si te queda claro o le dejas en paz o te abro la cabeza hueca que tienes, una amenaza responde otra amenaza…

—¿Lo ves? —añadió Docal—. Este tío no se corta ni con una teniente de alcalde. Y no solo eso. Tras poner la denuncia, Leire Díez subió a su blog una entrada dando las gracias por las muestras de solidaridad que había recibido, y contando lo que había pasado con las amenazas de los nazis. Y Markos dejó un comentario en el blog de la concejala, con un enlace a su propia página. Es un provocador, un loco, o está muy seguro de que no pueden pillarle. Lo que sí sabemos es que toma muchas medidas de protección de su identidad en internet, y eso significa que algo tiene que ocultar.



GUARDIA CIVIL
REGISTRO DE ENTRADA
Número: 120
Fecha: 9/9/13 Hora: 17:20

Yo, María Leire Díez Castro, con D.N.I [redacted] nacida en Bilbao el 28 de Junio de 1973, domicilio en [redacted] y teléfono de contacto [redacted] deseo hacer AMPLIACIÓN a las denuncias interpuestas ante este cuartel los días 27 de agosto y 6 de septiembre de 2013.

El pasado día 9 de septiembre recibí otra amenaza de un perfil llamado @MarkoSS88 que decía ser "camarada" de @EnEstadoDGuerra y en el que se me advertía que "mira te lo voy a dejar claro, si no sale absuelto de cargos yo mismo subo a Santander a hacerte una visita" para seguir diciendo "a ver si te queda claro o le dejas en paz o te abro la cabeza hueca que tienes, una amenaza responde a otra amenaza".

Denuncié la cuenta a Twitter y ésta fue suspendida. Pero el día 10 de septiembre recibía en mi correo electrónico una notificación de que alguien había hecho un comentario en mi blog "Sin perder el Norte" en el que este perfil MarkoSS88 enlazaba su propia página con simbología nazi y en la que volvía a increparme con los mismos comentarios que ya había escrito en la red social Twitter. Aporto pruebas gráficas tanto de los pantallazos de Twitte

http://ns-markoss88.l
cargo-ni-por-su.html

El mismo día pc
EstadoDGuerra ha
@ARRIBA_AE (adjunt
advertía de que se pro

El 11 de septi
electrónico de Patxi I

usurpado mi identidad y que han hecho un perfil en Twitter en mi nombre proporcionándome el enlace al mismo (adjunto correo electrónico) recibido. Una vez que accedo al mismo observo que han copiado las imágenes de mi perfil verdadero y que han utilizado el nombre más similar que han encontrado para hacer parecer ese perfil falso al real. Hay 10 tuits escritos a los que no he podido acceder dado que han protegido la cuenta.

https://twitter.com/leirediezvdp

Se trata de un claro caso de suplantación de identidad que no hace otra cosa que seguir en la senda de acoso que llevo sufriendo desde la primera denuncia que interpuse.

En esta denuncia de ampliación aporto todos los documentos gráficos de los que dispongo y que me han sido facilitados por usuarios de las propias redes sociales o personas conocidas.

Siento que mi integridad personal se encuentra vulnerada en el momento en que observo que alguien pretender suplantar mi identidad sin saber qué intenciones tiene el que desea hacerlo (y deduzco que no van a ser loables). También mi integridad como cargo público puesto que será incontrolable el contenido de esa cuenta pudiendo causar un perjuicio grave a mi actividad pública

para que así conste

Me despedí de David y subí a la moto dándole vueltas a todo esto mientras me dirigía a ver a Esteban Ibarra. A él, por su parte, lo conocí cuando iniciaba mi investigación sobre el movimiento skinhead NS. Cuando me presenté en el local del Movimiento Contra la Intolerancia y le dije que pretendía infiltrarme entre los cabezas rapadas intentó, con buen criterio, que olvidase la idea. Años más tarde tendría la amabilidad de presentar la primera edición de *Diario de un skin,* en vista de que yo no podía hacerlo. Después me embarqué en otra investigación y no volví a verlo hasta años más tarde, en el macrojuicio contra Hammerskin, pero nunca dejé de seguir y admirar su trabajo.

Esteban, en mi opinión, es un héroe que lleva décadas advirtiendo sobre la amenaza del resurgir neonazi en Europa. Mucho antes de que en 2014 el NPD alemán, el FPO austríaco, el UKIP británico, el Frente Popular francés o el Amanecer Dorado griego sufriesen un inquietante aumento de votos en las elecciones al Parlamento Europeo, disparando todas las alarmas, Esteban Ibarra ya se había dejado la voz clamando en el desierto para advertirnos de que eso iba a ocurrir.

El Movimiento Contra la Intolerancia edita el Informe Raxen, una de las mejores referencias para seguir la evolución de la violencia neonazi. Y su observatorio suele monitorizar la actividad skinhead en las redes sociales. De hecho, en su número especial de 2011 dedicaba un reportaje al «Ciberodio y nazi-fascismo en internet».[80]

Ahora necesitaba de nuevo de su consejo. Cuando llegué a nuestra cita, en una cafetería del centro, le noté visiblemente desmejorado. Y conozco la razón: Ibarra ha sido el blanco despiadado de las más brutales campañas de propaganda y acoso neonazi en la red. Se le veía agotado, exhausto, físicamente demacrado. Sin embargo, no había perdido ni un ápice de la pasión en sus convicciones.

Esteban Ibarra acababa de sufrir un nuevo ataque por parte de los neonazis españoles. Algún malnacido, apostaría a que alguno de los tipos imputados en las innumerables causas de agresiones nazis en las que el Movimiento Contra la Intolerancia se había personado como acusación particular, había filtrado sus datos personales. De pronto, su teléfono, su dirección, el teléfono de su esposa, etcétera, estaban en manos de quienes han jurado matarlo. A partir de ese día Esteban y su familia vivieron un infierno. La campaña en Facebook «Yo también pienso que Esteban Ibarra debe morir» aún coleaba en su memoria, y de pronto los nazis tenían su teléfono y el de su mujer, y no dejaban pasar la oportunidad de hacer uso de él. Es admirable que a pesar de todo el odio que ha sufrido, Ibarra continúe luchando por lo que cree.

Recuerdo perfectamente que, tras abandonar el restaurante, caminamos juntos durante un trecho antes de despedirnos. Y me impresionó observar su actitud. Estábamos a la altura de Barceló con Fuencarral, al lado del metro de Tribunal, donde yo viví uno de los episodios más intensos de *Diario de un skin,* al ser perseguido por un grupo de antifascistas que intentó agredirme al salir de esa boca de metro. Así que sé por experiencia propia que esa no es una zona de influencia neonazi, más bien al contrario. Sin embargo, Esteban caminaba tenso, sin prestar apenas atención a mis palabras. Sus ojos saltaban de un transeúnte a otro, buscando una posible amenaza. Y de pronto me vi reflejado en su angustia.

Recuerdo, como si fuese ayer, que en un momento determinado dos

turistas nórdicos se pusieron a nuestra espalda, caminando distraídos mientras admiraban la fachada del Museo Municipal, a nuestra izquierda. Esteban debió de notar su presencia también porque de pronto todos sus músculos se tensaron. Como si estuviese esperando la llegada del primer puñetazo, o el filo de la primera navaja rasgándole la carne…

No soy capaz de expresarlo, pero justo en ese instante comprendí todo el peso que soportan sus hombros, porque muchas veces yo me he sentido así. Y solo quien haya experimentado esa angustia, esa vulnerabilidad, ese temor a simplemente caminar por la calle como cualquier otro ciudadano, podrá comprenderlo. No obstante, vi que estaba moderadamente satisfecho porque habían condenado a dos años de cárcel al internauta que hizo el juego *online* «Mata a Esteban Ibarra», y porque han abierto más procedimientos judiciales por sus denuncias. Hace falta ser muy imbécil para pensar, a estas alturas, que se puede amenazar y acosar impunemente en internet.

Por supuesto, Esteban conocía a MarkoSS88 pero, para mi sorpresa, apenas tenían información sobre su identidad real. Para Ibarra, Markos también era un fantasma en la red.

—Ten cuidado, Toni, si oculta tanto su rastro, es porque tiene buenas razones…

Yo creí haberlas descubierto.

Los extremos se tocan. Hace mucho tiempo que lo aprendí. En *Diario de un skin* ya advertía de cómo me había encontrado los mismos tópicos, prejuicios y justificaciones en un margen y otro del espectro político. Skinheads NS y skinheads antifascistas, utilizaban exactamente las mismas palabras para definir la implacable persecución que sufrían de la Policía (que siempre era menos dura con los contrarios), para justificar sus acciones como una lucha por la clase obrera, para cuestionar al poder…

Cuando años después viví con miembros de grupos armados «revolucionarios», constaté el mismo fenómeno. Para ellos, no importaba que un compañero hubiese atracado un banco, violado a una menor o asesinado a un rival. Su estancia en prisión automáticamente lo convertía en un preso político sometido a las hordas fascistas y opresoras del sistema. En el extremo opuesto ocurre justo lo mismo. Cualquier neonazi condenado a prisión por un crimen común asciende en el acto al rango de mártir de la causa NS. Y MarkoSS88 no iba a ser menos. Ridículo, pero real.

Change.org es una plataforma en internet concebida para la recogida de firmas en apoyo de tal o cual causa. Cualquier usuario puede abrir una petición dirigida a cualquier institución y/o particular. La plataforma posibilita además compartir la petición en las redes sociales, invitando a tus contactos

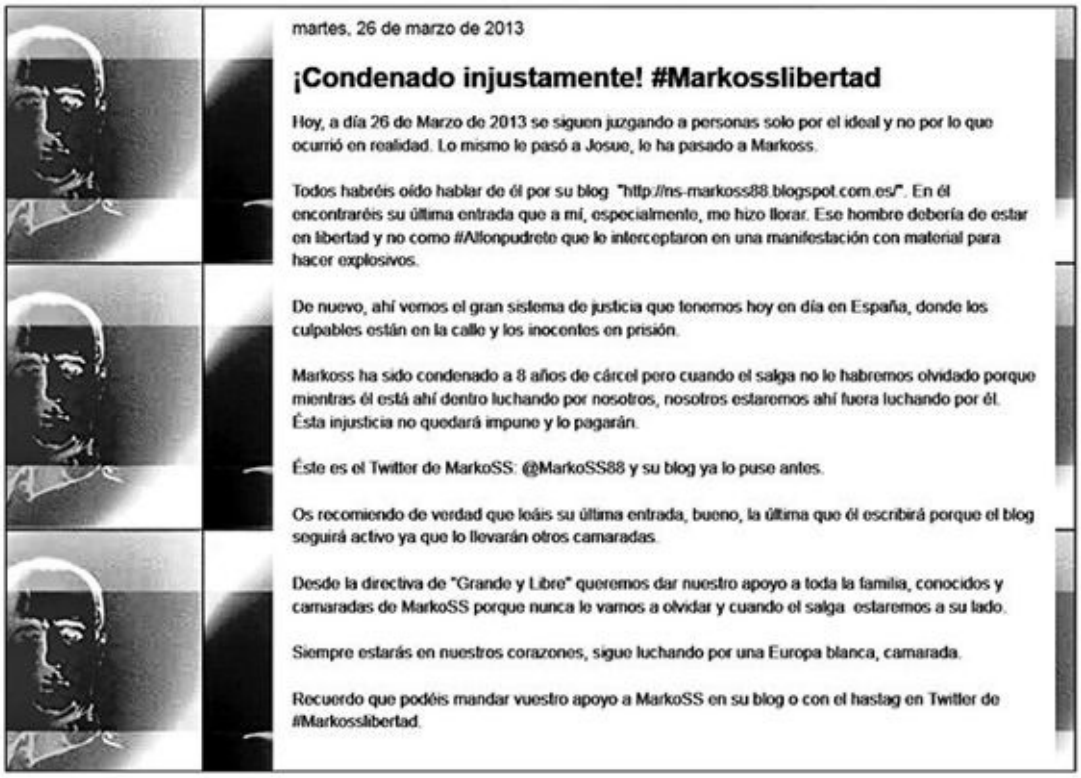
a que la suscriban.

En marzo de 2013, alguien había creado en change.org una plataforma de apoyo a MarkoSS88, encabezada con el siguiente texto, que transcribo literal, erratas incluidas:

> Pedimos la libertad de un chico joven que fue acusado indebidamente. Otro chico de origen latino «Latin king», se acercó a Markos, de ideología fascista, puñal en mano decidido a acabar con su vida. Markos, se vió obligado a defenderse siendo acusado de agresión, en cambio, el latino, que tenía intención de apuñalarlo quedó como víctima condenando a Markos a prisión. Recordemos que fue en defensa personaly que Markos no utilizó ningún arma. Esta recogida de firmas ha de ser apoyada por la injusticia a la que someten a los partidarios de ideología fascista, los llamados presos patriotas, hacemos un llamamiento porque no se condena debidamente si no que tienen en cuenta ante todo de que ideología es cada persona. Según los derechos humanos, una persona tiene totalmente la libertad de expresarse libremente.[81]

Algo más de un centenar y medio de jóvenes neonazis se adhirieron a aquella petición de «justicia» para MarkoSS88, que habría asesinado al latin king en defensa propia. El día 20 de ese mismo mes de marzo, supuestamente dos días antes de que MarkoSS88 ingresase en prisión por el homicidio, en Twitter se creó el *hashtag* #MarkosLibertad,[82] que se unía a las campañas #markossestamoscontigo y #todosssomosMarkoss, también creadas en Twitter.

En paralelo a las campañas de apoyo a favor del joven nazi «injustamente» condenado por matar a un latin king en defensa propia, en Twitter se creó un *hashtag* antifascista (#MarkosLibertad), dedicado a burlarse de la condena de MarkoSS88: #markospudrete.[83] En algunos blog nacionalsocialistas, como Grande y Libre, se hicieron eco de la campaña.



martes, 26 de marzo de 2013

¡Condenado injustamente! #Markosslibertad

Hoy, a día 26 de Marzo de 2013 se siguen juzgando a personas solo por el ideal y no por lo que ocurrió en realidad. Lo mismo le pasó a Josue, le ha pasado a Markoss.

Todos habréis oído hablar de él por su blog "http://ns-markoss88.blogspot.com.es/". En él encontraréis su última entrada que a mí, especialmente, me hizo llorar. Ese hombre debería de estar en libertad y no como #Allonpudrete que lo interceptaron en una manifestación con material para hacer explosivos.

De nuevo, ahí vemos el gran sistema de justicia que tenemos hoy en día en España, donde los culpables están en la calle y los inocentes en prisión.

Markoss ha sido condenado a 8 años de cárcel pero cuando el salga no le habremos olvidado porque mientras él está ahí dentro luchando por nosotros, nosotros estaremos ahí fuera luchando por él. Ésta injusticia no quedará impune y lo pagarán.

Éste es el Twitter de MarkoSS: @MarkoSS88 y su blog ya lo puse antes.

Os recomiendo de verdad que leáis su última entrada, bueno, la última que él escribirá porque el blog seguirá activo ya que lo llevarán otros camaradas.

Desde la directiva de "Grande y Libre" queremos dar nuestro apoyo a toda la familia, conocidos y camaradas de MarkoSS porque nunca le vamos a olvidar y cuando el salga estaremos a su lado.

Siempre estarás en nuestros corazones, sigue luchando por una Europa blanca, camarada.

Recuerdo que podéis mandar vuestro apoyo a MarkoSS en su blog o con el hastag en Twitter de #Markosslibertad.

Y durante el tiempo en que Markos estaba en prisión, alguien se dedicó periódicamente a colgar, cada mes que pasaba, mensajes en su web, pidiendo el apoyo de los camaradas a MarkoSS88.

Si de verdad Markos había matado a un joven latin king —nunca se mencionó su nombre—, parecía razonable que pudiese temer las represalias de sus compañeros latinos. Quizá esa fuese la razón de que ocultase con tanto empeño su verdadera identidad… O quizá no.

Capítulo 8
Los hackers de ETA

«Nosotros odiamos a España con nuestra alma, mientras tenga oprimida a nuestra Patria con las cadenas de la esclavitud. No hay odio que sea proporcionado a la enorme injusticia que con nosotros ha consumado el hijo del romano. No hay odio con que puedan pagarse los innumerables daños que nos causan los largos años de dominación.»

Sabino Arana, *Bizkaitarra,* núm. 16

Terrorismo vasco en la red

En su número 1.711, correspondiente a febrero de 2009, la revista *Interviú* destacaba en su portada el titular: «El manual informático de ETA: Las órdenes de matar viajan encriptadas en *pendrives*. Los mapas de Google que utilizan para sus atentados».

Los redactores del prestigioso semanario habían tenido acceso al manual de seguridad informática de la banda terrorista redactado por Arkaitz Landaberea, informático del diario *Gara,* acusado de pertenecer a la banda desde 2006, y detenido durante la desarticulación del Comando Urruti.

Ana María Pascual firmaba el extenso reportaje sobre el hacker de ETA. Según dicho reportaje, Landaberea había escrito un manual de hacking para terroristas, mucho antes de que Al Qaeda, Boko Haram o el Ejército Islámico aprendiesen a gestionar la red. Y lo había hecho por orden de un viejo conocido: Francisco Javier López Peña, alias «Thierry», el jefe de ETA en aquel momento, que había sido detenido en Francia el 20 de mayo de 2008. Él fue el responsable de ordenar el atentado de la T4 del aeropuerto de Barajas el 30 de diciembre de 2006, un día después de que el presidente Zapatero hiciese aquellas triunfalistas declaraciones: «El fin de ETA está cerca». En el atentado perdieron la vida los ecuatorianos Carlos Alfonso Palate y Diego Armando Estacio… Ni siquiera eran españoles. Daños colaterales, diría mi «padrino» Carlos el Chacal.

Thierry murió en París el 30 de marzo de 2013, y a pesar de que no era un nativo digital, siempre tuvo claro lo importante que era internet para ETA, por eso habría encargado al informático de *Gara,* según la investigación policial, la redacción de un manual para cifrar los ordenadores, *pendrives* y tarjetas de memoria utilizados por los comandos. Y sobre todo, para establecer comunicaciones seguras entre los etarras escondidos en Francia, Venezuela, España o cualquier otra parte del mundo.

Un opúsculo de dieciséis páginas, en euskera, que se había terminado de redactar en septiembre de 2008. Pero su cifrado no resultó lo bastante sólido. Los hackers de la Guardia Civil consiguieron romperlo tras la detención de Thierry y el análisis forense de su ordenador. Dos meses después de la redacción del manual de Seguridad Informática de ETA, Landaberea era detenido.

Como escribía Ana María Pascual:

> Para ETA se ha demostrado primordial que la puerta de acceso a su información esté bien cerrada y que la llave la tengan solo algunos activistas escogidos. Las últimas investigaciones han confirmado que las órdenes para matar se contienen en mensajes cifrados que se intercambian, sobre todo, mediante *pendrives*. Esos pequeños dispositivos USB, fácilmente ocultables en buzones de la banda, determinan cuándo y a quién se va a matar. Por ello, el informático Landaberea pone todo el énfasis en su manual en que se logre una clave segura. Así, insta a sus compinches a aprenderse la clave de memoria y los orienta a la hora de elegirla: «Debemos tener la clave memorizada y no apuntada en ningún sitio, por consiguiente no puede ser demasiado larga. Hay técnicas para arreglar este asunto, por ejemplo, en un libro/revista la primera frase de la página 34, o memoriza cualquier cosa así. Si no tiene significado, mejor, así en el caso hipotético de que quieran romper nuestra clave, no podrán utilizar un diccionario». Landaberea también aconseja, para fabricar la contraseña: «Cuantos más caracteres no alfanuméricos [que no sean letras ni

números, sino, por ejemplo, puntos, comas…] por lo tanto mejor (sic)».

En su manual, el informático de ETA también aborda otra preocupación de la banda: cómo eliminar de una forma segura los archivos. «Cuando borramos los ficheros que están en nuestro ordenador de una forma normal, no los borramos físicamente del disco duro, se quedan ahí (aunque los borremos también de la papelera de reciclaje). Por lo tanto, esta información se puede recuperar con diversos instrumentos, y muchas veces eso no queremos que ocurra. [El programa] Freespace wipe hace una eliminación segura sin utilizar nuestro disco duro (…) elimina de una forma segura los ficheros borrados anteriormente con una eliminación normal. (Ni que decir tiene que nos vendría muy bien realizar esta acción de vez en cuando)».

El último capítulo del manual de hacking terrorista estaba dedicado al intercambio de información entre los comandos. Sus emails no transitaban cifrados por la red, y se limitaban al cifrado de los archivos adjuntos. Bendito error. Por eso Landaberea insistía en que era preferible utilizar memorias USB.

Muchas de esas memorias fueron incautadas durante diferentes operaciones policiales. No fue posible descifrarlas todas, pero las que han podido romperse incluían información sobre futuros objetivos de la banda, como ertzainas o guardias civiles. Ahí estaban sus rutinas: dónde acudían a desayunar todos los días, las fotos de sus caras… Gracias a toda aquella información incautada al Comando Urruti, se averiguó que, entre otros planes, ETA barajaba la posibilidad de exportar técnicas como la bicicleta-bomba, utilizada por sus camaradas colombianos de las FARC o el ELN. Con el macabro matiz de añadir una silla infantil en la bicicleta, para no levantar sospechas. El objetivo de aquel atentado serían los ertzainas de la comisaría de Ondarreta.

Tal y como cuenta el fascinante reportaje de *Interviú:*

Tanto debieron gustarles a los dirigentes etarras los servicios de Landaberea como asesor informático que un miembro del aparato de logística le propuso dos veces pasarse a Francia y trabajar en París con la tapadera de una tienda de informática que le montaría ETA. Con ello, la banda tendría además resuelto el suministro de material informático. Es esta una de las cuestiones logísticas más dificultosas para los etarras. Los ordenadores y los *pendrives* llevan una serie de referencias internas por las que se puede llegar, al menos, al establecimiento donde se vendieron. Si la tienda tiene cámaras de seguridad, o si su responsable lleva un control de ventas, puede saberse quién los adquirió. Arkaitz rechazó la oferta de París. Prefirió seguir en San Sebastián, donde llevaba dos años trabajando en el diario *Gara,* con un sueldo de 1.100 euros mensuales, y donde vivía con su novia.

En la banda se tomaron en serio lo de la encriptación y la seguridad informática. Uno de los lugartenientes de Txeroki, José Segurola, fue de los primeros etarras en usar el programa PGP del que me habló el capitán César Lorenzana. Hasta su detención en Francia en 2005, la policía había visto pocos archivos informáticos de miembros de la banda encriptados con un sistema que Landaberea elogiaba: «Ofrece seguridad para años, y mirándolo desde muchos puntos, eso puede ser una seguridad del 100 por ciento, es decir, quizás nos daría igual que dentro de 5-10 años cayera esa información en malas manos, ¿no?», preguntaba.

En mayo de 2011 Julen Etxaniz García y Arkaitz Landaberea, el autor del manual de hacking etarra, eran condenados a ocho años de prisión por pertenencia a banda armada. Ellos habían sido los encargados de buscar a los objetivos, guardias civiles y

ertzainas, seguirlos, grabarlos, documentar sus rutinas y después introducir toda esa información en los USB cifrados.

La ponente de la resolución, la juez Manuela Fernández Prado, recordó su manual, y explicó cómo las memorias USB cifradas según el sistema de Landaberea eran depositadas en buzones previamente convenidos, donde «ellos se encargaban de comprobar la veracidad de estos datos (…) y después devolvían la información». Con ella, los comandos encargados de ejecutar los atentados ya estaban en disposición de cometer el próximo asesinato. Y esta vez le tocaría a un ertzaina.

En el siglo XXI la guerra contra el terrorismo, y no solo el yihadista, también se libra en la red. Y de la misma forma en que ETA aprendió a potenciar su seguridad informática la Ertzaintza ha tenido que ponerse las pilas.

El otro «informático de ETA», así lo bautizó la prensa, fue Iraitz Guesalaga. En febrero de 2012 la Sección Cuarta de la Sala de lo Penal de la Audiencia Nacional lo absolvió de las acusaciones presentadas por la Fiscalía, que lo consideraba el heredero de Landaberea en el hacking etarra. Basándose también en la documentación rescatada del ordenador de Thierry, la Guardia Civil y el instructor (el juez Fernando Grande-Marlaska), habían concluido que en 2008 Guesalaga había viajado a Venezuela y de allí a Colombia, para formar a la guerrilla de las FARC en el uso del cifrado en las comunicaciones electrónicas, pero la Audiencia Nacional dictaminó que las pruebas aportadas por los policías «no solo han sido absolutamente insuficientes para desvirtuar la presunción de inocencia», sino que, además se obtuvieron «en contra de los parámetros de legalidad».

Aun así, la ciberlucha contra ETA nunca se limitó a la investigación policial y a las actuaciones judiciales. En su día, algunos hackers, jóvenes y geniales, también intentaron aportar su granito de arena, manifestando abiertamente su desprecio a la lucha armada. Uno de ellos fue GriYo.

GriYo es uno de los nombres históricos del hacking español. Mercè Molist se refiere a él en varias ocasiones en su imprescindible *Hackstory*, y yo mismo escucharía su nombre en los labios de varios hackers contemporáneos durante mis encuentros con la comunidad del siglo XXI. Hoy trabaja para una gran empresa, pero GriYo fue uno de los primeros escritores de *malware* españoles, y un buen ejemplo de que el *malware* también puede tener su lado positivo.

Entre las muchas creaciones de GriYo destacan obras como Marburg, el primer virus polimórfico de 32 bits, que se propagó por todo el mundo a gran velocidad debido a que revistas del sector, como *PCGamer* o *PC Power Play* regalaron en su día CD infectados con Marburg. También juegos como el MGM/Wargames salió al mercado infectado con el mismo virus. En aquellos días, octubre de 1997, los hacker se habían empeñado en desenmascarar la publicidad engañosa de los antivirus que se vendían como infalibles, y GriYo lo probó colando en el mercado un «bicho» que los antivirus no detectaban. Pero lo realmente curioso es que GriYo fue el autor de uno de los primeros virus «anti-ETA», cuyo código escribió conmovido por el asesinato

de Miguel Ángel Blanco.

Aunque inocuo, el virus «anti-ETA» hacía aparecer en la pantalla de los ordenadores infectados una mano blanca, símbolo de la protesta multitudinaria por la cruel ejecución del concejal de Ermua. Fue uno de los primeros virus hacktivistas de la historia.

Un año antes, otros hackers españoles ya les habían tocado las narices a los terroristas al hackear una de sus páginas web de apoyo.

En febrero de 1996, ETA contaba con una página de propaganda alojada en un servidor ubicado en la localidad belga de Gante: www.knooppunt.be. Desde allí, la web de apoyo al «Complejo ETA» llamada Euskadi Información distribuía la propaganda de la banda a todo el planeta. Tras el cobarde asesinato del catedrático de Derecho Francisco Tomás y Valiente, el 14 de febrero de ese año, un grupo de hackers españoles decidió hacer algo. Y qué mejor que joderle a los terroristas su plataforma publicitaria en internet.

La web www.knooppunt.be/~euskadi no pudo resistir el ataque de los hackers. Las pantallas de la web se llenaron de lazos azules, en símbolo de protesta por el profesor asesinado. Y no solo los correos electrónicos de Euskadi Información, sino también los de la empresa que los albergaba, se saturaron con el ataque de lazos azules. Los atacantes consiguieron expulsar de internet a los miembros del colectivo de apoyo al «Complejo ETA» durante dos meses, hasta que en abril abrieron otra web.

Es irónico, pero los de ETA calificaron a los hackers que habían desarrollado el ataque como «ciberterroristas». Y yo no podía imaginar en estos momentos que, unos meses más tarde, descubriría que el hackeo a la web de ETA se hizo desde la Escuela Universitaria La Almunia de Doña Godina, en Zaragoza (entre otros sitios y sin el menor conocimiento del centro), y que conocería y entablaría amistad con uno de los hackers que impulsaron aquella acción.

28 / ABC NACIONAL VIERNES 12-4-96

Los proetarras anuncian desde Bruselas su vuelta a Internet para difundir su apoyo a ETA

Sus promotores califican como «ciber terrorismo» el bloqueo sufrido en febrero

San Sebastián

Los sectores proetarras vuelven a disponer de un servidor para distribuir su versión favorable a la banda terrorista ETA y sus grupos afines, a través de la red Internet, después del bloqueo sufrido el pasado mes de febrero a raíz de que un pistolero del «comando Madrid» asesinara al catedrático de Derecho Francisco Tomás y Valiente. Por su parte, la editorial Txalaparta ha editado un CD-ROM sobre ETA, autora de casi mil asesinatos.

Ertzaintza 2.0

Llegué a las instalaciones de la Ertzaintza a primera hora de la mañana. Quería tener tiempo para charlar con el jefe de la Sección Central de Delitos en Tecnologías de la Información de la Unidad de Investigación Criminal y Policía Judicial, Manuel Viota Maestre. El edificio era grande y moderno, no tanto como las fastuosas dependencias de los Mossos d'Esquadra a las afueras de Sabadell,[84] pero no estaban mal.

La unidad que lidera el suboficial Viota lleva más de quince años rastreando el delito en las redes informáticas. Así que son «vieja escuela» en toda regla, y el primer servicio policial español que creó grupos especializados en la criminalidad en la red.

—¿Cuándo nació vuestra unidad?

—En enero de 1998. Fuimos de los primeros. Primero se creó la de la Guardia Civil y luego nosotros. Yo no tuve constancia de la de Policía Nacional hasta un tiempo después.

—Vaya, pues fuisteis muy intuitivos, porque esto ya es el presente y el futuro de la delincuencia…

—O el pasado —me corrigió el suboficial—, porque esto va tan deprisa que ya es el pasado de la delincuencia…

Manuel Viota, coautor de varias monografías sobre seguridad informática, y participante en diferentes eventos, es sin embargo muy escéptico con el uso alarmista del término *ciberterrorismo*. Para ETA y para cualquier otra organización.

—Ciberterrorismo como tal no ha existido hasta ahora. Nosotros tenemos otra unidad, la de lucha contra el terrorismo, que es la que se ocupa. No hemos tenido una actividad ciberterrorista. Lo que sí hemos tenido es cuestiones de propaganda o captación a través de la red.

—Ahora sí está penado lo de las amenazas o la propaganda terrorista en Twitter, por ejemplo…

—En realidad, lo ha estado siempre. No hay un delito tipificado exclusivo para la red. La apología ha estado penada siempre, lo que ocurre es que antes lo hacían por pasquines y a través de cartas amenazantes, y ahora lo hacen por Twitter o Facebook. El delito es el mismo, lo que ha cambiado es el medio. El Código Penal sigue protegiendo los mismos preceptos básicos que hace dos siglos. Protege a las personas, el dinero, la libertad, los grandes valores siguen estando ahí. Bien es verdad que algunos delitos han crecido o han nacido con la informática. El ataque a sistemas es un delito nuevo, pero claro, porque la propia tecnología es la víctima.

El suboficial me puso un ejemplo muy interesante, especialmente teniendo en cuenta que estábamos en Euskadi, donde muchas empresas habían sufrido la extorsión de ETA.

—Aquí hemos pasado de muchas medidas de seguridad (el vigilante armado en la puerta, las cámaras de videovigilancia, la caja fuerte…) a nada. Las empresas creen

que como sus datos están metidos dentro de un ordenador, ya está. Y no es así. Vamos a muchas empresas porque les han encriptado los datos, y cuando les preguntamos si tienen copia de seguridad, nos dicen que no. Hay empresas que han tenido que cerrar por eso. Es un problema de ignorancia.

—Vale, ese es el lado negativo. Pero imagino que desde el punto de vista policial, toda esta tecnología, las apps, etcétera, ofrece unas herramientas de investigación brutales…

—Sí, así es. Desde luego. Porque la gente no es consciente de la información que da. Ni las víctimas ni los delincuentes. Todo el mundo vierte su vida en internet y eso es perfectamente explotable. En nuestro caso, es lógico que investiguemos, pero en el de los delincuentes, tienen un montón de víctimas que están exponiendo toda su vida. Antes, un pederasta tenía un trabajo enorme: debía localizar a una víctima que fuese de la edad que quería, tenía que chatear con ella un montón de tiempo para sacarle información, qué le gustaba y qué no, dónde estudiaba, que le mandase una foto… Era un trabajo previo muy arduo. ¿Ahora? Vas a Tuenti o a Twitter y localizas enseguida a la que tú quieres. Todo ese trabajo se lo estoy dando yo como víctima. Mis gustos, mis aficiones, mis fotos… Es mucho más fácil engañarme con todo ese trabajo previo. Es un catálogo de víctimas.

—Antes al empezar, en el 98, os limitabais a los chats, los emails, el IRC…

—Los BBS en su momento.

—Ahora con las redes sociales, el campo que debéis cubrir será mucho mayor.

—Y tanto. Cada día nacen redes nuevas, y mueren otras. A veces nos llegan denuncias por un acoso en una red, y ni la conocíamos. Claro, tienes que darte de alta en la red, estudiar cómo funciona, qué parámetros sigue, a quién hay que pedirle los datos… El problema que tenemos es que no terminamos nunca. Aquí trabajamos siete u ocho horas diarias, pero en casa seguimos trabajando. Porque nos gusta lo que hacemos. Si no estuviésemos enamorados de este trabajo, no podríamos estar aquí.

—Supongo que la gran revolución llegaría con los teléfonos móviles.

—Buf, eso es otro mundo. Fíjate: cuando empezamos nosotros, las víctimas estaban muy limitadas en el tiempo y el espacio. Porque cuando tú te conectabas a internet lo hacías a través del módem. Y solías conectarte de noche, porque de día las tarifas eran abusivas. Las tarifas planas iban de ocho de la noche a ocho de la mañana, pero tampoco podías estar conectado las doce horas, porque mientras te conectabas a internet, tu casa se quedaba sin teléfono, y tu madre te decía «¿Dónde vas, campeón?». Navegabas una, dos, tres horas, las que te dejaba tu madre, y ya está. Es decir, que tu ventana de exposición eran esas tres o cuatro horas que estabas conectado. Si alguien quería atacarte, tenía que hacerlo entonces. Pero ahora ya no. Con la salida de las ADSL hay mucha gente que compra el ordenador, lo conecta a internet y no lo apaga hasta que se le quema. La ventana de exposición es permanente. Está expuesto veinticuatro horas al día. Pero claro, estás expuesto en tu casa. Te pueden atacar el ordenador, robarte la información… Pero ahora, con los

móviles, estamos veinticuatro horas al día conectados nosotros, lo llevamos siempre encima.

El ertzaina cogió su teléfono móvil, que estaba sobre la mesa, y me lo mostró.

—Esto no es un teléfono, es un ordenador. Y algunos sospechan que también vale para hablar por teléfono. En serio, no es broma. Cuando le preguntas a los menores quién habla por teléfono, ninguno. Quizá para llamar a sus padres, y de forma puntual. El teléfono lo usan para Telegram, Line, para wasapear… ¿Por qué crees que las compañías telefónicas ahora regalan las llamadas? Lo que cobran son los datos… Antes en las charlas le decíamos a los padres que colocasen el ordenador en el salón de casa, a la vista, para que la navegación estuviese controlada. No por nada relacionado con la intimidad, sino inculcando a los críos que es un electrodoméstico, una herramienta más. Pero ahora no podemos. Si pones el ordenador en el salón, y el chaval se lleva el móvil a su cuarto, o al baño… En un portátil hay una cámara, pero en un móvil hay dos, una delante y otra detrás. El nivel de captación de imágenes es el doble.

—Has dicho charlas… ¿Hacéis concienciación entre los menores?

—Sí, es un proyecto que tenemos y el resultado es increíble, increíble. Los chavales disfrutan una barbaridad con nosotros, porque les hablamos un lenguaje que entienden. Y sabemos de lo que hablamos. Les ponemos casos que hemos vivido nosotros, y que les han ocurrido a otros chavales como ellos. Cuando se lo dice un padre, piensan: «Ya está mi viejo rayándome», pero cuando un policía les dice: «No hagas esto porque la semana pasada detuve a uno que estaba haciendo esto con un chaval de tu edad, que además es del pueblo de aquí a lado». O: «Cuidado con lo que mandas a tu pareja, porque esta chica le mandó una foto desnuda a su novio, rompieron y ahora la foto fijaos dónde está»… Flipan con nosotros.

—¡Qué bueno!

—Claro, porque además conseguimos varias cosas. Algunos ni siquiera saben que lo que hacen es delito. Lo hacen como una broma, pero que puede llevarte a la cárcel. Leerle los mensajes a un hermano mayor es como cuando le leías el diario para ver cómo se ligaba, o las fotos que tenía, pero ahora si eso lo haces digitalmente, vas a la cárcel. O quitarle la cuenta para hacer una broma, o suplantar su identidad para insultar a otro… Todo eso es delito.

En ese instante el policía guardó silencio un instante, con la mirada perdida en algún punto del despacho oficial en el que nos encontrábamos. Como si estuviese intentando recordar algo…

—Recuerdo un caso que nos llegó cuando una niña, no tenía ni quince años, vino a denunciar que alguien se había colado en su ordenador a través del email, donde tenía unas fotos comprometedoras… Vamos, ligerita de ropa. El pederasta, un asqueroso, contactó con ella y le dijo que si no le mandaba una foto desnuda, le enviaría a sus padres, profesores y amigos las que ya tenía. Con esa edad no tienes los recursos psicológicos para enfrentarte a algo así. La cría aceptó y se la mandó. Pero el

tipo dijo que esa no le gustaba, que le mandase otra y las borraba todas. Y le mandó otra. Lo mismo, no me gusta, hazte otra. Y otra, y otra más. Y así durante un año, que es lo que tardó en venir a denunciar. La chavala estaba totalmente destrozada. Bueno, pues cuando denunció, al tío le pillamos en un mes. Cuando entramos en casa del sinvergüenza y le analizamos los ordenadores vimos que todo lo que decía la niña era cierto, tenía allí todas las fotos. Pero no solo eso, sino que allí encontramos fotos y vídeos de otras cien niñas más, y ninguna había denunciado. Si solo una hubiese denunciado antes, las demás quizá no habrían pasado por eso…

La reflexión del ertzaina merece ser subrayada. A veces, el miedo a denunciar no solo nos condena a nosotros a sufrir el chantaje de un cracker en silencio. Con ese silencio podemos estar condenando a muchas otras personas a pasar por el mismo calvario. Me quedo con la frase del policía: «Si solo una hubiese denunciado antes…».[85]

—Bueno, pues le detuvimos. Estuvo en preventiva, y cuando salió ¿sabes lo primero que hizo, el campeón? Lo volvió a hacer, con otras quince niñas. Lo volvimos a pillar, y ahora está cumpliendo condena. Diez años le han caído. Pero ¿sabes lo mejor? Un año después se repitió, en Donosti, otro tío le había quitado las cuentas de correo a otras quince niñas, y lo mismo, las chantajeaba para que le mandasen fotos. Pero ¿sabes cuántas de esas quince niñas aceptaron el chantaje?

—¿Todas? —respondí.

—Ninguna. Ni una. En lugar de eso todas denunciaron. ¿Qué diferencia había entre un caso y otro?

Me encogí de hombros. Ni idea.

—Pues la diferencia fui yo. Porque tres meses antes había estado en su instituto, les había dado la charla, y esas chicas estaban presentes. Y cuando les pasó esto, se acordaron de la charla… «Coño, si Manu nos dijo que pasaba esto.» Cogieron a la madre de la mano: «Ama, vamos a comisaría». Y así le pillamos. Ha cambiado el paradigma de la Policía: yo ya no estoy centrado en el delincuente, estoy centrado en la prevención. Si me das a elegir entre pillar a quince delincuentes o evitar una víctima, yo me quedo con evitar la víctima. Lo más importante es que esto se sepa y que las víctimas sepan cómo actuar.

Una vez más, esta vez a través del ertzaina, la Providencia me dejaba claro la urgencia de tratar este tema. Porque cada día que pasaba nuevas víctimas caían en alguna de las trampas de la red. Y nadie está a salvo.

—Todos podemos ser infectados, y si me pueden infectar hasta a mí, que soy de Bilbao, imagínate…

NOVIEMBRE DE 2014
SILVIA, LA NOVIA DE MARKOSS88

«Las mujeres más bellas pertenecen por derecho a los combatientes.»

Adolf Hitler, en las memorias de su secretaria Christa Schroeder

—¿Sabías que Markos tiene novia?

Álex, uno de los miembros del CNP que se desvivió en la investigación sobre MarkoSS88, consiguió sorprenderme con su aportación. Aunque ahora está destinado en otra unidad, viene de Información, y sabe investigar.

—Sí, me lo ha mencionado alguna vez…

En efecto: en un email del 11 de julio de 2014 Markos mencionaba a una tal Silvia.


YAHOO! MAIL Buscar Buscar mensajes Buscar en Internet tonisalas2000

Saludo (3) Gente

NS Sin Censura jul 11 a las 1:43 AM

Para Antonio Salas

Hola, no quiero ser pesado pero... hoy necesito hablar con alguien y al único al que le puedo contar las cosas y me va a guardar la mierda eres tú, te cuento, llevo no se cuanto tiempo en el hospital, uno vino a por mí y con lo único que reaccioné fue con una navaja bueno pues sus amigos me pegaron una paliza, acabé con el movil destrozado perdí todo, fotos, contactos las notas de tu libro , pruebas... acabé con los huesos destrozados, ayer por fín me dieron algo de comer, unos dolores insoportables he tenido... bueno increible, un camarada me dejó un teléfono para ponerme en contacto con mis camaradas por telegram, vale pues.. hace un par de días por facebook habia , un guarrete, provocandonos, bueno creíamos que era un guarrete pues... es del CNP, es un puto policía corrupto e infiltrado que provoca amenazas e insultos para hacérselo saber a sus superiores, eh... yo he flipado, iba a por mi el hijo de puta, que se ha informado de mi caso que fuí a por un panchito que yo alegué defensa personal que si sus compañeros me conoce como markos matamoros que si esos no son mis apellidos reales....pues yo hice el trato de que dejara a todos los camaradas en paz y eso recayera sobre mi, porque soy así de gilipollas, estuvimos hablando y me dijo que el año pasado dio aviso de un grupo de gente que se juntaba en el drakkar, claro,mis camaradas de US le dije lo mismo que yo me hacía responsable, hablé con los camaradas del facebook de que no hablaran con el, pues ahora soy yo el malo el que ha jodido todo... el poli me ha bloqueado por facebook y ya no se lo que publica , dice o hace... y que soy un egoista me dicen! ni que yo quisiera que me encerraran de nuevo no te jode...no se dan cuenta de que les estoy intentando salvar el culo a todos y soy muy malo, me saca de quicio, me acaba de pasar y le he dicho al medico que incluso firmaba el alta voluntana que yo me iba a liarla y es el que me ha parado para no hacerlo, el policía me la ha liado, tengo a silvia, mi novia cabreada, los camaradas llamándome egoista y están cabreados conmigo y yo sin poder moverme de aquí... así que lo unico que se me ha ocurrido con la rabia que tengo es contartelo, tambien tengo de decirte que terminé el libro por suerte apunté algunas cosas ahí, cuando salga te diré todo lo que pienso, lo bueno y lo malo y las preguntas y mis reflexoones

Un saludo

—Fíjate, es una auténtica preciosidad —me dijo Álex mientras me mostraba unas capturas de Twitter—. Se llama Silvia Hierro y es de Madrid. Muy activa en Twitter.

Estudiante de segundo de Medicina, diecinueve años, tenía cuentas en casi todas las redes sociales: Ask, http://ask.fm/TuMiradaybasta; Twitter, @TuMiradaybasta; Facebook, etcétera. Se presentaba como «Apasionada de la fotografía y el kick boxing, madridista y madrileña, me desvivo por los míos, intenta conocerme antes de criticarme». Y Álex tenía razón, era una chica realmente hermosa.

Justo es reconocerlo, Markos también era un tipo muy atractivo. De

hecho, al contemplar sus fotografías en Twitter, Facebook o Telegram, cualquiera podría pensar que se encontraba ante una pareja de modelos (ella lo es, pero yo aún no lo sabía), más que ante un skinhead nazi condenado por homicidio y su novia.

A diferencia de MarkoSS88, que entraba al trapo con todo antifascista que le provocase, Silvia adoptaba una actitud mucho más serena, tranquila y conciliadora, cuando no simplemente despectiva. Porque solo por ser la novia de Markos, recibía ataques de lo más feroces y desproporcionados de los antifas, incluyendo brutales amenazas: «Para cortarle el cuello, y a ti también por salir con ese ser»; «A tu novio le vamos a matar y a ti te vamos a violar», etcétera. Y lo extraordinario de verdad es que Silvia, como Markos, aparecía en sus perfiles sociales a cara descubierta, es decir, con sus rostros perfectamente visibles y sin modificar.

Podía poner cara al joven neonazi que me confesó que había intentado asesinarme el 5 de marzo. Y a su novia también.

Lo primero que pensé al visitar sus perfiles en Facebook, Twitter, Ask, Telegram, etcétera, es en cómo reaccionaría si por casualidad me los encontrase por la calle. Y, sobre todo, en cómo reaccionaría un bloque de antifascistas, envalentonados por el grupo, si se encontrasen con Markos accidentalmente en el metro, en el autobús, a la salida del estadio… En su perfil de Facebook era posible ver varias fotografías de Markos y Silvia en el Bernabéu. Los que visitamos aquellas gradas —en mi caso con mis antiguos camaradas de UltraSSur— las reconocíamos al instante, pero sus odiados antifas también, y no parecía tan difícil identificarlos a la salida del estadio teniendo sus rostros. De hecho, el mismo Markos me decía en su email del 12 de abril de 2014: «Lamentablemente, antifas y latin entre otras bandas conocen mi cara».

En sus tuits, MarkoSS88 excedía todos los límites de la provocación. En varias ocasiones llegaba a retar a sus interlocutores, antifascistas, para quedar físicamente y pelear. Aunque no encontré ninguna referencia a que ninguna de esas peleas llegase a materializarse, esos tuits nos serían muy útiles más tarde para geoposicionar desde dónde habían sido enviados.

En los foros antifascistas llegó a tratarse el problema de MarkoSS88 y sus constantes provocaciones. Por ejemplo, el 27 de agosto de 2013 el Forocomunista[86] se hacía eco de las amenazas publicadas por MarkoSS88 en su blog. Aseguraba poseer la dirección del domicilio de Alfonso Fernández Ortega, alias «Alfon», y su familia. Y anunciaba que iba a publicarla. A Alfon lo habían detenido el 14 de noviembre de 2012, durante la huelga general, transportando un artefacto explosivo de fabricación casera, y su proceso judicial despertó un gran revuelo mediático. Alfon ascendió al rango de héroe entre los antifascistas, y la campaña «Alfon Libertad» recorrió

toda España. Para los nazis, sin embargo, era un símbolo de todo lo que ellos desprecian. Como yo. De hecho, Markos me había confesado en uno de sus primeros emails que las dos personas que más odiaba en el mundo eran Alfon y Tiger88.

Markos no solo entró en Forocomunista para ratificarse en su amenaza a los antifascistas, sino que la cumplió. El 3 de diciembre de 2013 publicaba la dirección de Alfon y su familia. No parecía preocuparle las consecuencias de aquella temeridad. Es evidente que divulgar la dirección de un objetivo de la extrema derecha como Alfon ponía en peligro tanto la integridad y la vida de Alfon, como la de sus padres y hermanos. Por fortuna, la dirección era falsa. De nuevo Markos utilizaba una información que sabía errónea, como había hecho con mi identidad, para promocionarse.

Tenía razón en algo, todos los antifas conocían su cara. Y yo también. No me fue difícil memorizar el rostro de mi asesino. Lo veía casi todas las noches en mis sueños. Y también durante el día. Cada vez que viajaba a Madrid para reunirme con mi editora, o para acudir a una tertulia con David Madrid y nuestros amigos, o para entrevistar a un nuevo hacker. Caminaba por las calles con los nervios en tensión, pegando un brinco cada vez que me cruzaba con un joven moreno, de pelo corto, atlético, en el que creía ver a MarkoSS88 a punto de saltar sobre mí para rajarme la garganta, como hacía en mis pesadillas. No le deseo a nadie esa sensación.

Pero a pesar de ello, doy mi palabra de que todavía creía que podía cambiar su forma de pensar, que podía ayudarle a salir del NS. Ahora me siento un poco estúpido.

Capítulo 9
Estafados en internet

«Los temores, las sospechas, la frialdad, la reserva, el odio, la traición, se esconden frecuentemente bajo ese velo uniforme y pérfido de la cortesía.»

Jean-Jacques Rousseau

Estafas en serie en la red

Las estafas han existido siempre. Puede que tú mismo recibieras alguna en casa cuando eras crío. Soy el Príncipe de Zamunda —o qué sé yo—, estoy preso aquí en Nigeria y necesito que me mandes 5.000 pesetas, y cuando salga te voy a dar un millón como muestra de agradecimiento. Esto sigue funcionando… solo que ahora se hace a través del correo electrónico.

Había comentado ya algo en mi viaje al País Vasco, cuando me reuní con el suboficial Manuel Viota:

—El timo 419 o la estafa de la carta nigeriana es el mejor ejemplo de cómo los viejos fraudes se han adaptado a las nuevas tecnologías —me contaba el ertzaina—. Todos hemos recibido esos mensajes de *phishing* en alguna ocasión. Un email con muchos errores gramaticales y sintácticos, de un príncipe, banquero, militar o rey retenido que no puede acceder a sus cuentas bancarias y nos ofrece una compensación millonaria si le ayudamos a sacar su dinero del banco. El timo *online* tiene muchas variantes: un tío en América, un premio en la lotería, un militar en Irak, un préstamo, una exuberante rusa enamorada… Todos buscan los mismo: nuestro dinero.

Yo había tenido ocasión de ver algunos de esos timos. Desde luego, la estafa es un arte, y algunos de esos emails llegaban acompañados de documentos, informes, certificados, perfectamente elaborados. Todo falso.

—El origen de este engaño hay que buscarlo en «La carta del prisionero español» y el «Timo del entierro» —me informó Viota—. En el siglo XVIII los estafadores se aprovecharon de las secuelas de la guerra de la Independencia española y las guerras carlistas para idear un engaño que se ha prolongado hasta nuestros días. La víctima recibía una carta manuscrita, firmada por un noble que se encontraba prisionero en una cárcel española, y que debía ocultar su identidad. El remitente prometía al receptor un tesoro oculto bajo tierra, pidiéndole a cambio una pequeña suma por los planos del tesoro, o por su fianza para salir de prisión, o por cualquier otra cosa.

Voilà: ya habían inventado el *crowdfunding*.

El engaño, que apelaba a la avaricia de la víctima, funcionó tan bien que comenzaron a improvisarse variables. Hasta el punto de que se conservan cartas del «prisionero español» escritas en perfecto inglés. El depositario del tesoro, que necesitaba una pequeña suma para recuperarlo, podía ser ahora un militar que había huido con los fondos del ejército, una viuda, o un intermediario entre el receptor y el prisionero, que quería pagar su defensa.

—Cuando la víctima pagaba, surgían unos inoportunos imprevistos que se solventarían rápidamente, con otra pequeña suma. Pero no se solventaban, y la víctima seguía soltando dinero hasta que se cansaba. Entonces el «prisionero español» desaparecía para siempre en la profundidad de las ficticias mazmorras.

Como ahora en la red. Es increíble, pero miles de personas continúan picando en pleno siglo XXI.[87]

El suboficial Viota tenía toda la razón: si estás avisado, si eres consciente de que estos timos están a la orden del día, lo más probable es que no caigas en la trampa. Pero por desgracia aún hay gente que de verdad cree posible que un abogado de Burkina Faso le escriba (precisamente a él) para proponerle un negocio suculento, o que le toque una lotería a la que nunca ha jugado…

—Que no, mamá, que no. Que eso es un timo. No se te ocurra pinchar en ese enlace.

—¿Enlace? Ay, hijo, qué raro hablas. Yo no sé qué es eso. Te digo que me avisan por la internet de que me ha tocado la lotería. Qué ilusión, a mí nunca me había tocado.

—El enlace son esas letras en color azul que deben aparecer en la parte de abajo del mensaje que has recibido, mamá. ¿Y cómo te va a tocar la lotería, si no llevas ni un número? Te digo que eso es un timo. Y te lo repito, no pinches en las letritas azules.

Desde que inmigró a la cultura digital, las llamadas de mi madre se sucedían cada vez que se encontraba algo inusual en su correo. Yo había sido muy estricto con eso. Y sus llamadas eran cada vez más frecuentes, porque cada vez la industria del cibercrimen encuentra nuevos vectores de ataque para personas tan vulnerables, informáticamente hablando, como ella. La llamada «brecha digital», que es como los expertos llaman a la distancia que separa a los nativos de los inmigrantes digitales, se agranda en lugar de acortarse, ante la velocidad con la que cambian las tecnologías e irrumpen nuevas ciberamenazas.

Y un año después, la historia se repetiría. Pero en esa ocasión, a gran escala…

Ransomware: el cibertimo de Correos

—Mira que te lo dije, mamá, si no conoces al remitente, no lo abras…

Odio este intercambio de papeles. Antes eran los padres los que enseñaban a sus hijos, los que los cuidaban y los que les regañaban cuando hacían las cosas más. En la actualidad, la revolución digital ha invertido los papeles, y ahora son los nativos digitales, más familiarizados con la tecnología que domina cada vez más nuestras vidas diarias, los que deben tutelar a sus mayores para que no se metan en líos. Porque se meten. Y cada vez con más frecuencia.

—¡Pero si el remitente era Correos! —respondió mi madre, indignada—. Con su logotipo y todo. Me decían que me había llegado un paquete el 29 de abril y que no habían podido entregarlo, y que pinchara en las letritas azules para ver quién lo mandaba. ¿Qué querías que hiciera? ¿Y si es importante? Pero ahora no puedo verlo porque se ha bloqueado todo el ordenador…

Entre febrero y mayo de 2015 cientos de miles de españoles recibirían un email similar. Y muchos pincharían en las «letritas azules», como las llama mi madre. ¿Resultado? En unos segundos su ordenador quedó bloqueado, todos los datos de su disco duro cifrados, y un mensaje en la pantalla les indicaba que si querían recuperar sus fotos, vídeos, documentos, etcétera, tenían que pagar una suma de dinero. En torno a 300 euros por víctima. Era la última mutación del *ransomware* CryptoLocker, y un ejemplo inmejorable de la astucia con que evoluciona el cibercrimen, y de la vulnerabilidad de los inmigrantes digitales como ella.

Un *ransomware* es un tipo de *malware,* un programa informático malicioso, que tiene la capacidad de bloquear el acceso a determinadas funciones del ordenador que ha infectado. Entran en nuestra máquina a través de un correo electrónico *spam,* que nos invita a visitar una página. En este caso la supuesta web de Correos. Y así se ejecuta el virus. Y luego los que lo han metido te piden un rescate (*ransom*, en inglés) para limpiarlo.

La explotación del *ransomware* arrancó en los países del Este, con las bandas de cibercrimen organizado. Especialmente en Rusia. Pero a partir de junio de 2013 comenzaron a atacar otros países tras cambiar la apariencia del ataque, y adaptar un remitente al perfil de usuario escogido, mutando sin cesar para evitar ser detectados… Solo en el primer trimestre de ese año, la prestigiosa empresa de software McAfee publicó que había detectado más de 250.000 tipos de *ransomwares* únicos. El de Correos sería solo su última apariencia.

Pero nada, a mi madre ni siquiera le convencía lo que le digo siempre:

—¿Tú crees que una institución oficial o cualquier empresa seria, te escribiría «tendrá derecho a reclamar una indemnización a usted para el esta manteniendo en la cantidad de 8,95 euros por cada día de cumplir»? ¡Pero si esto ni siquiera es castellano!

Mira antes de cruzar la calle. Lee antes de pinchar un link…

—Eso no puede ser —me decía un tanto asustada mi madre—. ¿Cómo van a tener mi correo unos mafiosos rusos? El tuyo vale, que no paras de darnos disgustos con los sitios en los que te metes. Que a tu padre lo vas a matar un día de la preocupación… Pero ¿el mío? ¿De dónde van a sacar unos criminales mi email?

Mi madre seguía sin ser consciente de que algo tan inocente como reenviar una foto, un chiste divertido, o un llamamiento solidario tras una tragedia a todos tus contactos, sin proteger sus correos, puede estar incrementando los archivos de los cibercriminales que han iniciado esa cadena. Al final esa tierna foto, ese vídeo humorístico, o esa petición de ayuda ante tal o cual catástrofe regresa a los criminales con miles de direcciones de email operativas. Porque cada amiga de mi madre le reenviaba a su vez a todas sus amigas ese correo. Y esas a las suyas. Y así en una cadena sin fin que facilita a los atacantes la información que necesitan: qué correos electrónicos están funcionando y cuáles no. Así ya saben a quién deben dirigir el siguiente email con el virus.

A los cibercriminales no les importa que un porcentaje alto de los receptores de sus emails envenenados no caigan en la trampa. Si lanzan un millón de emails, con que solo un 1% de los receptores sientan la tentación de «pinchar en las letritas azules», ya tendrían 10.000 ordenadores infectados y bajo su control. A 300 euros por víctima… es una fortuna.

Obviamente, mi madre no pagó. No tenía nada en su ordenador que fuese de vital importancia. Sin embargo, en abril y mayo de 2015 miles de usuarios españoles, y millones en todo el mundo incluyendo a infinidad de empresas, verían cómo todos sus archivos se esfumaban a causa de una maldita campaña de *ransomware*. Según el FBI, las pérdidas ascendieron a 18 millones de dólares.

En España, mis nuevos amigos, consultores de seguridad, no daban abasto. Cientos de pequeñas y medianas empresas caerían en la trampa. Yo conocí a algunas de esas víctimas. De la noche a la mañana, el trabajo de años, la contabilidad, los listados de clientes y proveedores, etcétera, todo había desaparecido. Algunos de ellos aceptaron el chantaje y pagaron a los criminales, pero la mayoría de las veces ni siquiera así restituyen los archivos cifrados. Y si lo hacen, el programa que debe recomponer el ordenador llega con otro virus escondido que se activará pasado un tiempo para exigir un nuevo rescate. Un infierno.

Esconder el *ransomware* bajo la apariencia de un mensaje de Correos fue una idea brillante. Casi todo el mundo, especialmente las pequeñas empresas, envía o recibe paquetes en alguna ocasión. Era una tapadera perfecta para colocar el virus. Pero sería un error pensar que solo debemos desconfiar de los emails del servicio postal. Debemos desconfiar de todo.

La de Correos fue la última versión de una estafa que comenzó dos años antes, en 2013. En otras campañas los delincuentes utilizaban la tapadera de la Policía o la Guardia Civil. En otros países, el virus se escondía tras la pantalla del FBI, la Gendarmería, Scotland Yard… En algunos casos, los atacantes más sofisticados

incluían en el código una aplicación para que el mensaje que aparecía en la pantalla fuese personalizado, con tu dirección de email, la IP del ordenador e incluso activando la webcam en remoto, para que la víctima se viese a sí misma en la pantalla de su ordenador, y se sintiese aterrada al creer que el FBI o la Policía le estaba vigilando en ese instante para que pagase la supuesta multa. Y pagaban, vaya si pagaban…

Diseñaron distintos disfraces en función del país donde vivían los usuarios de las direcciones de email previamente compiladas. O simplemente escondían el virus en páginas web, y cuando un usuario confiado las visitaba, infectaban su ordenador. Como ocurrió con la página web de la actriz Marta Torné en 2007.

Pero por desgracia, una campaña de spam o una web infectada no son las únicas formas que tienen de entrar en nuestro ordenador. O en nuestra vida. Por eso es tan importante, no me canso de repetírselo a mi madre, aceptar las actualizaciones de los programas, vigilar el navegador y desconfiar, siempre desconfiar.

Roi, un estafador en serie

La llamada de mi madre para darme la buena noticia de que «le había tocado la lotería británica» me pilló camino de Málaga para reunirme con una de las víctimas de las estafas en la red. No podía ser más propósito.

—Pero ¿cómo va a ser un timo? —insistía—. Si viene todo muy bien explicado. Con sus sellos del Banco de Inglaterra y todo…

—Déjalo. Tú no hagas nada. Ya me ocupo yo de borrarlo desde aquí.

Borré el mensaje de spam en el correo de mi madre y continué camino. La joven que me esperaba no tiene nada en común con mi madre, salvo que ambas cometieron el error de pensar que puedes fiarte de lo que llega a través de la pantalla de tu ordenador.

Yo no sé, no puedo saberlo, por qué Blanca entró en aquella página. Quizá por curiosidad o por aburrimiento. Tal vez por morbo, o porque tenía la esperanza de encontrar allí a un hombre interesante, íntegro, divertido, inteligente… Lo que no encontraba en la calle. Pero los motivos tampoco son importantes. Lo importante es que todos los días, todas las noches, millones de chicas como ella entran en páginas parecidas, en busca de un hombre especial. Hijas, madres, sobrinas, hermanas, amigas… podía haberle ocurrido a cualquiera. De hecho, les ha ocurrido a muchas. Con el mismo miserable y con otros miserables parecidos.

Por avatares del destino, Blanca había tenido una relación muy cercana con Jorge V., mi viejo camarada de Blood & Honour y ahora compañero de Pepe en la Policía. De ahí nuestra amistad. A veces el mundo es un lugar muy pequeño… Joven, guapa, inteligente. Psicóloga social, con un Máster en Intervención Psicosocial y Comunitaria, Blanca no es estúpida. Todo lo contrario. Descendiente de una gran familia vinculada a las Fuerzas Armadas, se le presupone además un instinto para advertir de un peligro inminente como el que la amenazaba, pero una de las cosas que aprendí de su amarga experiencia es que, si le ocurrió a ella, le podría ocurrir a cualquiera… A menos que no tenga corazón. Porque para el perfil de ciberdelincuente con el que se topó Blanca en la red, los sentimientos son el vector de ataque.

Nuestra primera entrevista fue en su casa, en Málaga. Supongo que se sentía avergonzada por lo que me iba a contar, así que opté por eliminar la grabadora.

La primera noticia sobre Roi —el caso más longevo, sangrante e infame de «estafador emocional en serie» que he encontrado en la red— la escuché de sus labios. Ese de «Roi» es uno de los diferentes alias que utiliza en la red. Tú podrías habértelo encontrado bajo la identidad de Ravenshill, Redhood, Adrian, Roy, Roy P. A. Varafinder, Leto, Shrapnel, Vanger, wardog, winter, wayreth, Ravnos o Voivoda. Utiliza muchos nombres.

—¿Cómo conociste a Roi?

—En www.adoptauntio.es.

—¿Una web?

—Sí, una web de contactos.

Adoptauntio alcanzó cierto protagonismo mediático en 2013, como adaptación española de la exitosa web francesa Adopteumec.[88] Por una vez las mujeres no eran las cosificadas. Desde su aparición, el 2 de abril de ese año, los hombres eran expuestos y clasificados en función de sus características: zanahorios, rockeros, «geeks», tatuados y perforados, simpáticos, bigotes, barbas, rizos… Ahora eran ellas las que podían examinar el catálogo de pretendientes, y echarse unas risas a costa de nuestras aspiraciones de donjuán. A la empresa le fue bien. La página evolucionó saltando de la web a la app, y en 2015 llegó a contratar anuncios en la televisión nacional, lo que implica que los ingresos se multiplicaban.

Adoptauntio era solo uno de los cotos de caza de Roi. Blanca y él se conocieron allí, aunque bien podrían haberse conocido en cualquier otra red social o página de contactos, como Facebook, Badoo, etcétera. Las hay a decenas y Roi y otra gente como él se infiltran en ellas, da igual lo serios o minuciosos que sean los criterios de verificación. No siempre está en mano de las empresas evitarlo, sino en las nuestras.

—¿Cómo fue el proceso de acercarse a ti?

—Me mandaba mensajes. Mejores que lo normal. Tampoco muy pedantes. Pero al menos tenía temas de conversación interesantes y, evidentemente, mostraba interés por lo que decías. Luego me pidió el teléfono y pasamos al WhatsApp, lo que le permite hablar más. La verdad que estaba toooodo el día escribiendo y luego hablando por teléfono. Está pendiente de ti, notas que te escucha, muestra interés en ti como persona, no como un trozo de carne con tetas y ojos.

Por descontado, en ese momento Blanca no podía imaginar que Roi alternaba ese «interés» y atención a través de internet y WhatsApp, con varias docenas de chicas de manera simultánea…

—Tú eres una tía inteligente, con formación. Y Roi no parece precisamente un Brad Pitt… ¿Cómo pudo atraerte?

—Utiliza la conquista a distancia, para que cuando veas ese pedazo de orco delante no te sientas tan superficial por juzgarle por el aspecto. Esa es la técnica: hacerte sentir culpable si le rechazas por su físico, después de ser tan interesante y respetuoso.

De hecho, cuando pude acceder a cientos de fotos y vídeos de Roi, me di cuenta de que cada una de las imágenes subidas a sus perfiles, con distintas identidades, estaba meticulosamente estudiada. Sabía sacarse partido, aunque los trucos de iluminación y cámara no le valían cuando se encontraba de frente con sus víctimas. Pero para entonces todas estaban tan seducidas por sus poemas, sus versos y su oratoria, que el físico pasaba a un segundo plano.

—Por fin lo metes en casa. ¿Cómo era la convivencia?

—Él se tiraba todo el día colgado al teléfono y al ordenador. Todo el día. A mí me importaba poco, porque así yo estaba más a mi bola, ya que me agobiaba tenerle

metido en casa. Luego, de vez en cuando, hacía sus «viajes» y me daba un respiro. Solía irse una semana, más o menos, y siempre en fin de semana.

—¿Notaste algo raro?

—¿Algo? Todo era raro. Siempre estaba metido en grandes proyectos. Hacíamos planes para irnos de viaje un fin de semana, y siempre pasaba algo a última hora y yo me quedaba con las maletas en la puerta esperando.

—Y un día te pide dinero.

—Me pidió una cantidad pequeña, con la excusa de que tenía que pagar no sé qué urgente y la tarjeta no le iba. Como le dije que no, nunca más volvió a intentarlo.

Blanca fue mucho más lúcida que otras víctimas, y quizá por eso Roi no consiguió sacarle nada, pero un buen día recibió un correo electrónico de otra chica que sí había perdido mucho más que su tiempo y su dinero con el joven ciberdonjuán.

—De pronto descubres que no es quien dice ser. ¿Qué pasó?

—Cuando le largué de casa yo ya sabía que algo no cuadraba, y sentí que tarde o temprano sabría quién era… Meses más tarde me localizaron desde Barcelona y me contaron toda la historia. Flipé, pero tampoco me extrañó, ya que me esperaba cualquier cosa.

—Y descubriste que había cientos de chicas en la misma situación… ¿Qué se siente al descubrir algo así?

—Al principio me dio igual, estaba contenta porque por fin había descubierto quién era y me alegré de haberle sacado de mi vida… pero luego, cuando empiezas a oír las historias de las demás, de cómo les ha destrozado la vida el muy hijo de puta, de cómo algunas han terminado endeudadas, denunciadas o en tratamiento psicológico… da una rabia enorme.

—¿Hay muchas afectadas?

—Calculamos unas doscientas. Mira, este es el cronograma que hemos preparado…

Entonces Blanca tomó su ordenador portátil y abrió un documento de Excel. Era un listado ordenado de docenas y docenas de chicas, de distinta edad y perfil social, a las que Roi había «captado» durante los últimos años.

—Pero ¿quién ha hecho esto? —pregunté con asombro, admirado por la increíble ciberinvestigación que reflejaba aquel documento.

—Gloria. Tienes que conocerla.

Los designios de la Providencia siempre son inescrutables. Por algún tipo de justicia divina, el estafador emocional en seriehabía navegado libre durante años por el océano de internet, lanzando sus redes para pescar, al arrastre, a bancos enteros de incautas. Hasta que se topó con un tiburón…

Con un Máster de Marketing *online* por la Universidad de Londres, Gloria es una activa y emprendedora *social media manager,* organizadora de varios eventos de seguridad informática en las universidades del País Vasco, a los que acuden algunos de los primeros espadas del hacking español. No era una simple usuaria. Y Gloria,

una de las víctimas más dañadas por Roi, fue la principal impulsora de la investigación que terminaría por descubrir las miserias del donjuán de las redes sociales.

—A finales de enero va a estar en Fitur, en Madrid —me dijo Blanca—. Si quieres, puedo presentártela…

Los falsos Antonio Salas

Abandoné la casa de Blanca con una profunda sensación de tristeza. Siempre he pensado que quienes trafican con los sentimientos y las emociones deberían ser considerados delincuentes de la peor calaña. Y a pesar de que sus actuaciones no estén tan perseguidas por la ley como debieran, lo cierto es que pueden causar tanto dolor, angustia y tormento como el peor de los crímenes.

Con frecuencia ese tipo de estafadores emocionales en serie, hombres oscuros, de vida gris, adoptan falsas identidades para seducir a sus víctimas. Y no siempre a través de la red.

En agosto de 2013 un policía local de Alicante era detenido por hacerse pasar por agente del CNI para obtener favores sexuales. El falso espía desplegaba toda su elocuencia, y un currado atrezo, para seducir a jóvenes incautas, haciéndose pasar por un intrépido James Bond. Entre mis compañeros periodistas la noticia se trató con evidente guasa y Francisco H. P., el falso agente secreto de cincuenta y seis años, tuvo que soportar todo tipo de chanzas y burlas. Pero a mí no me hizo ni puta gracia…

Cada cierto tiempo, sobre todo tras la publicación de cada nuevo libro o reportaje, vuelve a ocurrir. Resulta tedioso, aburrido y redundante, pero no importa cuántas miles de veces haya repetido lo mismo, siempre hay algún ingenuo, y sobre todo ingenua, que vuelve a caer.

Estoy harto de explicarlo una y otra y otra vez. Lo he dicho en mis libros, lo he repetido en cientos de entrevistas, y he dedicado varios posts de mi blog a aclararlo, pero sigue sucediendo. Espero que esta sea la última vez que tengo que insistir en lo mismo: si alguien te dice que es Antonio Salas, te está mintiendo.Así de sencillo. Y sin excepciones.

La madrugada del 1 de enero de 2014, cinco meses después de la detención del falso James Bond de Alicante, dos buenas amigas, compañeras periodistas, se encontraban celebrando la Nochevieja en la Sala Bikini con un grupo de amigos, cuando se les acercaron dos jóvenes para intentar que la noche y el cotillón tuviesen un buen fin de fiesta. Tras unos minutos de charla intrascendente —me cuentan mis amigas—, y de invitarlas a una copa, los aspirantes a donjuán entraron a saco:

—¿Y vosotras qué estudiáis?

—No estudiamos. Trabajábamos, pero nos hemos quedado en paro. ¿Y vosotros?

—Periodistas —dijo uno.

—Periodismo de investigación —añadió el otro—. Ya sabes. Infiltraciones, cámaras ocultas… No podemos hablar mucho de eso.

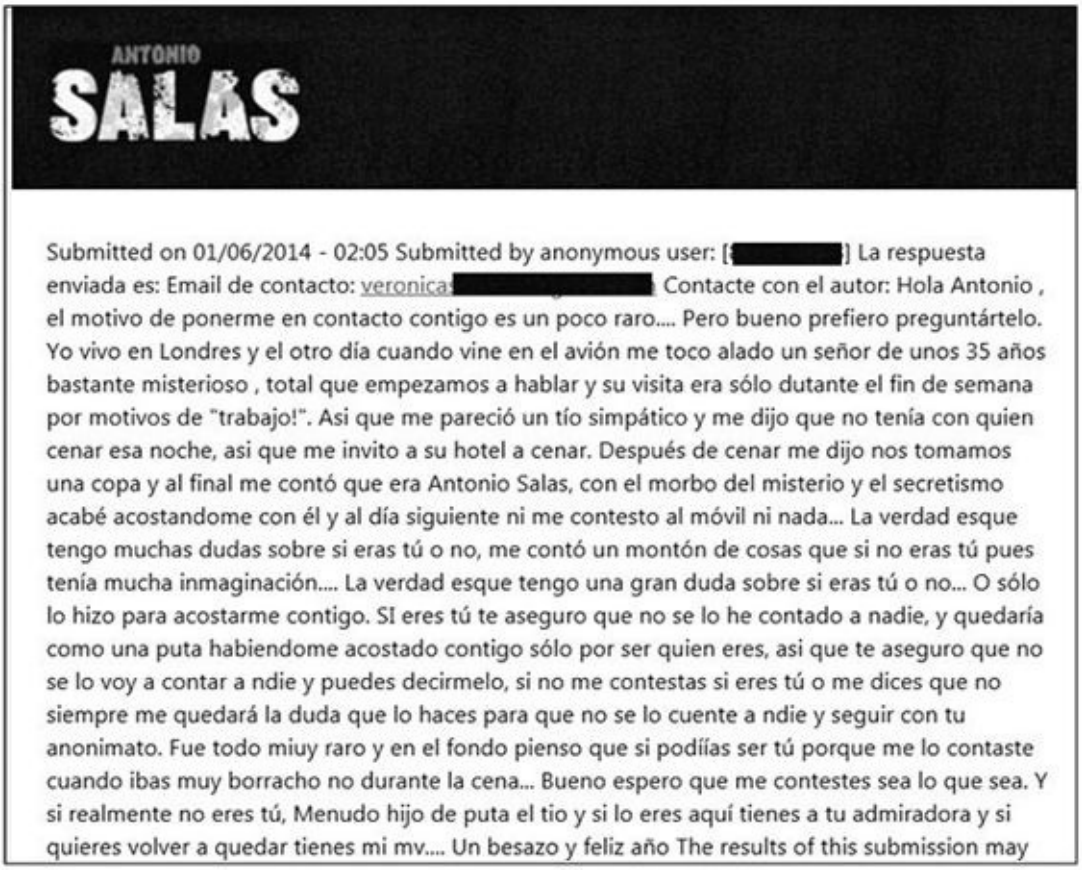
Pero habló, vaya si habló. El más lanzado se ocupó de «vender» a su amigo, al que presentó como «Antonio, un conocido periodista encubierto»:

—Ahí donde lo ves, mi colega es la caña… Quizá hayáis oído hablar de él. Se ha infiltrado en los skin, en el terrorismo islámico y en los Ángeles del Infierno, y yo

soy el que le acompaña en todas sus infiltraciones para cubrirle las espaldas —argumentaba el supuesto reportero, mientras se terminaba el tercer cubata y atacaba con apetito los canapés de jamón.

Mis amigas no daban crédito. Según me cuentan, pasaron un buen rato vacilando a los falsos periodistas, les sacaron un par de copas más y después se volvieron a su grupo de amigos y me mandaron un sms muertas de risa… Pero a mí tampoco me hizo gracia. Cualquiera de mis amigos lectores, incluso aunque no me conozca personalmente, sabe que no bebo, que hace años que no como cerdo y que yo trabajo solo. No existe «el que le acompaña en todas mis infiltraciones para cubrirme las espaldas». Y sabe también que yo jamás, jamás, digo quién soy. No hay excepciones. Por eso repito que si alguien te dice que tal o cual persona es Antonio Salas, miente.

No es la primera vez que ocurre. Ni mucho menos. Y probablemente la anécdota se quedaría en eso, pero una semana después, la noche de Reyes, recibí a través de la web www.antoniosalas.org un nuevo email que reproduzco:


ANTONIO
SALAS

Submitted on 01/06/2014 - 02:05 Submitted by anonymous user: [[redacted]] La respuesta enviada es: Email de contacto: veronica[redacted] Contacte con el autor: Hola Antonio , el motivo de ponerme en contacto contigo es un poco raro.... Pero bueno prefiero preguntártelo. Yo vivo en Londres y el otro día cuando vine en el avión me toco alado un señor de unos 35 años bastante misterioso , total que empezamos a hablar y su visita era sólo dutante el fin de semana por motivos de "trabajo!". Asi que me pareció un tío simpático y me dijo que no tenía con quien cenar esa noche, asi que me invito a su hotel a cenar. Después de cenar me dijo nos tomamos una copa y al final me contó que era Antonio Salas, con el morbo del misterio y el secretismo acabé acostandome con él y al día siguiente ni me contesto al móvil ni nada... La verdad esque tengo muchas dudas sobre si eras tú o no, me contó un montón de cosas que si no eras tú pues tenía mucha inmaginación.... La verdad esque tengo una gran duda sobre si eras tú o no... O sólo lo hizo para acostarme contigo. SI eres tú te aseguro que no se lo he contado a nadie, y quedaría como una puta habiendome acostado contigo sólo por ser quien eres, asi que te aseguro que no se lo voy a contar a ndie y puedes decirmelo, si no me contestas si eres tú o me dices que no siempre me quedará la duda que lo haces para que no se lo cuente a ndie y seguir con tu anonimato. Fue todo miuy raro y en el fondo pienso que si podíias ser tú porque me lo contaste cuando ibas muy borracho no durante la cena... Bueno espero que me contestes sea lo que sea. Y si realmente no eres tú, Menudo hijo de puta el tio y si lo eres aquí tienes a tu admiradora y si quieres volver a quedar tienes mi mv.... Un besazo y feliz año The results of this submission may

Por supuesto respondí al email, aclarando a la interesada que había sido víctima de un engaño. Pero no había sido la primera, ni posiblemente será la última.

La primera vez que tuve conocimiento de que existían estafadores que se hacían pasar por mí fue a través de la revista *Tiempo*. En un artículo firmado por Fernando Rueda, bajo el título «No lo digas cariño, soy Antonio Salas», el periodista mencionaba varios casos de usurpación de identidad del que éramos víctima algunos infiltrados que, por obvias razones, no podemos salir a la luz pública. Casos que

parecían extraídos del guion de la película *Mentiras arriesgadas*, pero que por reales resultan mucho más dramáticos. Describen el oportunismo de esos estafadores sentimentales, que se aprovechan de la ausencia de una cara que relacionar con un nombre, para superponer la suya propia, en busca de favores sexuales.

En concreto, se detallaba el caso de un falso Mikel Lejarza «el Lobo», que Fernando Rueda resumía así:

> Una mujer de Elche me llamó asegurando que llevaba siete años manteniendo relaciones con «El Lobo». Raudo y veloz me fui a verla. Me habló de un hombre que aparecía y desaparecía de su vida continuamente. Que le contaba los detalles de su lucha contra ETA, en la que seguía después de que hubieran pasado casi veinte años de su famosa infiltración en la banda. Que ella le era absolutamente fiel y que estaba locamente enamorada de él. Por una serie de detalles, no tardé en descubrir la falsedad de ese hombre casado que cuando podía iba a acostarse con ella, sin adquirir ningún compromiso…

Es evidente la semejanza con el policía local de Alicante, detenido en 2013.

En el mismo texto se mencionaba también el lamentable episodio de otro de esos falsos «Antonio Salas»:

> En la facultad de Periodismo de esa universidad mediterránea hay un profesor crápula que les va contado a sus alumnas muy íntimamente, muy en secreto, que no digan nada, que nadie lo sabe, pero que él es Antonio Salas, «ya sabes, el periodista de investigación que se ha jugado la vida denunciando a los *skinheads* y a los traficantes de mujeres». Las chicas, según parece, le piden detalles de sus investigaciones, sienten que su admiración por ese profesor crece por momentos y terminan convencidas de que es el hombre de sus sueños. Claro, sienten que no deben traicionar la confidencia personal con nadie… excepto con sus amigas y demás. Así se ha sabido que el crápula ha conseguido mantener relaciones con un buen número de alumnas utilizando a Antonio Salas como disfraz.

Varias webs nazis llegaron a colgar el artículo de Fernando Rueda como advertencia a sus lectores, empeñados en encontrarme, para que no se dejasen engañar por los imitadores.[89] Obviamente ni MarkoSS88, ni Salvador Yanguas, ni el Chino Carías, lo leyeron.

Lo dramático es que cada cierto tiempo y a pesar de que los estafadores les insisten en que no escriban a los emails de contacto que aparecen en mis libros, alguna de las afectadas lo hace, cuando el falso Salas desaparece de sus vidas sin dejar rastro. Y entonces es cuando yo descubro sus dramas.

Los emails que transcribo a continuación son absolutamente reales:

> conocí a 1 persona q aseguraba q era antonio salas, llamado alberto, o duende o muchos más nombres, a veces lo creía a veces no, siempre dudé, pero ahí estaba, fue importante en mi vida. Hace 2 años desapareció, quiero despejar mis dudas, si eres quien pienso sabrás quién soy, pistaaaaaaaaaaa, valencia, fallas, inma, hotel sin pagar, día en valencia con pedro taxi con tu padre recogiendo cosas en el piso de tu expareja Si eres el duende despéjame las dudas en este correo, quiero tener un buen recuerdo del duende, pero las dudas lo impiden, yo estoy bien, SI NO LO FUERAS PERDON, HE LEIDO TODOS TUS LIBROS.

Más dramático si cabe resultó el de otra joven, que me agradeció que la sacase de su engaño, después de relatarme el grado de implicación que ella había puesto en la relación con el estafador.

Asunto: ¿que tal?
Fecha: miércoles, 3 junio, 2009 9:12 PM
De: ……@hotmail.com
Para: *antoniodavidsalas@yahoo.es*

Apreciado Antonio: disculpa mi osadía al escribirte, ya sé que me pediste que te olvidara. Te escribo porque necesito hablar con alguien aunque sea así. Pensaba que me ibas a llamar para darte una explicación del recibimiento que te di en mi casa, no me esperaba tu visita, no tienes nada de cobarde pero sí de timidez

Quizá fue a causa de estas experiencias personales por lo que la historia de Blanca me despertó una particular tristeza. En su caso, el estafador no solo las engañaba para meterse en su cama, también aspiraba a colarse en su vida. Y en su cuenta bancaria. Definitivamente, acudiría a conocer a Gloria a la cita en Fitur, o donde fuese necesario, cuando ella me lo pidiese.

FINALES DE NOVIEMBRE DE 2014
LA PISTA OKUPA

> «En España, bajo la dominación de los árabes, la civilización alcanzó un nivel que raramente se ha repetido. La intromisión del cristianismo ha traído el triunfo de la barbarie. El espíritu caballeresco de los castellanos es efectivamente una herencia de los árabes. (…) Esta religión recompensa el heroísmo, promete a los guerreros la gloria del séptimo cielo.»
>
> Adolf Hitler (28 de agosto de 1942) *Hitler's Table Talk 1941-1944*, pág. 667

Tras la confesión de Markos volvimos a revisar uno a uno todos los emails que nos habíamos intercambiado, todas las entradas en su web, todas las referencias bibliográficas de su libro, todas las actualizaciones y mensajes de sus redes sociales. Todo. Esto fue lo que recopilamos:

Utilizaba diferentes cuentas en redes sociales y distintos correos electrónicos:

Tuenti: NacionalSocialismo Sin Censura

Twitter: ns_sincensuras y markoss88, aunque en su blog menciona una anterior: orgullo_fss

Correos: ns.sincensura@gmail.com, markos.markitos.sb@gmail.com y markoss88.ns@gmail.com

Facebook: NacionalSocialismo SinCensura

Canal en YouTube: https://www.youtube.com/user/markosNSsiempre

El Twitter de Markos se creó en octubre de 2012 y su blog en diciembre, aunque no subió su primera entrada hasta el 21 de enero de 2013. Sin embargo, aparecen mensajes en foros y webs nacionalistas firmados como MarkoSS88 anteriormente.

En un *site* anterior: http://nssc.mforos.com/users/markoss88, un foro sobre NS creado por él, figura una fecha de nacimiento: el 17 de febrero, y una edad: diecinueve años.

Según los comentarios de su blog, habría entrado en prisión por el homicidio del latin king el 22 de marzo de 2013 y habría salido de la cárcel el 25 de junio de 2013.[90]

También teníamos a su novia: Silvia Hierro, estudiante de Medicina de diecinueve años, en alguna facultad universitaria madrileña.

Además, estaba su vinculación a UltraSSur. Y su presunta relación con el Hogar Social Patriota, que sugería haber inspirado.

Había suficientes pistas de las que tirar.

Lo más sencillo parecía investigar la casa okupa nazi. Hacía poco que la primera había sido desalojada por la Policía, y los archivos periodísticos y policiales estaban llenos de información, fotos e imágenes de los «patriotas» identificados en su interior.

Reunimos docenas y docenas de fotografías de los ultras que frecuentaban el hogar social. En este sentido, y como ya había ocurrido durante mi investigación del movimiento neonazi, «los enemigos de mis enemigos» siguen siendo mis amigos. Los foros antifascistas estaban repletos de información sobre la casa okupa fascista. Y eso unido a los archivos de todos los medios periodísticos que habían cubierto la noticia, nos entregaba en bandeja la cara de todos los ultras que habían pasado por el local.

Buscamos, con lupa, una y otra vez. Foto a foto. Fotograma a fotograma… Nada. El rostro de Markos, que conocíamos tan bien gracias a su perfil de Facebook, no aparecía en ninguna de ellas. No iba a ser tan sencillo como habíamos pensado.

Así que nos olvidamos de la cara, y buscamos por el nombre. Entre los identificados en el hogar social había muchos viejos conocidos el mundo ultra y skin: Jonathan A. de Ultras Vallecas; Raúl A., Combat España y actualmente UltraSSur y Liga Joven del MSR; Javier T. M. miembro de UltraSSur y Liga Joven, y así una lista interminable. Todos ellos fotografiados e identificados en las redes antifascistas.

Lo cierto es que en su guerra contra los neonazis, los antifas habían hecho un trabajo sorprendente, filmando a los ultras que visitaban el hogar social y rastreando después las redes sociales hasta conseguir emparejar cada cara, con un perfil. Una labor digna de Anónymous.

Pero solo aparecía un Marcos.

Marcos A., nacido en agosto de 1980. No fue difícil descubrir sus antecedentes, domicilio y DNI haciendo una búsqueda en distintos navegadores, tal y como me había enseñado Selva Orejón: Yahoo, Bing, DuckDuckGo, etcétera. Marcos era un habitual en las notificaciones de sanciones del Boletín Oficial de la Comunidad de Madrid. Y ahí se publica

todo. DNI: 5087…

También había tenido varios encontronazos con el Cuerpo Nacional de Policía, pero solo dos identificaciones por parte de la Guardia Civil.

—¡Ya lo tenemos! —exclamó Álex más entusiasmado aún que yo—. Mírate el email que te mandó MarkoSS88 el 4 de octubre.

Tenía razón. Se notaba que los años en la Unidad de Información del CNP habían potenciado su memoria para retener datos relevantes entre montañas de información estéril. Álex, además, es probablemente uno de los mejores expertos españoles en las Maras, y una de las primeras voces en alertar que estas peligrosas bandas criminales ya se habían asentado en nuestro país. Así que, si él lo decía, tenía que ser verdad. Corrí al archivo de mensajes enviados por Markos, que por precaución capturaba de la pantalla e imprimía… Bendita precaución. Gracias a eso hoy podemos conservarlos tras el ataque a mi correo realizado por Markos en 2015…

En ese email MarkoSS88 me escribía:

> CNP son unos hijos de la gran puta, el otro día tuve problemas con ellos y estoy a ver qué me dicen mis abogados sobre si poner una denuncia o no porque también podría perjudicarme, se volvieron a pasar de la raya, como siempre, yo tengo un libro de aventuras para escribir porque, madre mía, con la GC creo que solo tuve dos «malentendidos» y en pueblos, no en el centro de Madrid. Dicen que están para proteger y defender al pueblo, lo dudo y mucho.

Respiré aliviado. Al menos ahora conocía la identidad de quien confesaba haber intentado matarme. Eso no impediría que continuase en mi empeño por ayudarlo a salir del NS, por convencerlo de que se estaba jodiendo la vida, y la de las personas que le querían, por todo el odio y la violencia que llevaba dentro… pero estaba equivocado. No iba a ser tan sencillo.

En cuanto localizamos las fotografías de Marcos A. en internet —simplemente buscando su nombre y dos apellidos en las redes sociales—, nuestro gozo se diluyó. Nuestro candidato no se parecía en nada a las fotografías que llenaban los perfiles sociales de Silvia Hierro y su novio. Aunque ambos eran altos y atléticos, Marcos A. no era un cabeza rapada voluntario, sino forzado por una precoz alopecia. Además, nuestro candidato era cinco años mayor que MarkoSS88. El primer intento erró el tiro. Debíamos abrir otra línea de investigación. Y eso hice: había llegado el momento de volver con UltraSSur.

A finales de 2014, el movimiento neonazi volvía a estar de rabiosa actualidad. Un año antes el director de *Infolibre* se puso en contacto conmigo para pedirme un reportaje sobre la situación de la extrema derecha en Europa, que se publicó en el número 9 (diciembre de 2013). Y mi admirado colega Ildefonso Olmedo, director de *Crónica* del diario *El Mundo,* me pidió

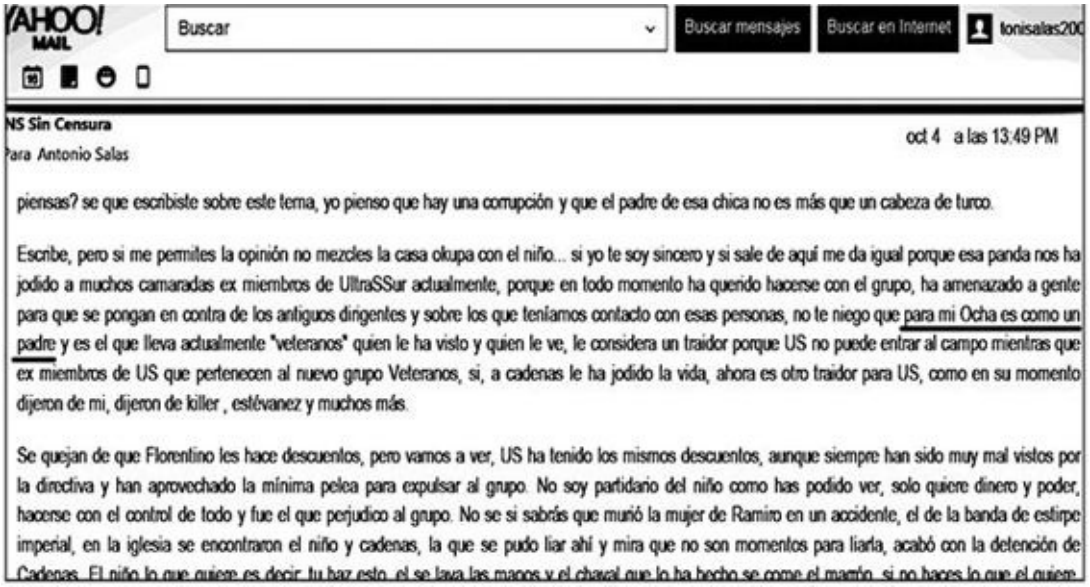
un texto sobre Antonio Menéndez, alias «el Niño», el nuevo líder de UltraSSur tras la guerra interna que sufría la peña ultra del Real Madrid. Hasta ese instante no se conocía la cara de nuevo líder de UltraSSur, pero el Niño era un viejo camarada con el que tenía muchas cosas en común. Mi reportaje sobre él se publicaría en la edición del 8 de diciembre y levantó un gran revuelo.[91]

Pero aunque Markos siempre se mostró crítico con el sector liderado por Menéndez, nunca traicionó a sus camaradas. Jamás. Prometo que no me facilitó ninguna imagen ni dato sobre él. Como demuestra la fecha de publicación de mi artículo, yo ya disponía de esa información antes de que MarkoSS88 entrase en mi vida. Para desgracia de Antonio Menéndez, yo había tenido una relación muy cercana con la familia de su novia, hoy abogada en el bufete de su padre, catedrático de Derecho en una universidad madrileña. Y sobre todo había tenido una estupenda relación con su «cuñado». Así que no me fue difícil ponerle cara. La única ventaja de mantener el anonimato es que, en momentos así, puedes volver a por más información, sin que nadie sospeche de ti.

Así pues, MarkoSS88 no me ayudó en ningún momento, salvo cuando utilizó el reclamo de que había descubierto mi identidad o la dirección de Alfon —una ayuda involuntaria, por otro lado—. Sin embargo, en octubre de 2014 Ildefonso Olmedo me propone escribir algo sobre el repunte nazi a raíz de los hogares sociales neonazis de Madrid.

Sabía que Markos había comentado a algunos camaradas suyos que hablaba con Tiger88, y ante el riesgo de que alguno de ellos pudiesen sospechar que me facilitaba información sobre el movimiento, le escribí para pedirle su autorización antes de redactar el reportaje. No estaba dispuesto ponerle en peligro por un par de artículos, y menos aún cuando mi intención seguía siendo sacarlo de ese mundo.

Markos me autorizó a escribirlos, y durante algunos emails profundizamos sobre su relación con UltraSSur. En uno de sus correos de octubre había definido a José Luis Ochaíta, el anterior líder de los ultras, «como un padre», literalmente.


YAHOO! MAIL Buscar Buscar mensajes Buscar en Internet tonisalas200

NS Sin Censura
Para Antonio Salas
oct 4 a las 13:49 PM

piensas? se que escribiste sobre este tema, yo pienso que hay una corrupción y que el padre de esa chica no es más que un cabeza de turco.

Escribe, pero si me permites la opinión no mezcles la casa okupa con el niño... si yo te soy sincero y si sale de aquí me da igual porque esa panda nos ha jodido a muchos camaradas ex miembros de UltraSSur actualmente, porque en todo momento ha querido hacerse con el grupo, ha amenazado a gente para que se pongan en contra de los antiguos dirigentes y sobre los que teníamos contacto con esas personas, no te niego que para mi Ocha es como un padre y es el que lleva actualmente "veteranos" quien le ha visto y quien le ve, le considera un traidor porque US no puede entrar al campo mientras que ex miembros de US que pertenecen al nuevo grupo Veteranos, si, a cadenas le ha jodido la vida, ahora es otro traidor para US, como en su momento dijeron de mi, dijeron de killer , estévanez y muchos más.

Se quejan de que Florentino les hace descuentos, pero vamos a ver, US ha tenido los mismos descuentos, aunque siempre han sido muy mal vistos por la directiva y han aprovechado la mínima pelea para expulsar al grupo. No soy partidario del niño como has podido ver, solo quiere dinero y poder, hacerse con el control de todo y fue el que perjudico al grupo. No se si sabrás que murió la mujer de Ramiro en un accidente, el de la banda de estirpe imperial, en la iglesia se encontraron el niño y cadenas, la que se pudo liar ahí y mira que no son momentos para liarla, acabó con la detención de Cadenas. El niño lo que quiere es decir tu haz esto, el se lava las manos y el chaval que lo ha hecho se come el marrón, si no haces lo que el quiere

En la guerra por el poder que se estaba viviendo en la cúpula de UltraSSur, Markos se decantaba sin ambigüedades por el sector más veterano, reseñando su amistad con Ocha y con Álvaro Cadenas, protagonistas ambos de *Diario de un skin*. Otra línea de investigación oportuna para poner nombre a quien trató de asesinarme.

Aproveché un viaje a Madrid para regresar a la calle Marceliano Santamaría, donde vivía un buen amigo, y preguntar por MarkoSS88…

Regresar a la calle de los UltraSSur, donde todo empezó, donde viví algunos de los momentos más intensos de mi carrera, y uno de los escenarios fundamentales de *Diario de un skin,* resultó sobrecogedor. Volver a pisar aquel asfalto, ahora sin las Dr Martens con punta de acero, rodeado de ultras que serían felices reventándote la cabeza con un bate de béisbol, no es tranquilizador. Por suerte he mantenido contactos cercanos a la cúpula del movimiento todos estos años, y un motero con pinta de Ángel del Infierno no desentona entre los skinhead neonazis. Pero el resultado no pudo ser más descorazonador.

El territorio de UltraSSur seguía igual. El Drakkar, que yo conocí como Moai y antes como Mr. Raff, continuaba siendo el punto de encuentro de los ultras, a pocos metros del Bernabéu, pero nadie conocía a Markos. Ni siquiera Ocha o Cadenas. Aseguraban estar al tanto de la existencia del blog, pero para ellos su autor era tan desconocido como para mí… ¿Cómo era posible?

En un correo enviado el 11 de noviembre de 2014 se lo pregunté directamente:

> La semana pasada estuve en Marceliano Santamaría. Tiene cojones volver a la calle de UltraSSur después de tanto tiempo. Tengo un buen colega allí y tenía que verlo por la nueva investigación, pero fue antes de que me mandases tu mail, si no le habría preguntado. Lo que sí hice fue preguntar por ti… y es extraño que nadie te conozca allí, ¿no? ¿Cómo me explicas eso?

Markos me contestó ese mismo día:

> … lo de US creo que te lo conté yo: al salir de la cárcel me dieron de lado. Yo me posicionó a favor de Cadenas y de Ocha. El Niño y yo amigos precisamente no somos. Como yo hay más, pregunta por Javier Estévanez o por Killo, otros que pasaron por la misma situación. Pregunta por David Castillo, exdirigente de la sección de bcn, te dirán que es un traidor, los amigos de Ocha, de Cadenas, no somos bien recibidos y cuando yo estuve en la cárcel se encargaron de amenazar a los míos diciendo que si decían que me conocían, que se olvidaran de US y tengo pruebas y gente que me lo ha afirmado. Tú vete dando señales de vida anda, yo veré lo que puedo hacer.

La pista de UltraSSur había resultado tan infructuosa como la del hogar social. Markos siempre tenía respuesta para todas las incongruencias de su historia, pero aquello empezaba a emanar un tufillo extraño…

Capítulo 10
Esteganografía, hacking wifi y espionaje

«Nuestra habilidad para entender el mundo en que vivimos depende fundamentalmente de los intercambios no autorizados y no vigilados entre los periodistas de investigación y sus fuentes.»

Edward Snowden, en el prólogo a *El pequeño libro rojo del activista en la red*, de Marta Peirano

CyberCamp: «Buscamos talentos»

El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Industria, Energía y Turismo y de Red.es. Fundado en 2006, con el nombre de Instituto Nacional de Tecnologías de la Comunicación (INTECO), el 28 de octubre de 2014 cambió su denominación a INCIBE, según el acuerdo adoptado en Junta General del 27 de octubre de 2014 con el Gobierno de España. Con dicho cambio de denominación e imagen, INCIBE reestructura estratégicamente su infraestructura, enfocándola más hacia la ciberseguridad.[92]

Al menos desde 2005 y hasta 2013, INTECO organizaba el Encuentro Internacional de Seguridad e Información (ENISE), reuniendo en León a lo más granado del mundo de la ciberseguridad. Para entonces, INTECO ya contaba con unos recursos envidiables y envidiados. El presidente Zapatero había puesto mucho empeño en que León, su ciudad, contase con el centro, que recibía subvenciones millonarias cada año. Con 73 empleados directos, las empresas vinculadas al Instituto daban trabajo a setecientas personas en el sector de las nuevas tecnologías, así que Zapatero podía estar orgulloso.

Pese a su incuestionable cualificación, ni siquiera INTECO se libró del ataque de los *blackhats*. En 2006 el Instituto señero de la Seguridad Informática en España sufrió un acceso no autorizado a sus servidores, y el robo de datos de 20.000 usuarios de su plataforma de formación *online*.[93]Pero el lamentable incidente no consiguió frenar el ascenso de INTECO y en 2014, ya convertido en INCIBE, organizó el mayor evento sobre Seguridad Informática de la historia de España: CyberCamp. Y yo estaría allí.

A diferencia de otras convenciones, como X1Red+Segura o Navaja Negra, la CyberCamp es un evento colosal, inmenso, y un poco caótico.

En 2014 la CyberCamp se celebró en el Pabellón Multiusos I, el antiguo Madrid Arena, un recinto tristemente conocido por la tragedia que el 1 de noviembre de 2012 se saldó con cinco jóvenes muertas y docenas de heridos. Dos años después, el inmenso pabellón, situado en el recinto ferial de la Casa de Campo, recibía a algunos de los especialistas más reputados del planeta en hacking y seguridad informática.

Más de 4.000 visitantes. 206 ponentes. 14 conferencias magistrales en el Auditorio Central y otras 21 en las diferentes salas habilitadas. 23 talleres para formación de padres y familias, 18 talleres destinados empresas y proyectos y 17 talleres técnicos sobre criptografía, *reversing*, hacking wifi, *exploiting*, forense, auditoría de código, hacking web, etcétera. A lo que había que sumar los *hackatones*, y una infinidad de charlas y comunicaciones presentadas por diferentes empresas que «buscaban talentos». Y docenas de expositores del Ejército, la Guardia Civil, o empresas como Buguroo, que también «buscaban talentos» y que flanqueaban todo el perímetro de la segunda planta. Una locura. Imposible asistir a todo.

Cientos de especialistas llegados de todo el planeta se dieron cita en aquel evento, brindándome la oportunidad de asistir a conferencias, talleres y cursillos intensivos a cual más fascinante.

Allí tuve la oportunidad de conocer a personajes ilustres, como Richard Stallman, principal impulsor y referente moral del software libre, provocador y audaz en sus planteamientos informáticos. Como Joanna Rutkowska, investigadora polaca especializada en *malware* y fundadora de Invisible Thing Lab, y una de las pocas mujeres en la primera línea del hacking internacional. Como Antonio Ramos, director del programa de referencia *Mundo Hacker* que para entonces ya me había empollado, rastreando en YouTube, Vimeo y demás plataformas todos los capítulos emitidos tanto en Discovery Max, como en GlobbTV. Más que recomendable.

Fueron tres días de locura. En las tres plantas del pabellón se celebraban, al mismo tiempo, conferencias, seminarios, talleres y cursos simultáneos, obligándome a dejar la cámara de vídeo en uno, la grabadora en otro y asistir a un tercero, tomando notas como un loco. Corriendo permanentemente de una sala a otra, y de una planta a la superior, y luego a la inferior, para cambiar las tarjetas de memoria e incorporarme lo antes posible a la siguiente. Podría escribirse no uno, sino varios libros, detallando el brutal torrente de conocimientos e información sobre hacking que se vertió allí durante esos días.

Todas fueron magistrales, y profundamente enriquecedoras. Sobre todo para un profundo ignorante que estaba empezando a conocer el mundo de la seguridad informática. Y aprendí tanto, que solo puedo estar agradecido a cada uno de los participantes, imposible reseñarlos a todos. A algunos, como Fernando de la Cuadra, Juan Antonio Calles, David Insonusvita, Blanca Tulleuda o Angelucho, ya los conocía de X1Red+Segura. A otros, como Francisco Pérez Bes, abogado y secretario general de INCIBE, ya los había visto en otros eventos de seguridad informática. Pero a otros solo los conocía a través de sus libros. Como es el caso de Alejandro Ramos, que me ayudó mucho sin saberlo con su magnífica novela *Hacker épico*.[94]

Ellos no me conocían a mí, pero yo a ellos sí. Cuando ocho meses más tarde Alejandro Ramos contactó conmigo en Twitter, y le revelé que, además de en la CyberCamp, yo había asistido «clandestinamente» a otras conferencias suyas, no se lo quería creer. Tuve que enviarle las fotos que había tomado en sus charlas para demostrarle que no era un farol.

Allí estaba también Javier Marcos, uno de los poquísimos españoles fichados por el Departamento de Seguridad de Facebook, y recién llegado de los Estados Unidos para compartir con nosotros el punto de vista de la seguridad, desde dentro de un gigante como la red social de Mark Zuckerberg. Y el genial Chema Alonso. Nadie comunica mejor el mundo del hacking que «el Maligno». Yo he gozado con cada una de sus conferencias, incluso cuando no entendía ni una palabra sobre los aspectos técnicos. Pero si alguien ha conseguido hacer asequible este mundo, es él.

También pude conocer, por fin en persona, a la inspectora Esther Aren, que junto

a la inspectora Silvia Barrera y Carolina González ponen un rostro femenino al Cuerpo Nacional de Policía en las redes. De hecho, antes de aquel día, a Esther solo la conocía por su activa presencia en Twitter como @chicageo68. A Silvia la entrevistaría al año siguiente, tras su ascenso al mando de la Brigada de Delitos Informáticos del CNP, en circunstancias un poco más accidentadas.

Con algunos de los participantes en la CyberCamp que conocí aquellos días, y que naturalmente no sabían quién era yo —absolutamente nadie sabía que estaba allí — surgió una empatía especial. Como con Eduardo Alberto Sánchez Ferrezuelo, director de Comunicación y Marketing de Buguroo, una de las empresas patrocinadoras de X1Red+Segura, que solo en este momento descubrirá quién era el pesado que le hacía tantas preguntas. Me disculpo por la clandestinidad que implica mi oficio.

Otros me impresionaron por el contenido de sus conferencias. Como es el caso de M. Ángeles Pérez García, psicóloga salmantina, que consiguió estremecerme con los casos de ciberacoso que expuso en sus charlas. O Sara Degli Esposti, investigadora del Center for Research into Information Surveillance and Privacy (CRISP) en la Open University Business School (UK) y directora del Proyecto Big Data Protection, que dibujó un panorama siniestro de la criminalidad en la red.[95]

Allí estaban muchos de los colaboradores habituales del programa *Mundo Hacker* que me habían acompañado tantas madrugadas. Y lo fantástico es que varios de ellos ofrecían talleres intensivos sobre algunos de los aspectos más fascinantes del hacking.Como Ángel Ochoa y Jesús González, que dirigieron dos talleres sobre *exploiting* y hacking web, a cual más fascinante. Solo faltaba el gran Dimitri. Los seguidores del programa sabrán a quién me refiero… Pero el taller que más me impresionó fue sin duda el de Yago Hansen, «el hombre wifi»…

Hacking wifi

Durante varias horas, Yago Hansen compartió con los asistentes a su taller sobre hacking wifi alguno de los secretos que lo han hecho merecedor de ese cariñoso mote. Y mientras estaba atento a su conferencia, no pude evitar acordarme de un comentario que me había hecho meses atrás el capitán César Lorenzana, *whitehat* de la Guardia Civil:

—El hacking wifi es otro mundo —me había dicho—. Ya no tiene que ver con programación con sistemas… Son señales radioeléctricas. Todo lo que emites a la red son ondas radioeléctricas y pueden ser capturadas. Por ejemplo, imagina que te vas a un hotel y el atacante sabe que estás en ese hotel. Cuando te conectas a la wifi pública, todos los usuarios conectados ven que estás ahí. A menos que lo hagas de forma invisible, y no aparezcas entre los conectados a la red. Pero claro, si el atacante va a por ti y sabe que estás ahí, te va a localizar. O puede utilizar una antena wifi desde allí —añadió señalando la azotea del edificio de enfrente a su despacho—, orientarla hacia tu ordenador y estar pillándote la señal… Por eso tienes que encriptar las comunicaciones. Las pueden pillar igual, pero van a tener que desencriptarlas después…

Ahora Hansen estaba dispuesto a proporcionarme una demostración en vivo. Se había traído, para mostrarnos a sus asombrados alumnos, algunos de sus «juguetes» más preciados. Antenas capaces de interceptar la señal wifi de un usuario a más de medio kilómetro de distancia.

Más allá de los virus troyanos y gusanos, del robo de conexión al vecino, y del *phishing*, el hacking wifi supone otra dimensión de nuestras vulnerabilidades. Ya no es necesario tocar el ordenador de la víctima. Utilizando antenas direccionales, como las que Hansen presentó en aquel taller, es posible introducirse en un sistema desde un coche aparcado en la calle o desde el edificio de enfrente. O lo que es peor, acomodarse en un lugar público, como una terminal de un aeropuerto, el vestíbulo de un hotel o una estación de ferrocarril, y solapar la wifi gratuita legítima del lugar, con una señal que emite el atacante, y que bautizará con un nombre inocente: «wifi gratis», «Renfe», «wifi Barajas», «Hotel Ritz», etcétera. Todo usuario que abra su ordenador o su teléfono móvil y se conecte a esa red estará entregando al atacante todo el contenido de su conexión… Escalofriante.

Por eso es tan importante prestar un poco de atención a nuestro *router*. Esa pequeña cajita que comunica nuestro ordenador con la red suele venir de fábrica con una configuración tipo que incluye contraseñas débiles, puertos sin abrir, velocidad baja… Vamos, que es uno de los puntos más vulnerables de nuestra conexión a y desde internet. Y con las herramientas de auditoría cuyos tutoriales pueden descargarse de la red no es necesario ser Yago Hansen para que te lo pirateen, así que merece la pena dedicarle un poco de tiempo a robustecer nuestra conexión wifi.

Hay muchas cosas que puedes hacer con tu *router*,[96] pero de entrada lo más urgente es cambiar el nombre de usuario y la contraseña que viene de fábrica. Si la que tú tienes es *admin*, mal vamos: son muy conocidas por los ciberdelincuentes, y les resultará muy fácil entrar en tu red. A partir de ese paso existen muchas maneras de restringir o dirigir la cobertura de la señal del *router*, cifrarla, identificar los dispositivos (ordenadores, tablets, teléfonos móviles, etcétera) que quieres autorizar a conectarse a través de tu *router*… Como siempre, todo dependerá del número de capas de protección que quieras colocar a tu cebolla. Ninguna estará de más.[97]

Raúl Siles, que también trató el tema en el mismo evento, lo sintetizó en una frase demoledora: «Si no te atraigo a mi red, yo puedo entrar en la tuya».

Esteganografía: hacking para espías

Otro de los talleres que me resultó especialmente sorprendente fue el que dirigió Alfonso Muñoz: «Taller de ocultación de comunicaciones digitales: esteganografía y estegoanálisis». A pesar de su juventud, Alfonso Muñoz es doctor en Telecomunicaciones con más de diez años de experiencia en el campo de la seguridad informática en los cuales ha trabajado en proyectos con organismos europeos, ministerios y multinacionales en «proyectos avanzados no convencionales». Y probablemente uno de los principales esteganografistas españoles.

A diferencia de la criptografía, utilizada para cifrar o codificar información de forma que solo pueda ser descifrada por el receptor legítimo —por ejemplo los mensajes nazis de la máquina Enigma—, la esteganografía oculta dicha información en un «portador», para que en caso de ser interceptado, nadie pueda sospechar que dicho portador oculta un mensaje. Como si el mensaje de la Enigma fuese escrito con tinta invisible en una hoja de periódico.

La esteganografía —del griego στεγανος *(steganos):* «cubierto» u «oculto», y γραφος *(graphos):* «escritura»—, se concentra en las técnicas que permiten ocultar mensajes u objetos (textos, fotos, vídeos, etcétera), dentro de otros, llamados portadores, de modo que sea indetectable.

Cuatrocientos años antes de Cristo, el historiador Herodoto reseñó en su libro *Las Historias* el primer uso de la esteganografía en la Antigua Grecia, relatando cómo un personaje toma un cuadernillo de dos tablillas, raya la cera que las cubre y donde se escribían los textos, y en la madera misma graba un mensaje secreto antes de cubrirlo con cera de nuevo. El receptor solo tenía que derretir la cera con el texto portador, para acceder al verdadero contenido secreto. En la misma obra, Herodoto describe cómo otro personaje rasura la cabeza de uno de sus esclavos y le tatúa un mensaje oculto en el cráneo. Cuando volvió a crecerle el pelo, lo envió a su destino convertido en objeto portador del secreto. En el libro *Hypnerotomachia Poliphili* («El sueño de Polifilo») de Francesco Colonna, que data de 1499, se incluye otro precedente de la esteganografía. Tomando la primera letra de cada uno de sus 38 capítulos se descubre el mensaje oculto: *«Poliam frater Franciscus Columna peramavit»* («El hermano Francesco Colonna ama apasionadamente a Polia»). Como es lógico, el uso de la esteganografía se potenció en las guerras mundiales. Los mensajes ocultos escritos con tinta invisible sobre otros textos, por ejemplo libros o periódicos, evolucionaron a la par que la química y ofrecieron a los servicios de Inteligencia nuevos compuestos más difíciles de detectar para ocultar sus mensajes. Pero la gran revolución de la esteganografía, subrayaba Alfonso Muñoz en su taller, llegó con la informática.

A diario pasan ante nuestros ojos millones de mensajes secretos ocultos en vídeos, fotografías, foros… Si te descargas porno, libros piratas, o haces compras en eBay, puedes estar compartiendo en tu ordenador personal mensajes de Al Qaeda o del Ejército Islámico.

Durante los últimos años los servicios de Inteligencia israelíes, británicos y norteamericanos han descubierto que, más allá del uso propagandístico de sus webs, la comunicación por cifrado PGP, o la compartición de buzones de correo, los terroristas habían desarrollado la estenografía para transmitir mensajes ocultos, por ejemplo a través del porno, y webs abiertas como eBay o Reddit. A la vista de todo el mundo.[98]

Los analistas se toparon con la sorpresa de que perfiles asociados a organizaciones terroristas, como Al Qaeda, utilizaban por ejemplo el tablón de Reddit para insertar anuncios en apariencia inocuos. Hasta que descubrieron que insertaban caracteres hexadecimales y números primos en el código fuente. Una vez descifrado, según publicó *The New York Post*, se encontraron con información e instrucciones sobre futuros atentados. A partir de ese instante, el Mosad, la CIA y el MI6 concentraron su atención, no solo en el contenido, sino también en el continente de todo lo publicado por los terroristas en la red.

Alfonso Muñoz consiguió fascinarnos a todos los presentes, citando casos prácticos del uso de la esteganografía en operaciones de espionaje, por ejemplo contra mis viejos «amigos» de Hizbullah. Así descubrí que mientras yo visitaba sus dominios en Beirut, o estrechaba una cordial amistad con Issan S., su exjefe de Inteligencia en América Latina, el Mosad escondía los mensajes a sus espías infiltrados en el entorno de Hassan Nasrallah en las etiquetas de botellas de licor.

De la misma forma en que un fichero de sonido puede emplear los bits que el oído humano no puede oír, para reemplazarlos por mensajes, los bits que controlan la gama cromática de las fotografías pueden contener informaciones ocultas. Y eso solo es el principio.

Unos meses más tarde, y durante una de mis reuniones con Hervé Falciani, el informático que hackeó a la banca suiza, me confesaría, por primera vez, que la esteganografía había sido una de las herramientas que utilizó para sacar la información de la «Lista Falciani» de los ordenadores del HSBC…

Muñoz nos mostró un sinfín de ejemplos de mensajes escondidos en fotos, vídeos o textos que viajan cada día por la red ante nuestras narices, sin que nadie pueda imaginar su contenido secreto. Por ello los especialistas en estegoanálisis desarrollan ataques pasivos (detección de los mensajes ocultos) y ataques activos (la anulación o manipulación de los mismos), en una guerra secreta que tiene como campo de batalla el código fuente en la red.

Desde la detección de los primeros usos esteganográficos de internet por parte de los terroristas, servicios como la CIA o el Mosad potenciaron sus departamentos de ciberdefensa, para detectar cualquier amenaza que pudiese transmitirse por la red. El enemigo ya no solo acechaba en el campo de batalla sobre el terreno. Las organizaciones como Al Qaeda habían aprendido mucho desde el 11-S, y habían reclutado a hackers como activos de su guerra contra Occidente. Y de la misma forma en que tenían la habilidad para ocultar mensajes en sus comunicaciones, existía el

riesgo de que pudiesen interceptar o manipular las nuestras.

Precisamente, tres de los participantes en la CyberCamp que más expectación despertaron entre los asistentes fueron la comandante Lorenzo Carrasco, el teniente Francisco J. Garrote y el coronel Enrique Cubeiro, los tres pertenecientes al Mando Conjunto de Ciberdefensa de las Fuerzas Armadas españolas, que presentaron una conferencia titulada «Operaciones en el ciberespacio».

«¡Antonio Salas! ¿Qué haces aquí?»

Creo que adelgacé un par de kilos. Desde que comenzaban las jornadas, a primera hora de la mañana, y hasta que concluían, ya entrada la noche, no paraba de correr de una planta a otra, dejando la grabadora en una conferencia, instalando la cámara de vídeo en un taller y tomando notas en una mesa redonda. Ya tendría tiempo más tarde de escucharlas todas con detenimiento.

En el fragor de mis carreras de un extremo a otro del recinto, recuerdo que en un momento determinado tropecé de bruces con dos tipos que me resultaban familiares.

—Perdón, llevo prisa y no os he visto.

—Nada chaval, no te preocupes…

Me alejé consultando a la carrera el programa de actos, y escogiendo en qué actividad dejaba ahora la cámara, pero con la sensación de que aquellas caras me resultaban familiares… Tardé un buen rato en darme cuenta. «¡Coño, si son Trancas y Barrancas!» Acababa de tropezarme con Juan Ibáñez Pérez y Damián Mollá, los actores que prestan su voz a las famosas hormigas del programa *El Hormiguero,* a los que había conocido años antes, cuando colaboraban con Pablo Motos en el programa *No somos nadie.* En los micrófonos de la Cadena Ser, Motos y su equipo me habían realizado dos de las mejores entrevistas que recuerdo sobre mis primeros libros, demostrando una sensibilidad, especialmente en el caso de *El año que trafiqué con mujeres,* que no percibí en la mayoría de mis colegas.

Pérez y Mollá participaban en varios de los eventos de la CyberCamp, como responsables de las entregas de premios, pero yo en ese momento no lo sabía. Como no podía saber tampoco que mis erráticas carreras de un piso a otro habían llamado la atención de alguien que me había reconocido en medio de aquella locura.

Aunque esperó a que terminasen los actos del segundo día para acercarse a mí, no negaré que me dio un susto de muerte.

Exhausto, me había sentado en una mesa de la cafetería de la segunda planta para acomodar el equipo antes de abandonar el Madrid Arena, cuando alguien se me acercó por la espalda y susurró mi nombre.

—Hombre, Antonio… Eres la última persona que esperaba encontrar aquí…

Casi se me sale el corazón por la boca. Me giré de un salto e hice frente a mi interlocutor, adoptando una posición defensiva. Sobre todo porque, aunque su cara me resultaba familiar, no era capaz de ubicarlo. Y dada la naturaleza de mi oficio, aquello me resultaba terriblemente inquietante…

—Perdóname, sé que te conozco, pero no caigo.

—Tres Cantos.

—¿Cómo?

—La Comandancia. Información…

Respiré aliviado.

—Joder, macho, no vuelvas a hacer algo así. Me has dado un susto de muerte…

El avispado observador que me había identificado en medio de aquellos 4.000 aspirantes a hackers era uno de los guardias civiles del grupo de Información de Tres Cantos, responsables de las operaciones contra Hammerskin. Berto es un *rara avis* en la Guardia Civil. De vocación tardía, llegó al Instituto Armado tras haber servido unos años en el Ejército. Especialista en Telecomunicaciones, sentía un natural interés por el mundo de la seguridad informática, y esta vez me vino de lujo encontrarle.

Berto me aclaró muchos conceptos que no están en los libros, ni en los blogs especializados. Tuvo la amabilidad de prestarme auténticas joyas bibliográficas, como un ejemplar de *La ética del hacker,* de Pekka Himanen, autografiado por el italiano Federico Sauri, encargado de Cisco System Italia, quien necesitó una oficina y un punto de acceso para iniciar remotamente un servidor en sus vacaciones, y a quien Berto le salvó de una situación incómoda facilitándole lo que necesitaba… Sauri pagó con un ejemplar de esa «Biblia» que explica una forma de pensar y vivir: el código hacker.

Pero hay más, de la mano de Berto, y en unas circunstancias tan insólitas como entrañables, conocería meses después a uno de mis «profesores» particulares de hacking ético. Un compañero del guardia civil, gracias a cuyo talento, probablemente, hemos conocido algunas de las historias más escandalosas de política, banca y corrupción, de las que han poblado los informativos en los últimos años. Chus, un guardia civil anónimo y muy alejado de la Brigada de Delitos Tecnológicos de la UCO, es uno de esos hombres que susurra a las máquinas… y las máquinas le responden. Doy fe.

MALLORCA. NAVIDAD DE 2014
COMPASIÓN POR UN NEONAZI

«Con humanidad y democracia nunca han sido liberados los pueblos.»

Adolf Hitler, *El enemigo de los pueblos*, párrafo 6

Finalizando el año 2014 la historia de MarkoSS88 dio un nuevo giro inesperado. Según aseguraba en sus redes sociales, había dejado Madrid para establecerse en Mallorca.

Las cosas no le iban bien. Según me explicaba en sus correos, como exconvicto por una pena de homicidio, no encontraba trabajo, vivía de prestado en casa de un camarada, y todos los martes y jueves tenía que firmar en el juzgado, momento en que, dependiendo del policía de servicio, lo trasladaban a comisaría donde —me aseguraba— con cualquier excusa aprovechaban para encerrarlo en el calabozo y darle una paliza. Me envió varias fotografías de las heridas, contusiones y traumatismos que según él le habían provocado esas palizas. En ninguna de ellas se le veía la cara, aunque no era extraño si se las había hecho él.

Tras confesarme su intento de asesinato, y en apariencia arrepentido por lo que habría estado a punto de hacer, Markos había aceptado que le entrevistase. Creo no equivocarme si afirmo que MarkoSS88 solo había concedido una entrevista en toda su vida… aunque era con trampa. En su blog se había entrevistado a sí mismo en 2013. Una argucia que utilizan muchos autores cuando quieren expresar un mensaje, y la entrevista es el mejor formato. Así se aseguran de que el entrevistador no haga preguntas estúpidas. Aunque no especifica que es él, tras leer todas las entradas de su página no es difícil detectar su estilo y biografía en las respuestas.

Pero una cosa es ser entrevistado por sus «cachorros», y otra por Tiger88. Así que le agradecí sinceramente que me concediese esa oportunidad de intentar atajar «imitadores», que se sintiesen tentados a probar suerte donde Markos había fracasado.

Siempre fui consciente de que quienes me cuestionaban no habían leído mis libros, y que los chavales de catorce, dieciséis o dieciocho años, que eran unos críos cuando se publicó *Diario de un skin,* y que piden mi ejecución en las redes sociales, hablaban con opiniones prestadas. Así que la experiencia de Markos me parecía la mejor manera de ilustrar que era lícito cuestionar mi trabajo, pero solo después de conocerlo. Si alguno de

aquellos chavales tenía la tentación de emular sus pasos, su testimonio podía ayudarme a prevenir males mayores.[99]

Claro, ahora lo veo absurdo —me respondía Markos—. En su día, lo justificaba yo mismo con cualquier excusa. Al principio, cuando empezaste a hablarme, y tú lo sabes, te hablaba con odio, era un sinfín de reproches y de estar alerta. Me sorprendió meterme un día en el correo y ver un mensaje tuyo. Todavía me acuerdo del rebote que me pillé. No sabía qué querías de mí. Me imaginaba cualquier cosa, denunciarme, amenazarme, echármelo en cara… Cuando seguí hablando contigo supe que no era por nada de eso. Llega un momento en el que todos: la prensa, los policías, los guarros, mis propios camaradas, repetían lo mismo, una y otra vez, que eras un traidor, que si les habías jodido la vida, que si detenciones, represiones… Eso se te va quedando en la cabeza y cada vez que se hablaba de ti, era para lo mismo, para decir cuánto daño habías hecho al movimiento. No quería leerme el libro porque consideraba que estaba traicionando a mis principios e incluso al hablar contigo me sentía como un traidor. Ahora… Ahora han cambiado muchas cosas. Me he leído el libro y, sinceramente, tiene su parte negativa, claro, pero también son nuestros actos en realidad, es decir, algunos sí que hemos pegado, hemos amenazado y hemos matado, pero no todos.

También tiene su parte positiva. Muestra muchos sentimientos, de odio, culpabilidad, tristeza, que todos nosotros tenemos. Cómo nos evadimos del mundo, del sufrimiento, y nos vamos a un bar a beber. A un concierto. A una calle… Leyendo el libro se me ha venido a la mente tantos recuerdos, buenos como malos… Ahora no lo veo un tema para matar, sino para reflexionar qué cosas tenemos que cambiar todos en el movimiento. Y sinceramente, limpiar nuestro nombre, enseñar la verdadera doctrina NS.

A medida que lo entrevistaba, enviándole las preguntas por email y repreguntando en función de sus respuestas, su historia personal me encogía el alma. Como a sus ciberamigas o novias antes que a mí.

Cuando yo era niño no era como el resto. Yo me sentaba en el comedor a ver la televisión, a ver los documentales de historia, siempre me ha fascinado la historia, me veía todos… Una vez, en nuestro primer piso, encontré unos libros que hablaban de un tal Adolf Hitler… A mi abuelo por parte de madre, le fascinaba Hitler… Cogí el libro y me lo llevé a mi cuarto. Todas las noches me sumergía en un nuevo mundo, que al principio no entendía muy bien. Yo de por sí era racista y muy echado para delante. Tenía problemas en el colegio, con mis padres, ellos siempre me tenían abandonado.

Mientras los niños jugaban en los parques, yo me formaba como nacionalsocialista. Así pasaron días, meses, años. Cuando ya fui un poco más mayor, debido a los problemas en casa, decidí meterme a deporte de contacto. Necesitaba ahogar toda esa rabia que tenía. Aprendí muchas técnicas que mi profesor me enseñaba. Estuve compitiendo en boxeo hasta que un día se me cruzó el cable y me expulsaron de allí. De todas formas no tardarían mucho en saber que yo usaba todo lo que aprendía en las calles.

Comencé en mi grupo ultra. Estuve dos veces en el correccional. Mis propios padres me denunciaron. Mi ideología se podía ver en mí, en mi entorno: botas, tirantes, cabeza rapada, banderas, armas, libros… Las detenciones eran constantes. Las peleas igual. Me consideraban una amenaza en el barrio… Una de las veces que salí del hospital, siendo mayor de edad, después de que mis propios padres me dijeran que debería haberme muerto ahí mismo, cogí las cosas, las pocas que me quedaban, porque se encargaron de tirarme todo, y me fui a casa de un camarada. En uno de los barrios de Hortaleza. Después de lo del latin king, entré en la cárcel. Gracias a mi abogado, al que le debo la vida de tantas veces que me ha salvado, no se pudo penar como homicidio. Me condenaron por mi ideología, cosa que vi peor… He llegado al punto de tener que irme de Madrid, y no sé ni siquiera si algún día podré volver. No sé si volveré a entrar en prisión, y no sé si cualquier día me matarán…

Markos ya me había reconocido que «Santos Navarro» no eran sus

apellidos. Que había renegado de los propios por el odio que sentía hacia su familia:

> … mi padre es camionero, reparte con el camión, aún no sé cómo no se ha matado por ahí, y mi madre es una pastillera depresiva que trabaja y después de trabajar se va a saber dios qué, mis primos y mis tíos son rojos, uno de mis primos es bukanero, más mayor que yo, los otros solo están en grupitos antifas, la gente me pregunta que por qué no celebro los cumpleaños o las Navidades o cualquier otra fiesta y es que en esa casa nunca se ha celebrado nada, desde que tengo uso de razón, te juro que no ha habido día que viniera mi padre de repartir y no viniera borracho, pero con una borrachera increíble y si estaba en casa, bebía en el sofá viendo la tele pegando gritos como un descosido, mi madre todos los santos días llorando y con pastillas y en la habitación, nadie hacía la comida en casa, nadie limpiaba en casa, pero es que lo peor es que mi padre quería pegar a mi madre y es algo que yo nunca consentí. Estando yo, jamás le puso la mano encima, porque las hostias y las palizas me las llevaba yo, día tras día, cuando ya iba pasando el tiempo, día tras día ya cogía él solo y me venía a buscar a mi habitación para darme otra vez y claro, yo iba al día siguiente al colegio y mi madre decía: este niño que siempre se está pegando o se ha caído o no tiene cuidado jugando. Mi madre jamás ha sacado la cara por mí, JAMÁS, ella estaba en la habitación mientras mi padre me acorralaba y jamás salió a defenderme, porque está loca esa mujer…

Quizá por eso en las Navidades de 2014 no podía sacármelo de la cabeza. Me preguntaba dónde pasaría la Nochebuena, o la Nochevieja. Y le escribí para interesarme. Me respondió el día 25 de diciembre:

> Estuve en casa de un camarada. Él trabajaba y no tenía mujer. Ahora estoy en el piso de un chaval que se iba a pasar el mes con su familia a Valencia, así que estoy solo hasta enero, pero vamos, que la casa la piso por las mañanas y para ducharme porque si estoy entre cuatro paredes, me agobio mucho y necesito salir a la calle y encima ni duermo, pues la combinación perfecta, vamos. En enero no sé dónde iré, si iré a casa de alguien, si me buscaré la vida… no quiero ir a casa de ningún camarada porque no quiero molestar, me parece que soy una carga y con los de aquí tampoco tengo tanta relación como con los de Madrid. Y no trabajo, estuve en un equipo, me pagaban algo, me jodí la pierna, estuve en un bar, acabé enganchado con el jefe… Así que nada, en enero empezaré a buscar como loco de lo que sea, y comer, pues cuando cae la suerte. Es un día a día muy «sencillo» y más este mes, me tiro en la calle 23 horas diarias y solo, porque no quiero ver a nadie. Además, es tiempo de estar con la familia y demás y como yo a esa panda de hijos de puta no los quiero ni ver, pues para qué les voy a amargar las fiestas a los demás, es tontería.

Supongo que fue un impulso estúpido. Irracional. Pero lo consulté con su amiga Marga, con la que seguía manteniendo un contacto regular, y me ofrecí a conseguirle algo de dinero. Al menos para que pasase las fiestas con dignidad. Imagino que sonará extraño que alguien ofrezca ayuda al tipo que afirma que intentó asesinarlo, pero en los nueve meses que llevábamos escribiéndonos no había renunciado en ningún momento a que Markos dejase el NS, como cientos de lectores de *Diario de un skin* lo habían hecho ya. Y para que eso fuese posible, Markos debía tener al menos la capacidad de elegir. Encerrado en sí mismo, sin trabajo y odiando a todo el planeta, no había muchas posibilidades de sacarlo de ese pozo. No aceptó mi ayuda.

Volvería a intentarlo una semana después, en Año Nuevo, con idéntico resultado. Markos se mostraba demasiado digno como para aceptar la

caridad del periodista que tanto había odiado. Así que le propuse otra cosa: compraría un décimo de lotería para el Sorteo de El Niño, y si tocaba, nos repartiríamos el premio a partes iguales. «Tendría coña —le dije— que nos tocase la lotería a mí y al tipo que intentó matarme, ¿no crees?» Supongo que le hizo gracia la ocurrencia. Desgraciadamente nuestro boleto no salió premiado. Era el destino. Pronto averiguaría que Markos era desafortunado en el juego porque era afortunado en amores.

Capítulo 11
La Comunidad hacker

«Mi esperanza es que la democratización del intercambio de conocimiento, a través de la eficiencia en costos de internet más la criptografía, continuará y terminará con un registro histórico global que sea riguroso e indeleble. Y esto permitirá formas inmediatas de justicia que antes no estaban a disposición de la gente.»

Julian Assange

Hack&Beers

La CyberCamp era un buen lugar para hacer contactos y conocer a algunos de aquellos talentos, que con tanto ahínco buscaba el Ejército, la Policía o las empresas del sector. Ellos son el futuro, y todos los sabíamos. Pero existe un lugar mejor para estrechar lazos con la comunidad hacker. Un lugar más discreto al que solo accedes por la invitación expresa de uno de sus distinguidos miembros. El secreto club de las quedadas Hack&Beers.

Me sentí un privilegiado. La invitación de David Pérez, todavía miembro de la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, para acompañarlo a la Hack&Beers podría parecer irrelevante: un grupo de amigos compartiendo tapas, picoteo y cervezas, para charlar de pasiones comunes. Nada extraordinario. Pero dadas las circunstancias, a mí sí me lo parecía, porque aquella era una reunión de la comunidad hacker, y era una oportunidad extraordinaria para conocer e intimar con algunos de los personajes más influyentes, veteranos y/o prometedores del mundo de la seguridad informática nacional. Cerebros privilegiados dotados de un don, que a ojos de un profano como yo parecía casi sobrenatural. Mentes que habían evolucionado más deprisa que las del común de los usuarios, para adaptarse darwinianamente al entorno tecnológico. Eran los hombres que susurran a los binarios. Y los binarios les responden.

Los hackers son tipos fascinantes. Y por eso han seducido a la gran pantalla: desde el mítico David Lightman en *Juegos de guerra* (1983), hasta el psicótico Elliot Alderson de *Mr. Robot* (2015).

En la innovadora *Tron* (1982), Kevin Flynn (Jeff Bridges) es un programador que termina entrando físicamente en el sistema operativo de la máquina. Gus Gorman (Richard Pryor) pone en aprietos al mismísimo Superman en la tercera parte de la saga (1983). Antes de protagonizar *El Santo,* Val Kilmer dio vida a Chris Knight en *Escuela de genios* (1985). Kate Libby (Angelina Jolie) lidera a un grupo de hacktivistas en *Hackers* (1995). En *Blackhat* (2015), la CIA recluta a un macizorro Nicholas Hathaway (Chris Hemsworth) para luchar contra una ciberamenaza mundial. Pero al frente de todos los hackers del cine siempre estará Thomas Anderson, alias «Neo» (Keanu Reeves), en la saga *Matrix* (1999), aunque yo reconozco que me siento más fascinado por Lisbeth Salander, de la saga literaria adaptada al cine *Millennium.*

Los guionistas lo saben. La figura del hacker da mucho juego. En las nuevas películas y series de acción del siglo XXI es inviable un héroe que no tenga un hacker de cabecera, porque quienes escriben los guiones saben que no resulta creíble una trama ambientada en la actualidad, y que no los tenga en cuenta. ¿Qué sería del intrépido agente Jack Bauer *(24)* sin Chloe O’Brian, el único personaje que se ha mantenido en toda la saga y en la versión cinematográfica? ¿Qué sería de la brillante

Olivia Pope *(Scandal)* sin su fiel Hunk? ¿Cómo haría posibles sus misiones Ethan Hunt *(Misión Imposible)* sin la ayuda de Benji Dunn?

Cuando aparqué la moto en el lugar donde me había citado David, no tenía ni la menor idea de con quién me iba a encontrar, pero me sentía como si fuese a conocer a cualquiera de esos personajes de película. Los asistentes al conclave pertenecían a corrientes y tendencias diversas: hacktivistas, consultores de seguridad, forenses, *pentesters*, policías… Algunos, amigos de amigos, ni siquiera se conocían entre ellos, lo que me permitía una cierta comodidad. Pero todos estaban dotados de ese don maravilloso para el pensamiento lateral, el análisis lógico y la compresión del cerebro de los ordenadores. Todos menos yo.

Además de David, el único al que conocía era César Lorenzana, el otrora capitán del Grupo de Delitos Telemáticos de la UCO. Hacía tiempo que no lo veía, y me pareció que estaba mucho más delgado y demacrado que en nuestro último encuentro: se había pasado los últimos meses estudiando para el ascenso. Ahora era el comandante Lorenzana.

A medida que avanzaba la noche, y las cervezas desinhibían las lenguas, salían a la luz los nombres y trayectorias de aquellos genios que me rodeaban. Así, poco a poco, entre raciones de bravas y calamares, entre tapas de croquetas y mejillones, fui descubriendo quiénes eran mis compañeros de cena y tertulia.

Allí estaban Kio y Kaótica, hacktivistas comprometidos con las causas sociales a través de la tecnología. Kaótica fue una de las voluntarias que se dejó la piel, y la ilusión, en la plaza de la Puerta del Sol el 15-M, para que las ideas que surgían en aquel foro ciudadano se extendiesen por la red. Y Kio era uno de esos genios de los ordenadores capaces de hacer magia con la red wifi y de hacer obedecer al software con la pericia de un domador de leones.

También tuve el honor de conocer al siempre sonriente Mario A. Vilas, creador de WinAppDbg y responsable del imprescindible blog técnico breakingcode.wordpress.com, cuya erudición tecnológica me hacía sentirme como un pelotudo: recién llegado de la última CON internacional en Alemania, Mario compartía con sus colegas su entusiasmo por los últimos descubrimientos de la comunidad. Y conocí a Pablo San Emeterio, uno de los descubridores de las vulnerabilidades en WhatsApp, junto con Jaime Sánchez, y al que ya había visto en varias CON.

Pude brindar con el histórico Antonio Hernández (Belky), otro veterano de la vieja escuela, con su largo cabello blanco, que le daba un aire al sabio Gandalf, y que es el responsables de sistemas y comunicaciones en una conocida empresa del grupo Servinform. Y junto a «Gandalf», «S4ur0n», nick de Pedro Candel, el entrañable director de Navaja Negra,[100] uno de los encuentros de hacking más prestigiosos de España con ya cinco años de vida. Casi tan enamorado del mar y la montaña como de los ordenadores, es un rebelde con causa. No le gustan las corbatas ni los que las usan, y era de los más enfadados con la reforma de la ley del 1 de julio. No dejaba

escapar la oportunidad de expresarlo.

Pasé mucha hambre esa velada. Ante mí desfilaban las bandejas con oreja de cerdo, jamón y el plato fuerte del local, los torreznitos, uno de los argumentos de la masiva afluencia de hackers a la reunión. Pero no me importó en absoluto. Me alimentaba pegando la oreja a uno y otro corrillo, para escuchar retazos de entusiasta conversación sobre tal o cual vulnerabilidad recién descubierta, sobre la ponencia que presentarían en la próxima CON, o sobre la última entrada en los blogs de referencia.

Aquella noche pude percibir la indignación de Jesús Marín, que vivió en sus carnes el drama de ser el último eslabón de la cadena de subcontratados, por subcontratas, subcontratadas a su vez por el cliente de una empresa que cobrará cifras de seis dígitos, cuando el técnico, como Jesús, que al final hace todo el trabajo, cobrará cifras de cuatro. Ytuve el privilegio de brindar con el ingeniero gallego Jesús Cea Avión, que dirige su propio blog técnico y «ecléctico»,[101] y el investigador en seguridad Javier Espejo (Quemm). Ambos son parte del equipo de Podcast 1984, junto con Pedro Candel y Antonio Hernández.[102] Que precisamente dedicaría su primer programa, un tiempo después, a la reforma de la ley y su repercusión en el mundo de los hackers.

Para mí fue una noche mágica. Porque allí, integrado como uno más en su grupo, pude conocer esos aspectos del mundo del hacking que no se comentan en las CON, ni en los libros. Tendréis que perdonarme si no conseguí retener todos los nombres y he olvidado a alguien.

Confieso que, desde el principio, sentí una empatía especial con un joven de pelo corto, mirada inteligente y sonrisa sincera. No hablaba mucho, aunque cuando lo hacía sentaba cátedra. Lo llamaré Lucas.

Le pregunté a David quién era, y cuando me lo dijo no podía dar crédito. Aquel joven informático de currículo brillante y precoz era uno de los pocos españoles fichados por una de las compañías de internet más importantes del mundo… quizás la más importante. Estaba allí de casualidad, porque en cuestión de semanas abandonaría España para establecerse en la sede de su nueva empresa: iba a trabajar en el Departamento de Seguridad Informática de ese colosal gigante de la red.

Lucas terminaría convirtiéndose en otra pieza clave en mi viaje. Aquel Hack&Beers supondría nuestro primer encuentro. Después nos veríamos en otras ocasiones, ya solos, y de su mano conocería un punto de vista más autorizado sobre cómo funcionan los grandes gestores de internet. Pero no solo eso. Lucas sería mi garante para conocer a uno de los personajes más fascinantes de este viaje. A cambio, y debido a las estrictas cláusulas de confidencialidad con el colosal monopolio informático que se ha llevado de España su talento, solo me puso como condición que en ningún momento pudiese adivinarse su identidad en este libro.

Consultor de seguridad *free lance,* durante años se especializó en la seguridad de dispositivos móviles, y alguno de sus programas ha tenido millones de descargas en las páginas especializadas. Realmente lamento no poder dar más referencias, pero su

empresa es bastante reacia a que sus empleados hablen con la prensa, y bajo ningún concepto quisiera crearle problemas. Solo insistiré en que si uno de los gigantes de internet lo ha fichado para llevárselo de España, es porque es uno de los cerebros mejor amueblados del panorama hacking español. Estoy seguro de que la comunidad sabrá a quién me refiero…

Poco a poco, local a local, los hombres que susurran a las máquinas fueron retirándose a sus respectivos hogares, que imaginé laboratorios secretos, repletos de ordenadores cifrados, patrullando permanentemente la red en busca de vulnerabilidades… A las cinco y media de la madrugada, cuando ya nos habíamos recorrido todos los garitos de la zona, y tras la baja de David, solo quedábamos el patriarca de Navaja Negra, Pedro Candel, Kaótica y yo. Tirados en la acera, a las puertas del último local de Madrid que también había cerrado ya, y tratando de solucionar los problemas del mundo desde el punto de vista de un hacker. La llamada que recibió a horas tan intempestivas el legendario Román Medina-Heigl (RoMaNSoFt), cofundador de RootedCON y uno de los mejores hackers españoles, fue culpa mía, que me puse muy pesado con Pedro… Mis disculpas desde aquí.

La fecha clave del 1 de julio de 2015 se aproximaba inexorablemente, y con ella la entrada en vigor de la reforma del Código Penal: «Y un nuevo recorte —exclamaba indignado Pedro— de la poca libertad que nos queda a los hackers».

La regulación del hacking y de las consultorías de seguridad informática, como había ocurrido anteriormente, pendía como una espada de Damocles sobre las cabezas de la comunidad. Si los planes del Gobierno seguían su curso, la libertad de la que habían gozado los hackers para explorar sistemas, buscar y denunciar sus fallos, emplear herramientas de análisis y auditorías de seguridad, etcétera, podrían verse segada. Y la tenencia de esas herramientas, en realidad armas en las manos apropiadas, tipificada como delito. Y para veteranos de la vieja escuela como Pedro Candel, «que ya hackeaba sistemas antes de que me salieran pelos en los huevos», resultaba indignante, frustrante e inaceptable que el Gobierno pretendiese regular qué podía o no podía hacer con su ordenador. Me pareció lógico.

Imagino que la escena no tenía nada de original. Tres amigos, con esa exaltación de la amistad que favorece el pasar la noche en vela, alguno con unas cervezas de más, tirados en un rincón de la ciudad, a punto de amanecer, cagándose en la puta madre de los poderosos y tratando de arreglar el mundo… La diferencia es que si alguien tiene el poder para cambiar las cosas en el mundo actual son ellos. Los hackers.

«En local funciona»

Lucas es un escéptico. Cuando un tiempo después de nuestro primer contacto en la Hack&Beers accedió a mantener una serie de reuniones conmigo, antes de marcharse de España, me sentí un privilegiado. Como si pudiese quedar a comer o cenar con el mismo Steve Jobs para debatir los secretos de Apple. Con Lucas descubrí un punto de vista sobre la seguridad informática de los usuarios más optimista y menos alarmista que al que estaba acostumbrado.

—No te creas todo lo que escuches —me dijo de entrada—. En nuestra comunidad somos un poco vanidosos, y el reconocimiento de nuestros colegas ha sido, desde el principio de la historia hacker, una de nuestras prioridades. Entre otras razones porque los hackers no están para perder el tiempo enseñando a los novatos a configurar su ordenador o a cifrar su correo. Se supone que para frecuentar ciertos foros especializados tienes que tener un cierto nivel, y eso lo demuestran tus publicaciones y tu currículo. Por eso en muchas ocasiones verás que se presentan vulnerabilidades en nuestras conferencias, como la Rooted, No cON Name, Navaja Negra, etcétera, que pueden parecer alarmistas, como si cualquiera pudiese romper la seguridad de Google, Twitter, Facebook, Apple o Microsoft con la gorra… y no es verdad.

—Vaya, eso me alivia. Desde que os conozco, mi paranoia se ha disparado, y ya estaba planteándome tirar el móvil a la basura, y el ordenador detrás de él… Pero ¿eso significa que tus colegas mienten al presentar las vulnerabilidades que descubren?

—No, no, nada de eso. Tienes que entender que para descubrir una vulnerabilidad nueva, debes invertir meses de trabajo analizando un sistema. Son horas y horas y horas probando nuevos algoritmos, buscando debilidades, combinando muchas técnicas. Y lo haces desde tu laboratorio. O sea, desde tus ordenadores. Cuando un hacker descubre un fallo, lo hace en su equipo. En un entorno controlado. Con su red, su navegador, su software. Pero otra cosa es replicar eso en un entorno real. Mira, nosotros somos científicos, y en la informática ocurre lo mismo que en la física o la química. Una cosa es lo que ocurre en el laboratorio y otra en el mundo real. Hay una frase que debes tener presente, y que nosotros decimos mucho con cierta ironía… «En local funciona.» Otra cosa es que tu descubrimiento sea eficiente cuando sales a la red.

Estaba confuso, pero sentía un cierto alivio. Empezaba a contemplar la posibilidad de no volver a coger un móvil, y comenzar a utilizar el código morse.

—No estoy seguro de entenderlo. Supongo que si Gmail tiene un fallo y se puede romper su seguridad, ese fallo será explotable desde mi portátil o desde un cibercafé.

—Pues no es así exactamente. Un simple carácter distinto en un código puede hacer que una vulnerabilidad no funcione. Y una cosa es tu ordenador y otra muy distinta salir a la red real. Los navegadores, las conexiones que utilices, los continuos

parches de las compañías… Si te fijas, cuando hacemos una demo de nuestros descubrimientos en las conferencias, muchas veces la llevamos grabada. No es una demostración en tiempo real, porque sabemos que un protocolo en la conexión de la sala, o en el ordenador que nos deje la organización, o en el USB donde llevamos las transparencias, cualquier cosa puede afectar al programa y hacer que no funcione cuando estamos delante de un público de mil o dos mil personas. Sería muy embarazoso.

—O sea, que la leyenda de que un chaval de quince años puede hackear la NSA, bajándose un tutorial de YouTube y usando herramientas de hacking, no es cierta…

Lucas rompió en una carcajada sincera. Sabía que la opinión pública había aprendido a temer a los hackers tanto como a los terroristas, a causa de los titulares que exprimen de forma sensacional cada noticia sobre un nuevo ciberataque.

—No, no es tan sencillo. Las grandes empresas, como la mía, premian a los investigadores que descubren nuevas vulnerabilidades reales. Además del prestigio que te supone, descubrir una nueva vulnerabilidad implica una compensación económica porque, como te puedes imaginar, a las empresas les interesa más que a nadie ofrecer un producto seguro para sus usuarios. De lo contrario, se irán con otra empresa. Y cada nuevo descubrimiento implica que tú recibas en tu ordenador un mensaje pidiéndote que actualices tu equipo, precisamente para parchear esos fallos recién descubiertos, o simplemente para mejorar la velocidad o la capacidad de tu sistema. Por eso es tan importante ejecutar las actualizaciones cuando te llegan. Es tu primera línea de defensa. Y cada noticia sobre un nuevo ataque hace que la compañía nos ponga las pilas para reparar ese fallo. Por eso cada día los servicios son más seguros.

»Por ejemplo, después del Celebgate, Apple corrigió la vulnerabilidad de iCloud a los ataques de fuerza bruta… O WhatsApp: al principio no cifraba los mensajes. Podías saltar el proceso de verificación del número, que usaba filtros básicos, y hackear una cuenta, pero ya no. Ahora los ciberdelincuentes tendrán que buscar otro sistema para entrar, pero ya no podrán hacerlo como lo hicieron entonces.

Lucas me enunció entonces varias mejoras recientes en la seguridad de los grandes proveedores de internet, que yo mismo había detectado como usuario. Por ejemplo, al utilizar diferentes cibercafés de las ciudades por las que viajo, ese año comencé a recibir notificaciones de Facebook, Gmail, etcétera, cada vez que abría mi correo desde un dispositivo diferente. Esta es una medida adoptada por varios proveedores de servicios *online* para advertir al usuario si alguien ha accedido a su cuenta desde un dispositivo distinto al que utiliza normalmente. Y eso es bueno.

Esas medidas de seguridad se irían implementando en los meses sucesivos ofreciéndonos a los usuarios nuevos servicios para saber si alguien se había colado en nuestro perfil social, para ocultar contenidos ya publicados, para designar un heredero de nuestro perfil social, e incluso para comunicarnos con otros perfiles con los que no tenemos «amistad».[103] Por un módico precio, eso sí, pero para mí esa nueva función

en el caso de Facebook sería importante unos meses más tarde, al descubrir la verdadera identidad de MarkoSS88.

Sin embargo, al mismo tiempo, la industria del *malware* evoluciona a una velocidad de vértigo, creando falsos servicios y apps que atacan nuestra intimidad, infiltradas entre las herramientas legítimas. Por eso los especialistas insisten en que no nos descarguemos aplicaciones ni contenidos «piratas», ya que detrás de ellos no hay ninguna empresa conocida que asuma responsabilidades legales. Y a la larga ahorrarnos unos euros nos puede salir caro. El mejor ejemplo es la aplicación The Adult Player, una app —afirma el diario *ABC*— que promete contenido pornográfico gratuito a quien la descargue, y que en realidad, según se publicó en 2015, toma el control del teléfono móvil, te hace fotos con tu propia cámara contando con pillarte en alguna situación «comprometida» y subida de tono mientras ves las imágenes, y acto seguido te bloquea el teléfono y amenaza con subir las fotos a tus perfiles sociales si no pagas entre 440 y 500 euros.[104]

—En resumen —me dijo Lucas—, quienes trabajamos en seguridad para las grandes compañías no somos gilipollas. Y cada vez se lo ponemos más difícil a los cibercriminales. Cada día que pasa los sistemas son más seguros. Por supuesto que continuarán existiendo vulnerabilidades, aunque cada vez será más difícil romper un sistema en remoto, o sea, a distancia. Pero para eso está la ingeniería social, y el simple sentido común. El hacking tiene mucho de imaginación y pensamiento lateral. No todo es técnica.

—Creo que no te sigo. Ponme un ejemplo.

Y Lucas se lanzó a una demostración de pensamiento hacker que me dejó con la boca abierta…

«No todo el hacking es software»: el pensamiento lateral

—Has leído sobre Snowden, ¿verdad?

—Sí, claro, por supuesto —respondí un poco ofendido. No soy ningún hacker, pero me había tomado muy en serio la investigación y había estudiado mucho—. Conozco su historia perfectamente.

—Snowden nos desveló que la NSA utilizaba el programa XKeyscore. Antes de Snowden, ese nombre ya aparecía citado en algún artículo, currículo, etcétera, solo que no sabíamos lo que era. Ahora que lo sabemos, imagina que haces una búsqueda de XKeyscore[105] y la comparas con Linkedin. *Voilà!*, ya tienes identificados un montón de posibles técnicos de la NSA. Y todo sin escribir una línea de código.

—No puede ser tan sencillo… —repliqué perplejo.

Aun así, sabía que Lucas tenía razón. Aquel era un ejemplo perfecto del concepto «vulnerabilidad humana». Ninguno de aquellos técnicos al servicio de la NSA podía haber imaginado que Edward Snowden, uno de los suyos, fuese a revelar al mundo qué era XKeyscore, y por eso muchos lo incluían en sus currículos. Y no importa que después lo borrasen de sus perfiles. En la red todo permanece si sabes dónde buscar.

—A ver… Te pondré otro ejemplo —me dijo Lucas mientras se sacaba el móvil del bolsillo y buscaba una aplicación: Tinder.

Tinder es una app geosocial que permite a los usuarios comunicarse con otras personas desconocidas, en base a sus preferencias, y concretar encuentros. Su uso más habitual es el ligue; de ahí su éxito. En 2014 fue nominada app del año en los premios Enter.Co con más de 50 millones de usuarios. La app busca en la zona geográfica indicada otros usuarios de Tinder, generalmente identificados con una foto personal.

—Tinder te permite restringir el radio de acción —me explicó Lucas mientras señalaba las características de la aplicación en la pantalla de su teléfono—, y también falsear tu ubicación. Imagina que ponemos que estamos… no sé… en Quantico. Ahora vamos a *matchear*… ¿Quién piensas tú que puede aparecer en la pantalla?

—Agentes del FBI —respondí asombrado, mientras miraba de reojo los rostros que comenzaba a asomar al teléfono del ingenioso hacker. Ahora entendía por qué su cerebro había llamado la atención de aquel gigante de internet.

—Así es. Ya tienes un montón de datos sensibles. La identidad y la cara de los trabajadores del FBI que están en Quantico ahora mismo. Y sin tener que hackear ninguna cuenta de correo ni hacer nada ilegal.

Me vinieron a la memoria varios de los casos prácticos que había comentado con Selva Orejón en OnBranding. «Personas que deberían estar protegiendo su identidad y que en cambio la usan primero como la erótica del poder», me había dicho, o los ejemplos de sextorsión tras buscar datos personales de la víctima en apps paralelas.

—Cuando decimos que el mejor antivirus eres tú, nos referimos a cosas como

esta —seguía Lucas—. Las mejores vulnerabilidades son las humanas, porque son las más fáciles de explotar. Y no dejes que te engañen. No todo el trabajo de un hacker se basa en la programación informática. No todo el hacking es software. Nosotros podemos blindar tecnológicamente nuestros productos, o al menos intentarlo, pero eso no significa que los cibercriminales puedan encontrar la manera de utilizarlos para cometer delitos. Recuerda que la base del hacking es la imaginación. El pensamiento lateral. A veces solo es cuestión de usar las mismas herramientas que te da la tecnología, pero de una forma diferente, como te acabo de enseñar. Si no tienes un martillo a mano, a veces puedes clavar un clavo con una llave inglesa.

He de reconocer que todos mis encuentros con Lucas fueron una experiencia reveladora. Hasta el mismo momento en que abandonó España para incorporarse a su nuevo puesto. Y sus reflexiones, siempre fruto de su dilatada experiencia en el sector, resultaban renovadoras. Diferentes a la mayoría de las cosas que había escuchado hasta entonces.

—La ciberdelincuencia es un problema, es verdad. Existen muchas personas que se descargan cuatro herramientas y consiguen vivir del cibercrimen. Pero piensa un poco: tú has comprobado que nuestro sector no tiene paro. A poco que seas mínimamente competente, hay miles de empresas que se pegarían por contratarte. La seguridad informática está en alza, y cada vez irá a más. ¿Por qué un profesional medianamente cualificado va a complicarse la vida dedicándose al crimen, cuando puede disfrutar de un sueldo razonable en cualquier empresa legal? Seguro que existen excepciones, y que los crackers de los narcos o de las mafias cobran un sueldazo, pero en general, el 99% de los usuarios no son objetivos, y la mayoría de los atacantes no tienen recursos. Solo el 5% de los delitos informáticos se resuelven policialmente, pero averigua en cuántos de ellos el atacante era un vecino, un exnovio, un socio despechado, un trabajador resentido…

»Las herramientas de hacking realmente sofisticadas son muy caras. Inaccesibles para el usuario común. Es verdad que puedes comprarte una baliza en eBay por 20 dólares, pero una de las que utiliza la CIA cuesta 10.000. Lo mismo ocurre con las herramientas informáticas. Ningún vecino tuyo va a comprar un programa a los italianos del Hacking Team para encender en remoto la webcam de tu portátil y grabarte cuando sales de la ducha. Ese tipo de servicios solo está al alcance de gobiernos, servicios de Inteligencia o grandes empresas. Y esa es otra guerra.

—Me desconciertas, Lucas. Casi todos tus colegas me hablan de la terrible amenaza de la red, de lo vendidos que estamos, de cuánta protección necesitamos para un uso seguro de nuestro ordenador…

—Ya, pero es que nosotros vivimos de eso. Si no hay ciberamenaza, ¿de qué vamos a vivir los que vendemos la seguridad contra ella?

Supongo que mi cara de perplejidad era evidente. La autocrítica de Lucas hacia su sector me parecía de una honestidad aplastante. Y al mismo tiempo me aliviaba un tanto como usuario de internet. Una y otra vez volvía a mi memoria la máxima de

Angelucho, el guardia civil impulsor de X1Red+Segura: «El mejor antivirus eres tú».

—No pongas esa cara —se rio él—. Lo único que te digo es que no pierdas la perspectiva. Las cosas no son blancas o negras. Para nosotros, quienes utilizan las herramientas de hacking no merecen ser llamados hackers. Nosotros los llamamos *lamers*. ¿Te imaginas un piloto que despegase, hiciese el vuelo y aterrizase, todo ello con el piloto automático puesto?

Lucas tenía razón una vez más. Según me revelarían los funcionarios de las unidades de delitos telemáticos, de diferentes servicios policiales, un amplio porcentaje de los detenidos había utilizado herramientas de hacking, previamente configuradas por auténticos hackers, pero carecían de los conocimientos técnicos de estos.

Cuando estuve en el País Vasco, el ertzaina Manuel Viota me contó un caso que él mismo había vivido: «Dos chavalitos de once años, once, que se habían zumbado la página web del colegio porque a uno de ellos le habían suspendido siete asignaturas. Le montaron un ataque de denegación de servicio en toda regla, y cuando los identificamos, les preguntamos cómo lo habían hecho, y nos dijeron que habían encontrado en YouTube un manual y se habían limitado a seguir las instrucciones».

—Es probable que tengas razón, Lucas. Pero si a mí me roban las credenciales, y con ellas mi cuenta bancaria, o mis redes sociales, y las utilizan para blanquear capitales, en realidad me da igual que el autor del robo sea un ingeniero de sistemas del MIT o un crío que se ha bajado un tutorial en YouTube. El daño es el mismo.

—Sí, pero si quien te ha robado es el primero, estás totalmente exculpado, porque no tenías salvación. Pero si quien te ha robado es el *lamer,* la culpa es tuya por gilipollas. Porque con un poco de sentido común y una navegación mínimamente segura, no habría podido acceder a tus cuentas.

Así de demoledor y contundente es Lucas en sus razonamientos. Incrédulo, escéptico en cuanto a la mayoría de tópicos que los periodistas publicamos sobre el mundo del hacking y la seguridad informática. Y los aspectos judiciales y penales del hacking tampoco escapaban a su crítica.

—Todos usamos la red. Pero la visión que tenemos de la tecnología los profesionales y la que tenéis los usuarios todavía es muy diferente. A medida que pasen los años, y este terreno que os parece ignoto y misterioso sea más familiar, esa distancia se acortará. Pero ahora mismo es enorme. Por eso, cada vez que la comunidad lee las noticias que se publican sobre nosotros, nos morimos de risa. Periodistas, políticos, jueces…

—¿Jueces? ¿Te refieres a la nueva legislación?

—Por ejemplo. Todo eso que están planteando la Fiscalía y la judicatura, sobre utilizar códigos espía para interceptar terroristas o cibercriminales… No es real. Ni eso ni el alarmismo de los hacktivistas advirtiendo de que nuestras libertades terminarán cuando se autorice esa ley.

—Tío, me rompes los esquemas. ¿Cómo que no es real? Yo he estado con

fiscales, con policías, con guardias civiles que…

—Te digo que no es real —me interrumpió Lucas, molesto por que cuestionase su argumento—. Si utilizas un código espía para interceptar comunicaciones, o para entrar en el ordenador de un sospechoso, su abogado te va a obligar a adjuntarlo al sumario para cotejarlo con sus peritos. Por lo tanto, ese código sería público y ya no podría volver a utilizarse. ¿Y tú sabes cuánto cuesta diseñar uno nuevo? Yo no te quiero decir lo que tienes que creer. Solo te invito a que no te tragues todos los titulares sensacionalistas que puedas leer sobre este mundo. Es un mundo nuevo, y a los usuarios os llevará un tiempo aprender a diferenciar el trigo de la paja, pero créeme, la mayoría de las veces basta con no precipitarse y utilizar el sentido común.

No tengo palabras para expresar mi gratitud por las horas que un profesional tan reputado como Lucas perdió conmigo. Cada reunión con él suponía un punto de vista diferente, crítico y escéptico con muchas de las cosas que me llegaban desde otras fuentes. Fue mi abogado del diablo. El contrapeso imprescindible para evitar un desequilibrio en la balanza de la objetividad. Un antídoto contra la paranoia y el alarmismo. Y mi referente para acceder a otro personaje de la comunidad hacking, tan fascinante como él, pero infinitamente más esquivo e inaccesible.

Lucas y Lord Epsylon suponen los dos extremos del hacking. El primero ha fichado por una de las mayores multinacionales de internet. El otro ni siquiera tiene teléfono. El primero cobra un generoso sueldo por proteger los servicios de un gigante de la red. El otro participa en campañas de hacktivismo para atacar compañías como esa. Sin embargo, y esto es lo fascinante, ambos se respetan. Coincidieron en una prestigiosa conferencia sobre seguridad informática justo cuando yo comenzaba esta investigación, y puedo entender que entre ambos se estableciese una relación de admiración y respeto, pese a pertenecer a extremos opuestos de la ideología hacking. Porque, por encima de todo, ambos son científicos. Investigadores de las tecnologías. Hackers.

—Deberías conocer a Epsylon —me dijo Lucas durante uno de nuestros últimos encuentros—. Yo soy capitalista, he estudiado esta carrera para vivir de ella y cuanto mejor viva, mejor. Pero si quieres tener una visión completa de lo que es el mundo del hacking, deberías incluir el hacktivismo. Y yo no conozco a nadie más coherente en ese sentido que Epsylon. Hay mucha gente que se autodenomina hacktivista, pero Epsylon no lo dice, lo vive.

—¿Y cómo puedo localizarlo? —le pregunté.

—No puedes. Epsylon se ha metido en muchas movidas y a la paranoia implícita al hacking ha añadido la sobredosis que implica el hacktivismo. Ya sabes, Anónymous, Wikileaks, todo eso. No tiene móvil. Vive como un nómada. Creo que ahora está en una casa okupa en Francia o Alemania, vete a saber. Tú no lo localizas, él te localiza a ti. Déjame que hable con él y, si me autoriza, te paso su clave PGP. No intentes mandarle un correo normal, porque no te responderá. Solo contesta por sistemas cifrados, tipo PGP o Mumble. Pero aunque sea un poco engorroso, en mi

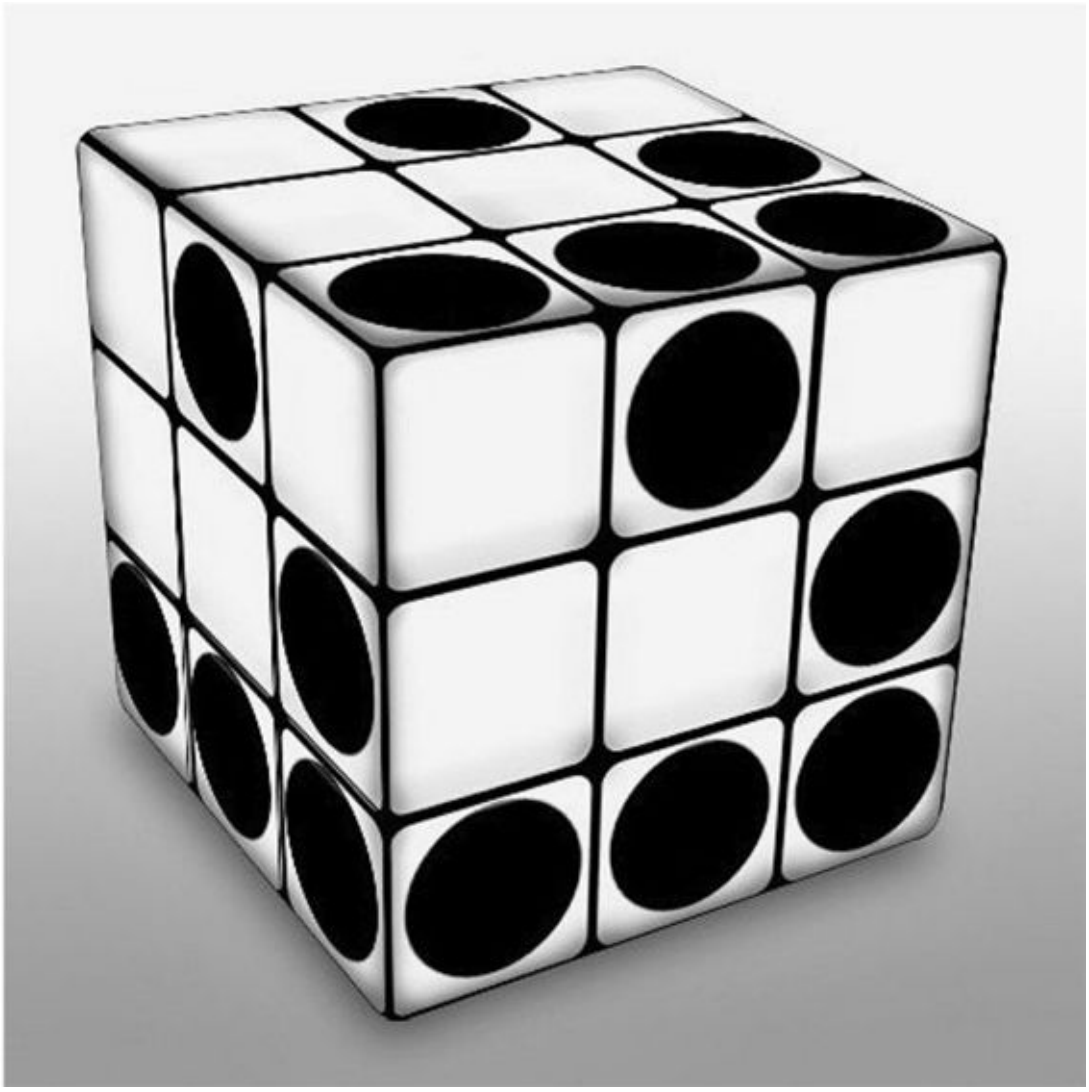
opinión deberías conocerlo. Te ofrecerá una visión diferente a todo lo que has visto u oído sobre el hacking.

Y por enésima vez Lucas tenía razón. Gracias a su intercesión, y a las referencias que le dio a Lord Epsylon sobre mí, comencé a intercambiar emails con él, siempre a través del sistema de cifrado PGP. El mismo que Edward Snowden exigió a Glenn Greenwald, para compartir con él su filtración de secretos de la NSA. Para mí, tan torpe con la informática como el mismo Greenwald, supuso un reto aprender a manejar el PGP. Desde luego, no me resultó tan sencillo como el comandante César Lorenzana me había explicado. Pero mereció la pena.

Desde que pude habilitar el programa de cifrado, gracias a la inestimable ayuda de David Pérez, en cada nuevo email Lord Epsylon despertaba más y más mi curiosidad. El problema es que yo no quería conformarme con una entrevista *online*. Yo quería tener un encuentro personal, y eso implicaba que alguien tan extremadamente paranoico como Lord Epsylon me concediese su confianza y me abriese las puertas de su último escondite. Desde el que era capaz de hackear cualquier cosas… hasta un satélite. Hoy me consta. Pero llegar allí iba a llevar unos meses.

Durante ese tiempo me facilitó, a través del correo cifrado, vídeos de sus conferencias, memorandos de Anónymous y otros grupos hacktivistas, textos, libros y páginas que debía leer si quería comprender el activismo en la red. E incluso, cuando más tarde se lo pedí, me orientó hacia el hacklab de París…

PARTE III



ENERO DE 2015
SORAYA, LA NUEVA NOVIA DE MARKOSS88

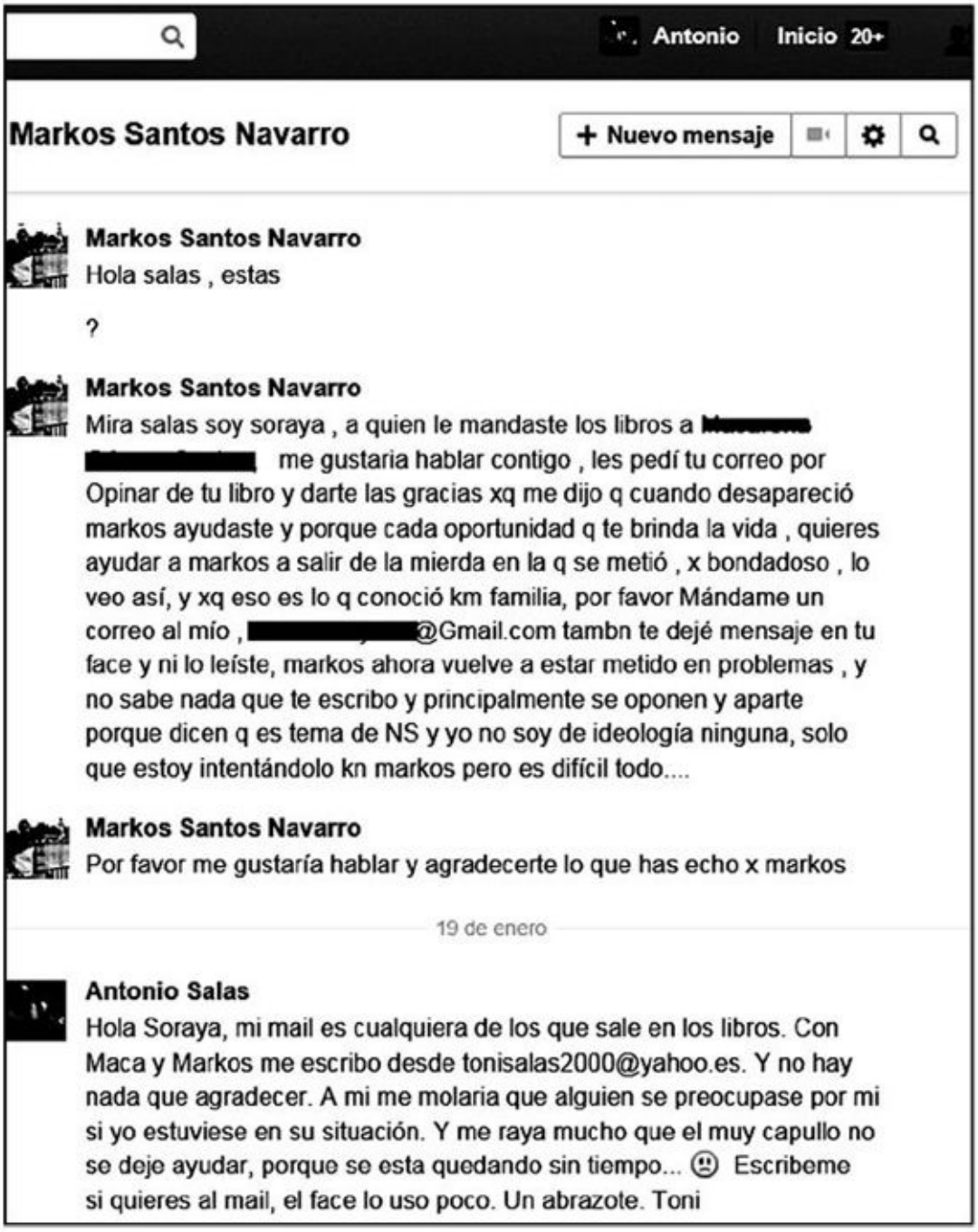
«Lucho por lo que amo, amo lo que respeto, y a lo sumo respeto lo que conozco.»

Adolf Hitler, *Mein Kampf*, Parte primera, cap. 3

Recién estrenado 2015 recibí varios mensajes en mi cuenta de Facebook enviados desde la de Markos. Me extrañó, porque Markos y yo siempre nos comunicábamos a través del email de su web. La explicación al misterio era sencilla. No era Markos quien me enviaba aquel mensaje.

Markos había roto con Silvia Hierro poco tiempo antes, y de forma abrupta. Me sorprendió, pero no me pareció oportuno indagar en un tema tan personal. En las fotos de sus perfiles sociales parecían un anuncio de la última comedia romántica de Hollywood. Atractivos, risueños, visiblemente enamorados. Esas cosas no se pueden fingir. Su forma de mirarse, de besarse, de cogerse de la mano… La pareja de las fotos estaba profundamente enamorada, y desde luego nadie podría imaginar que el joven fuese un asesino… Pero entonces ¿por qué se separaron?

Supuse que la ruptura con Silvia había sido el detonante para que Markos abandonase Madrid y se estableciese en Mallorca. Curiosamente los Facebook, Ask y Twitter de Silvia Hierro comenzaron a perder actividad desde la separación. Como si el desamor hubiese marchitado a la hermosa estudiante madrileña de Medicina, que cada vez actualizaba menos sus perfiles hasta abandonarlos por completo. Alguna referencia a su ex y después el silencio. Los revisé por última vez en el verano de 2015, justo antes de que desapareciesen, y el último mensaje dejado en su muro llevaba fecha del 14 de abril de ese año y era precisamente de Marga: «Silvia, ¿estás bien? Hace mucho que no se te ve por aquí. Besos, guapa».Silvia nunca respondió a la que también era su amiga. Al menos a través de la red.

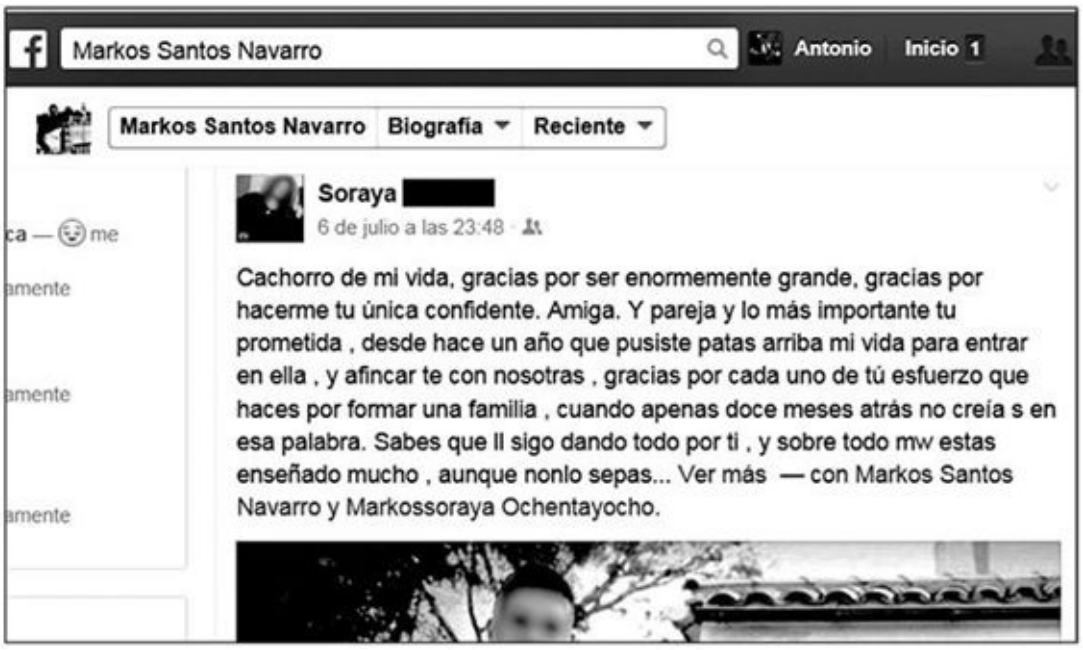


Soraya, sin embargo, vivía en un pueblecito de Alicante. Unas semanas atrás Markos me había pedido que le hiciese llegar un paquete con otros libros, y ella no había puesto ningún problema en facilitarme la dirección de su casa. Quizá porque no tenía nada que esconder.

Pese a que apenas tenía veintidós años, Soraya ya había sido madre de una niña preciosa. Y por lo que me contaba Markos, estaba encantado con la experiencia:

> Soraya bien, ¿te comenté que tenía una niña? Seis años tiene, y me llama «papá»… Yo, buff… No sé, son cosas que nunca me habían pasado antes y también me viene muy grande, estoy acostumbrado a formar cachorros, pero ¿hijos? Si no puedo cuidar ni de mí mismo… Me gustaría estar allí con ellas todo el tiempo y por eso estoy deseando que salga el juicio.

Aquello me parecía tremendamente precipitado. Di por hecho que Markos habría comenzado su relación con Soraya antes de dejar a Silvia, ¿qué otra explicación había? ¿Cuánto tiempo necesita un niño para llamar «papá» a alguien? No cuadraba nada. Si tanto las quería y en Mallorca no tenía a nadie, no entendía por qué había acabado allí en vez de irse a Alicante. Como pasaba cada vez con más frecuencia, había demasiadas preguntas sin respuesta, demasiadas «cosas raras». Supuse que exageraba, que intentaba impresionarme para que viese que estaba «sentando la cabeza», ¿era eso? Aun así me alegré al leerlo. De corazón. Me imaginaba al chaval de diecinueve o veinte años, perdido, lejos de sus amigos, y me decía que a lo mejor Soraya conseguía ser el tablón al que Markos podría agarrarse para no hundirse tras el naufragio de su vida. He conocido personalmente muchos casos, y es un hecho constatado por los especialistas que muchos skinhead abandonan el movimiento neonazi cuando estabilizan su vida con una relación sentimental o con un empleo. Pero con Markos me equivoqué. La corriente del odio en la que vivía sumergido lo arrastraba inexorablemente hacia el fondo.



Aparentemente las cosas iban mejor. El muro de Facebook de Markos recibía todos los días apasionadas declaraciones de amor de Soraya, y alguna de ellas dejaba claro que la relación —al menos cibernética— había comenzado hacía ya tiempo. Realmente se había enamorado hasta las trancas de aquel joven apuesto, atormentado por una vida difícil. El tipo duro y malote que todo guionista imaginaría para su película sobre bandas callejeras.

Por otro lado, Markos empezó a hacer deporte. En sus correos me explicaba que frecuentaba el gimnasio y que había empezado a jugar en un

equipo de fútbol local. Nada pretencioso, pero le ayudaba a quemar energía.

Continuamos realizando la entrevista vía email, debatiendo sobre cuestiones ideológicas y sobre el contenido de su libro. Sin embargo, Markos no daba un paso atrás en sus argumentos racistas y xenófobos, que trataba de justificar con citas eruditas y referencias bibliográficas. Markos no hablaba como un skinhead de diecinueve años como los que yo había conocido durante mi infiltración.

Markos hablaba de «herencias comunes que hermanan Europa», citaba referencias como «la Europa nórdica de la que habla Rosenberg, la Europa blanca de Romualdi», elevaba su registro mucho más que en nuestros cruces de emails, y argumentaba respuesta tras respuesta con la soltura de un experto.

Y a pesar de su supuesto arrepentimiento por haber intentado ejecutarme, el hecho de que en nuestro largo debate no mostrase ni el menor asomo de renegar de su ideología, ni de la violencia, no hacía más que reafirmarme en la necesidad de averiguar quién era realmente MarkoSS88. Y ninguno nos habríamos imaginado quién se escondía tras ese nick en internet, y tras las fotos de ese joven atractivo y violento…

Sin embargo, un suceso inesperado me obligaría a posponer la investigación sobre Markos. En enero de 2015 un atentado terrorista en París estremecería a la opinión pública internacional. El Estado Islámico había golpeado Europa, y la red se convertiría en un nuevo campo de batalla. Así que tendría que seguir mi viaje hacia el mundo de los hackers en París…

Capítulo 12
Operación Charlie Hebdo

«La tinta del sabio es más sagrada que la sangre del mártir.»

Profeta Muhammad (saas), hadiz compilado por Muslim

El ISIS ataca en el París del Chacal

El móvil empezó a repiquetear insistentemente mientras recibía varios mensajes y llamadas, todo a una. La noticia acababa de llegar a España y varios compañeros periodistas y policías querían ponerse en contacto conmigo para conocer mi opinión sobre la tragedia que estaba acaparando ya todos los titulares de los informativos: «Ataque terrorista en Francia».

A las 11 de la mañana de aquel triste miércoles 7 de enero de 2015, los hermanos Saïd y Cherif Kouachi, fuertemente armados, habían irrumpido en la redacción del semanario satírico *Charlie Hebdo* y habían abierto fuego contra los presentes, asesinando a doce personas e hiriendo a otras once. Creo que desde las acciones de mi «padrino» Carlos el Chacal en diferentes puntos de París, no se recordaba un ataque de estas características en la capital francesa.

François Hollande ordenó subir el nivel del Plan Vigipirate a escarlata, el más alto.[106] El Elíseo no tenía la menor intención de permitir que los responsables del ataque escapasen.A mediodía, los informativos de todas las cadenas se hacían eco de la tragedia. Haciendo gala de una audacia encomiable, un videoaficionado había tomado unas imágenes de los hermanos Kouachi en su huida por el bulevar Richard-Lenoir, enfrentándose a tiros a la policía, y ejecutando a sangre fría a un agente de la policía metropolitana, Ahmed Merabet.

A partir de ese instante, todos los servicios de Inteligencia franceses iniciaron la caza. Durante cuarenta y ocho horas el mundo estuvo pendiente de París.

A las 8:10 a. m. del día siguiente, y a la altura del número 91 de la avenida Pierre Brossolette, en Montrouge, otro terrorista entra en acción. Amedy Coulibaly, un ciudadano francés de origen maliense y amigo de los hermanos Kouachi, asesinó a la agente de la Policía Municipal Clarissa Jean-Philippe, de veinticinco años, y dejó malherido a un funcionario del servicio de basuras antes de parapetarse en el supermercado *kosher* Hyper Cacher de la Rue Albert Willemetz, en el sureste de París, con varios rehenes. Ejecutaría a cuatro de ellos antes de ser abatido por las fuerzas especiales del RAID y la BRI-BAC el 9 de enero, tras un largo y angustioso asedio televisado en directo para todo el planeta.

Finalmente, ese mismo 9 de enero los hermanos Kouachi fueron localizados en Dammartin-en-Goële. Sus armas automáticas les conferían una evidente superioridad contra los dibujantes de *Charlie Hebdo* desarmados, e incluso contra la pistola de Ahmed Merabet, pero no contra el armamento pesado de los grupos de operaciones especiales franceses. A pesar de haber tomado rehenes para protegerse, siguieron la suerte de Coulibaly y ambos fueron abatidos en el tiroteo.

Dos días después, el 11 de enero, dos millones de personas se dieron cita en París para unirse a una multitudinaria manifestación contra el terrorismo. Entre ellos, cuarenta mandatarios llegados de diferentes países, incluyendo al presidente español

Mariano Rajoy. Mi viaje había empezado muy poco después de eso.

Jorge es un funcionario de los servicios de Información, al que conocí hace más de un lustro, tras la publicación de *El Palestino*, cuando el juez Eloy Velasco dictó solicitud de repatriación contra Arturo Cubillas, para ser procesado en España como enlace de ETA entre Venezuela y Europa.

—Toni, tú te mueves mucho por el ambiente de las mezquitas… ¿Has oído algo? —me preguntó tras el atentado a *Charlie Hebdo*.

—Sí, claro. He oído que la comunidad musulmana está indignada. He oído que al día siguiente al ataque lanzaron granadas contra una mezquita en Le Mans, y tirotearon otra en Port-la-Nouve. He oído que a los niños musulmanes, o árabes —sean musulmanes, judíos o cristianos— los están insultando y acosando en las escuelas francesas, y también aquí. He oído que el miedo que sentían los musulmanes a salir a la calle tras el 11-M ha vuelto. Y también los insultos, el desprecio y las agresiones. Eso he oído.

—Discúlpame, no quería molestarte.

—Tú eres católico, ¿verdad, Jorge?

—Sí, claro.

—¿Y vas a misa?

—No mucho. Ya sabes que este trabajo no te deja mucho tiempo libre. Algún domingo, o en alguna boda, bautizo o comunión.

—¿Y alguna vez has oído en la iglesia algo sobre algún atentado de ETA, el IRA o el Ku Klux Klan?

Sé que la intención de Jorge no era ofender al islam, sin embargo, su visión de los musulmanes era tan simplista y errónea como la de la mayoría de los occidentales. Como lo era la mía antes de conocerlo desde dentro. Tras cada atentado yihadista los medios de comunicación se ceban con los musulmanes, empeñados en satanizar a la comunidad religiosa más numerosa del planeta por las atrocidades que un minúsculo grupo de radicales hacen en su nombre. Con la misma legitimidad que matan, violan o torturan, en nombre de Jesús, otros radicales que se autodenominan cristianos. Es decir, ninguna.

Para esa visión sesgada y tendenciosa de lo que es el islam, las mezquitas son centros de adoctrinamiento y captación yihadista. Algo tan estúpido como pretender que las parroquias católicas son centros de reclutamiento y formación de ETA.

Lamento decirlo, pero muchos compañeros periodistas, y también algunos funcionarios de las Fuerzas y Cuerpos de Seguridad del Estado, manejan una profunda desinformación en relación al terrorismo internacional, a mi juicio por dos razones fundamentales. La formación y las fuentes.

Durante la preparación del personaje de Muhammad Abdallah para *El Palestino*, me matriculé en innumerables cursos sobre terrorismo que se impartieron en universidades, academias militares y centros privados de formación en toda España. Buscaba información práctica, operativa, que pudiese utilizar durante el trabajo sobre

el terreno, en cuanto viajase a Siria, Líbano, Venezuela, Egipto, Túnez, Palestina o Marruecos. Mi intención era integrarme en la madrasas coránicas y en las mezquitas, y quería saber cómo podía identificar a un posible terrorista entre los musulmanes, pero para mi sorpresa, la inmensa mayoría de los formadores (no importa que fuesen militares, policías o profesores universitarios) jamás habían visto a un terrorista en persona. Su formación era puramente teórica, y basada en teóricos anteriores. Esa es la explicación de que falsedades como los campos de adiestramiento yihadista de Isla Margarita o el mito de Hizbullah-Venezuela se replicasen una y otra vez en aquellos cursos, y también en Google y Wikipedia. La formación teórica es importante, es fundamental, pero solo si los datos los contrastan fuentes humanas sobre el terreno.

Y en cuanto a las fuentes, siempre según mi experiencia personal, los servicios de Información e Inteligencia tienen un problema a la hora de manejar información sobre lo que ocurre realmente en las mezquitas. Existen muy pocos funcionarios de las Fuerzas y Cuerpos de Seguridad del Estado que hablen árabe y/o sean musulmanes. Y menos aún dispuestos a infiltrarse en el terrorismo yihadista. La figura del agente encubierto y el agente provocador apenas están recién legisladas en España, y en un país tan garantista como el nuestro, las trabas legales para hacer ese tipo de investigación encubierta son enormes.

Por esa razón, y como ocurre en muchos otros ámbitos de la investigación policial, los seguimientos y las vigilancias se hacen a distancia. Videocámaras de vigilancia, dispositivos GPS, teleobjetivos ocultos en furgonetas camufladas… Pero aunque ese tipo de vigilancia pueda aportar caras, matrículas, etcétera, no permite comprender quién es quién, y por qué está allí.

Creo que la mejor forma de ilustrarlo es con un ejemplo práctico. Pero no seré yo quien lo dé, sino David R. Vidal, el «agente Juan». Entre 2004 y 2010, durante mi infiltración en el terrorismo internacional, David ya trabajaba para el CNI, simultaneando la dirección de dos redes de informadores en África. Unos a sueldo del Ministerio del Interior y otros al servicio del Centro Nacional de Inteligencia. Pero además de la inmigración ilegal, el CNI solicitaba los servicios de David para algunos otros asuntos menos confesables, y que David tocará llegado el día y si lo considera oportuno.

En su libro *Diario de un espía*, y más concretamente en el capítulo «Islamismo radical», relata una anécdota que resume perfectamente el instante en que volví a encontrármelo, años después de su valiosa asesoría en *El año que trafiqué con mujeres.* Aunque más bien me encontró él a mí:

> Hace un par de años, un agente de los servicios de Inteligencia me mostró una fotografía donde aparecía un grupo de gente a la puerta de una mezquita, mientras me preguntaba si reconocía a alguno de ellos… En efecto, conocía a uno: allí estaba el periodista Antonio Salas ataviado con *styling* palestino. La verdad es que su aspecto era de lo más sospechoso. Parecía sacado de una película de serie B, en las que nada más aparecer el malo ya se sabe cuál será su papel en la trama… (dicha fotografía) había sido realizada por el servicio de información de la Guardia Civil adscrito a la comandancia provincial, quienes estaban intentando identificar al converso, blanco y barbudo…[107]

Y como los policías no suelen entrar en las mezquitas, la inmensa mayoría de la información manejada por nuestros servicios proviene de confidentes. Inmigrantes con pocos recursos, captados por tal o cual agencia de Inteligencia o servicio de Información, que cobran una gratificación por delatar a los terroristas. Si en la mezquita hay terroristas, hay gratificación. Pero si en la mezquita todo es un remanso de paz y no hay nada de lo que informar, el confidente no cobra.

Estoy seguro de que si el servicio que consultó a David Vidal hubiese preguntado a alguno de sus confidentes en aquella mezquita por el tipo de aspecto checheno recién llegado, se habría encontrado con alguna historia rocambolesca para mantener el interés de sus patrocinadores, y seguir ganándose el sueldo. Si además hubiese sospechado que el falso checheno era en realidad un «peligroso terrorista» adiestrado en Venezuela, recién llegado de Siria o Líbano, y con contactos directos con Carlos el Chacal, sin duda se habría ganado una paga extra, y yo tener que dar muchas explicaciones…

En mi humilde opinión, siempre es mejor trabajar sobre el terreno. Te da otra perspectiva y siempre, siempre, aparecen nuevas fuentes humanas. Por eso me fui a París.

Geografía del terror

En cuanto el comandante de mi vuelo anunció que estábamos a punto de aterrizar en el Aeropuerto Internacional de Orly Sud, sentí un ligero escalofrío. Yo había leído mucho sobre aquel aeropuerto, uno más en los puntos que salpican el mapa del terror en la capital francesa. Uno que me tocaba de cerca.

París es una de las capitales europeas con una mayor historia terrorista desde el siglo XIX. En la Nochebuena de 1800, Napoleón Bonaparte sufrió un intento de asesinato en la Rue Saint-Nicaise, cuando acudía a un concierto. Un carromato cargado con un tonel de pólvora explotó unos segundos después de que el carruaje de Napoleón lo rebasara: dejó 22 muertos inocentes y más de 50 heridos, Napoleón salió indemne. Aquel atentado sería una premonición de toda la violencia, sangre y muerte que viviría París en tiempo de paz. Durante el siglo XIX, nacionalistas y anarquistas atentaron en la capital francesa, pero durante el XX es cuando el protagonismo de París se consolidaría en la historia del terrorismo internacional.

En los años treinta los fascistas del Comité Secreto de Acción Revolucionaria, más conocidos como The Hood (La Capucha), realizaron varios atentados contra objetivos comunistas o antifascistas. Y en los sesenta y primeros setenta otras organizaciones terroristas de extrema derecha, como la Organisation de l'Armée Secrète (OAS) o el Grupo Charles Martel, continuaron sembrando de bombas la capital francesa. Sin embargo, en esa década de los setenta, la polaridad política del terrorismo cambia de extremo, y son grupos de izquierda, como la Organización para la Liberación de Palestina (OLP), o los españoles Grupos de Acción Revolucionaria Internacionalista, quienes comienzan a ejecutar operaciones en la ciudad del Sena. Y en este baño de siglas y armas irrumpe mi mentor, Ilich Ramírez Sánchez, «Carlos el Chacal», el mismo que mató a conciencia en París durante los años setenta y ochenta.

Como dice el periodista Stephen Smith, consultor histórico de la trilogía *Carlos* —dirigida en 2010 por Oliver Assayas y protagonizada por Edgar Ramírez— y probablemente una de las mayores autoridades internacionales en la figura del Chacal: «Carlos cambió el mapa de París con sus atentados». Y está en lo cierto.

Me asomé a la ventanilla para contemplar el aterrizaje y recordar todo lo que había estudiado sobre la trayectoria de Carlos el Chacal mientras me convertía en el webmaster de su página oficial en internet y de su perfil en Facebook. Justo allí, en aquel aeropuerto, el 13 de enero de 1975 Carlos organizó un ataque contra un Boeing 707 de las Aerolíneas Israelíes cuando despegaba con 136 pasajeros con destino a Nueva York. Pasajeros, como yo, civiles, que salvaron la vida de milagro, porque el proyectil erró el blanco y fue a impactar contra un DC9 de la MacDonnell Douglas que gracias a Dios acababa de desembarcar al pasaje.

Inasequible al desaliento, Carlos volvió a intentarlo en el mismo aeropuerto de París seis días más tarde. En esta ocasión la Policía detectó a los terroristas y tras un

tiroteo, varios de los camaradas de Ilich fueron detenidos. Chacal, como en tantas ocasiones, consiguió escapar…

Entre marzo de 2007 y mayo de 2010, yo fui el responsable de la vida digital de Carlos el Chacal. Localizar a su familia en Venezuela resultó muy complicado, pero ganarme su confianza fue una misión casi imposible. Sin embargo, sabía que convertirme en el gestor de su *website* oficial www.ilichramirez.blogspot.com, y de su perfil en Facebook reforzarían de forma extraordinaria mi tapadera como Muhammed Abdallah. Y así fue. Cuando cualquier «revolucionario» del planeta quería contactar con Ilich Ramírez a través de internet, en realidad contactaba conmigo. Y eso me supuso el acceso a personajes como Eduardo Rozsa, muerto el 16 de abril de 2009, acribillado a tiros con varios de sus hombres, durante una operación antiterrorista en Bolivia.

Creo que durante aquellos años llegué a conocer bien al Chacal. Siguiendo sus indicaciones —«Será bueno que grabases lo que hablamos»—, conservo docenas y docenas de horas de conversaciones telefónicas entre nosotros, ademásde haber tenido acceso a todas sus fotos, correspondencia íntima, documentos, expediente escolar, y demás, gracias a su madre doña Elba Sánchez, y a sus hermanos pequeños Vladimir y Lenin Ramírez, como relato extensamente en *El Palestino*.

Quizá por eso se me hacía extraño andar por aquellas calles. Porque sabía que estaba en la misma ciudad que él, tan cerca y a la vez tan lejos.

Durante horas visité los escenarios de la «obra» de Ilich Ramírez en París. El cruce del Boulevar Saint-Germain con la Rue Rennes, donde el 15 de septiembre de 1974 se produjo uno de los ataques más brutales del Chacal cuando hizo estallar la Publicis Drugstore —uno de esos locales que aúnan tienda, farmacia, cafetería y estanco—, dejando tras de sí dos muertos y 34 heridos, entre ellos cuatro niños. Los Campos Elíseos, donde el 16 de febrero de 1982 fue detenida Magdalena Kops, esposa de Ilich y madre de su única hija reconocida, Elba, cuando preparaba un atentado contra la revista *Al Watan Al Arabi* con un coche bomba, por órdenes del Chacal. El 33 de la Rue Marbeuf, donde en efecto se encontraba la redacción de la revista, que a las 9:02 a. m. del 22 de abril de 1982 saltó por los aires, dejando un muerto y 63 heridos, mutilados y amputados. Y la Rue Toullier, donde empezó todo.

Me sorprendió. Había cambiado mucho en estos años. No se parecía a las fotografías que había visto tantas veces, mientras me familiarizaba con la historia de Ilich Ramírez para preparar nuestras conversaciones semanales. Por aquellas calles caminó un Ilich ya asesino, pero todavía anónimo, disfrutando de la vida con amigos como Luis Enrique Acuña, a quien conocí en Venezuela durante la investigación.

El 17 de junio de 1976, en el número 9 de la Rue Toullier, Ilich ejecutó a dos policías franceses (dejando a un tercero malherido) y al enlace del FPLP en Francia,Michel Moukharbal, que había conducido a los agentes hasta el apartamento. Todos iban desarmados. Hasta entonces se había ocultado bajo la identidad de un peruano llamado Carlos Martínez; tras la masacre, las fotografías del sospechoso

fueron publicadas en todos los medios franceses, y Martínez fue inmediatamente identificado como el venezolano Ilich Ramírez Sánchez. A partir de ese día comenzó la caza del Chacal.[108] Allí, en la Rue Toullier, a pocos metros de la Universidad de la Sorbona, y muy cerca del Panteón donde descansa mi admirada Maria Salomea Skłodowska-Curie, se inició la leyenda de Carlos el Chacal. Y lo que resulta paradójico, concluyó a apenas un par de kilómetros.

Tomé un taxi, y en pocos minutos me apeé en mi último destino en aquel recorrido por el París del Chacal. Dos kilómetros, solo dos kilómetros separan la Rue Toullier de la prisión de La Santé donde Ilich cumple la pena de dos cadenas perpetuas.

Me senté en el rellano de un portal situado enfrente, a no más de 10 metros, y durante unos minutos me quedé embelesado contemplado los enormes muros que flanquean el centro penitenciario, y la entrada al mismo. Y recordé su voz. Me pasé horas y horas escuchándole cada vez que me telefoneaba desde allí dentro. Nunca habíamos estado físicamente tan cerca. Imaginé que tal vez en esos momentos estaba paseando por el patio interior de la cárcel con alguno de sus amigos de ETA, como Juan Cruz Maiza Artola, exjefe de logística, o el legendario Mikel Garikoitz Aspiazu Rubina «Txeroki», detenido en la localidad francesa de Cauterets el 17 de noviembre de 2008, mientras yo representaba al Chacal en una reunión internacional en Estocolmo. Ilich me confesaría en una de nuestras conversaciones que alguno de sus amigos etarras también se había convertido al islam, pero no me precisó quién.[109]

Casi podía sentir su presencia al otro lado de aquel muro. Y me pregunté qué pasaría si pudiese asomarse a la ventana de su celda y pudiese verme allí, en la calle, a solo unos metros. El Chacal, el terrorista más famoso de la historia hasta la aparición de Ben Laden, estaba acostumbrado a manipular a las personas en su beneficio, especialmente a las mujeres. Y después de tantos años, él había sido el manipulado, por un simple periodista *freelance*, que lo había utilizado como cobertura para su infiltración en el terrorismo internacional… Supongo que no le hizo gracia. Porque a pesar de que en cuanto se publicó le envié un ejemplar de *El Palestino* a prisión, nunca volvió a telefonearme ni a escribirme directamente. Amor propio, imagino.

En 2011, durante el juicio por los atentados de *Al Watan Al Arabi* y los trenes de París, y mientras el Chino y sus hombres me buscaban por Europa, Ilich Ramírez concedió una entrevista al diario venezolano *El Nacional* donde hizo unas explosivas declaraciones: explicaba que los más de cien atentados que había comandado durante sus sesenta y dos años de vida bien podrían haber causado entre 1.500 y 2.000 muertos. «Fueron golpes bien ejecutados, sin apenas errores. Tan sólo debió de haber doscientas víctimas civiles colaterales.»[110]

Parece evidente que Ilich está donde debe estar. Uno de los dos únicos lugares donde terminan todos los terroristas. El otro es el cementerio. Esa es la opción que Amedy Coulibaly y los hermanos Kouachi escogieron.

Anónymous y su #OpCharlieHebdo

A pesar de que todavía no nos conocíamos, cuando le dije al hacktivista Lord Epsylon que pensaba viajar a Francia y le pregunté si podía facilitarme algún contacto, tuvo la amabilidad de hacerlo. En uno de sus emails cifrados en PGP me indicó un lugar: un hacklab de París.

Louis (nombre supuesto) es uno de los hacktivistas que participaron en la Operación Charlie Hebdo, de Anónymous, y en las que se sucedieron. Tras los atentados del 7 y 8 de enero, Anónymous declaró formalmente la ciberguerra al Estado Islámico. «El 7 de enero de 2015, se lastimó la libertad de expresión —dijo Anónymous—. Es nuestra responsabilidad reaccionar». Así, el pistoletazo de salida de la #OpCharlieHebdo fue un vídeo colgado en YouTube el 9 de enero de 2015: un comunicado en francés de Anónymous al Estado Islámico:[111]

> Nosotros, Anónymous del mundo, hemos decidido declararos la guerra, terroristas. Localizaremos hasta el último de vosotros y será vuestro fin. Os permitís asesinar gente inocente, así que tenemos la intención de vengarnos en su nombre. Vamos a vigilar vuestras actividades en la red y vamos a tumbar vuestras cuentas en todas las redes sociales.
>
> No impondréis vuestra *sharia* en nuestras democracias. No dejaremos que vuestras estupideces destruyan nuestra libertad de expresión. Os lo hemos advertido, os espera la destrucción. Os seguiremos la pista en cualquier parte del planeta. No estaréis a salvo en ningún sitio.
>
> Somos Anónymous. Somos legión. No perdonamos. No olvidamos.
>
> Temednos. Estado Islámico y Al Qaeda, nos vengaremos.

La voz surge firme en el vídeo. Nos llega desde detrás de una máscara de Guy Fawkes que Anónymous ha convertido en su símbolo universal, aun cuando su historia real es muy anterior a internet y el hacktivismo.

Fawkes nació el 13 de abril de 1570 y fue un conspirador católico inglés que sirvió en los legendarios Tercios de Flandes españoles como mercenario. Posteriormente se unió al grupo del Restauracionismo Católico que luchaba contra la Iglesia Anglicana impuesta en Inglaterra por Enrique VIII, y que planeó la Conspiración de la Pólvora con objeto de volar el Palacio de Westminster y asesinar al rey Jacobo I de Inglaterra, a toda su familia y a los Lores británicos, para erradicar el protestantismo e instaurar la religión verdadera en Londres: el catolicismo. Mucho antes de la fundación del IRA, católicos y protestantes ya se mataban unos a otros en el Reino Unido. En otras palabras, Guy Fawkes era un terrorista religioso similar a los que Anónymous pretendía combatir. Paradojas de la historia.

El 5 de noviembre de 1605, Fawkes era el responsable de detonar los explosivos colocados bajo la Cámara de los Lores, pero algún compañero lo delató y fue detenido en la bodega situada bajo la cámara, con 36 barriles de pólvora listos para explotar. Torturado, Fawkes reveló los nombres de algunos de sus compañeros en la conspiración, aunque solo los que ya estaban muertos o aquellos a quienes ya conocía el Gobierno. Por esa razón fue considerado un héroe. Condenado a morir quemado en

la hoguera, su nombre y la fecha de su captura entraron en el imaginario popular británico y a finales del siglo XVIII comenzó a recordarse su historia utilizando máscaras de Guy Fawkes en la celebración de la Noche de las Hogueras cada 5 de noviembre.

Aun así, hoy quizá la máscara sea más conocida por el cómic en blanco y negro *V de Vendetta* —del guionista Alan Moore y guionizado por David Lloyd—, y su posterior adaptación cinematográfica —dirigida por James McTeigue y con una radiante Natalie Portman en el papel protagonista—. Y así, Guy Fawkes resurgió literalmente de sus cenizas para luchar contra una dictadura tecnocrática en el siglo XXI. La máscara de Guy Fawkes, ya estilizada, inundó las pantallas de los cines de todo el mundo. La escena de todos los ciudadanos manifestándose ante el Parlamento londinense ataviados con la máscara sin duda impresionó a muchos hacktivistas. Por eso, cuando en 2008 los primeros activistas de Anónymous se echan a las calles, durante el Proyecto Chanology contra la Iglesia de la Cienciología, algunos de sus simpatizantes lucen la máscara de Fawkes. Y desde entonces hasta ahora, cuando una voz tras esa misma máscara declara la guerra al Ejército Islámico y a Al Qaeda.

Los hacktivistas, hasta ese día criminalizados como un grupo de ciberbandidos antisistema, se ganaron la simpatía de todos los franceses al prometer que identificarían todos los sitios web yihadistas y las cuentas de sus usuarios en las redes sociales, y que harían pública su información personal. «No vamos a descansar hasta que caigan de rodillas.» Sin embargo, los servicios de Información no compartían el entusiasmo de la ciudadanía. Es comprensible: la lucha contra el terrorismo es muchas cosas, y entre ellas una gran partida de ajedrez donde a veces el sacrificio de un alfil o una torre, en un movimiento en apariencia inexplicable, pretende obtener un jaque mate a largo plazo.

Para los responsables policiales, militares y políticos de la lucha antiterrorista en Francia, la intromisión de los hacktivistas solo podía acarrear movimientos de fichas inesperados en el desarrollo de la partida. Y ninguno sería para bien. En el menor de los males, si Anónymous comenzaba a revelar cuentas de Twitter o Facebook vinculadas al yihadismo, podrían descubrir que muchas de esas cuentas pertenecían a agentes de Inteligencia. O a periodistas infiltradas como Anna Erelle. Pero a Anónymous nunca le ha preocupado mucho lo que opinen los responsables políticos o policiales.

Es importante comprender que Anónymous no se parece a otros grupos hacktivistas históricos como Network Liberty Alliance, milw0rm, Cult of The Dead Cow o los letales y divertidos Lulzsec.No es una organización, ni una asociación, ni siguiera un grupo estructurado. Es una dinámica. Una corriente de pensamiento que fluye por la red y en la que un número indeterminado de individuos, sin un rango, liderazgo o mando mayor que los demás, se dejan arrastrar para una acción determinada. Nunca los mismos ni por la misma razón. Una legión que no olvida, ni perdona, pero que funciona en sintonía con una idea, no con una junta directiva.

Desde su aparición en 4chan en 2003, el fenómeno Anónymous se extendió por la red como un gusano que se replica a sí mismo, llegando hasta los últimos rincones del planeta que dispusiesen de una conexión a internet. El ataque a la Iglesia de la Cienciología, que comenzó como una simple «troleada», descubrió a los internautas que juntos, coordinándose en una acción puntual, tenían un poder del que no disponía ningún individuo. Y desde ese instante fueron las causas las que condicionaron la acción. No la orden de una cúpula de mando.

La lucha contra la pedofilia, el apoyo a Wikileaks, o el ataque a los secretos de los gobiernos son causas que enseguida encontraron aliados en las redes, dispuestos a sumarse. De forma espontánea, sin afiliarse a ningún partido, organización o asociación. A partir de ahí, y con el paso de los años, los foros de internet, y la experiencia acumulada tras las detenciones de muchos participantes en alguna de sus acciones, fueron depurando el estilo, y estructurando los mecanismos de actuación.

En una circunstancia tan traumática como el ataque a *Charlie Hebdo,* no hizo falta discutir mucho. Casi todos los internautas franceses que frecuentaban dichos foros, muchos de ellos musulmanes, estaban de acuerdo. La necesidad de luchar contra el ISIS en la red era algo tan obvio como revelar la identidad de los pedófilos. Y comenzó el ataque, coordinado desde varias direcciones de internet, y tanto foros de chat como *hashtag* de Twitter.[112]

Las semanas siguientes serían agotadoras. Louis y sus compañeros se pasaron días y noches enteras, literalmente, pegados al ordenador. Buscando yihadistas.

El primer objetivo fue el foro yihadista Ansar-AlHaqq.net, que fue hackeado por los hacktivistas y terminó desapareciendo de la red.

Ya en 2010 varios moderadores y administradores del sitio habían sido formalmente acusados de «asociación criminal en relación con una organización terrorista»; pero la web continuó operativa. En 2013 se repitieron las acusaciones contra Ansar-AlHaqq.net, tras el casoMohammed Merah, el yihadista que asesinó a varios judíos y militares franceses en Toulouse y Mountalban en marzo de 2012; pero la web continuó operativa.

Los atacantes de Anónymous, que por su propia infraestructura deciden las acciones más por un impulso emocional que por una estrategia a largo plazo, no pudieron o no quisieron comprender que si una web frecuentada por yihadistas había continuado operativa, era porque el Gobierno francés, debidamente asesorado por sus agencias de Inteligencia, lo permitía. Quizá porque resultaba más beneficioso para la lucha antiterrorista toda la información que podían extraer de ella o como canal para infiltrar agentes, que cerrarla definitivamente.

Tras el ataque a Ansar-AlHaqq.net, la #OpCharlieHebdo de Anónymous identificó doscientas cuentas de Twitter de supuestos yihadistas o simpatizantes del atentado contra el semanario francés. Lo interesante no es que Anónymous alojase en una web el listado de esas cuentas de Twitter, sino que algunos prestigiosos medios de comunicación linkasen ese listado en sus crónicas sobre la campaña de los hacktivistas.

Ni yo ni nadie puede saber cuántos de los usuarios de aquellas cuentas eran en verdad simpatizantes del ISIS, y cuántos infiltrados que estaban tratando de obtener información para algún tipo de acción que causase más daño al Estado Islámico que cerrar una simple cuenta de Twitter.

Anónymous no descansaba. En febrero surgió la Operación ISIS. Bajo el *hashtag* #OpISIS, renovó su empeño en combatir el yihadismo en internet, y llegó a señalar hasta 10.000 cuentas de presuntos simpatizantes del Estado Islámico en Facebook y Twitter. No quedó ahí: en la nueva fase de su Operación Charlie Hebdo, a mi juicio más inteligente y perjudicial para los intereses del ISIS en la red, Anónymous generó contenidos en los buscadores de Google para desplazar los referentes al Estado Islámico. También establecieron un protocolo para que cualquier usuario de Facebook o Twitter pudiese localizar cuentas yihadistas y denunciarlas a Anónymous, la Policía o a los mismos responsables de la red social. En su memorando, Anónymous enseñaba a los usuarios a «hacer inteligencia» una vez identificaban una cuenta marcada como yihadista. Cómo rastrear a su usuario en otras redes sociales. Cómo seguir el hilo de Ariadna de sus contactos y *followers* hacia otros presuntos yihadistas…

Y probablemente una de las aportaciones más importantes de la ciberinvestigación digital a la investigación policial fue el descubrimiento de la cuenta que Saïd Kouachi se había creado en Facebook el 19 de abril 2014. Allí

estaban las señales de alarma, pero nadie supo verlas. Aunque Facebook cerró la cuenta de Kouachi después de identificarse como uno de los terroristas, todo lo que sube a la red se queda en la red. Los hacktivistas recuperaron las fotos, posando con armas, haciendo prácticas de tiro y demás, que habían estado allí, a la vista de todos, antes del ataque. Esas imágenes, comentarios y «amigos» de Kouachi en Facebook marcarían una de las líneas de investigación policial.

En abril de 2015 el Ejército Islámico perdía Tikrit, uno de sus baluartes en el frente sirio, y también 13.000 cuentas de correo y perfiles en redes sociales. Y Anónymous ejecutó la tercera fase de su particular ciberguerra, con una nueva publicación de cuentas y emails vinculadas al ISIS. 13.000 referencias de simpatizantes del Estado Islámico en la red.

Si esto hubiese ocurrido unos años atrás, estoy seguro de que mis cuentas como Muhammad Abdallah, y mis blogs, perfiles sociales o las páginas de Carlos el Chacal y el foro de Hizbullah-Venezuela que yo controlé habrían sido incluidas en ese listado.

En la campaña, como en todas las acciones pasionales y globales, pagaron justos por pecadores. Por ejemplo, también fue atacada Oumanger-halal.fr, una inofensiva web francesa que facilitaba a los usuarios musulmanes la ubicación de restaurantes y

tiendas de comida *halal*. Anónymous negó cualquier relación con el ataque, pero aquellos ataques a sitios inocentes, y la islamofobia que se extendió por la red en aquellos días, produjo otro fenómeno reseñable: la réplica de los hackers musulmanes no yihadistas.

Bajo el nombre de la MECA, Votr3x, TN Prodigy, equipo Fallaga, Makers Hacker Team, AnonGhost y otros tantos, algunos grupos de hackers habían decidido proteger la imagen del islam en internet.

Si bien la etiqueta Anónymous es global y anárquica, era predecible que dentro de una corriente tan multitudinaria comenzarían a establecerse pequeños subgrupos, en función de la empatía, el idioma, o la ubicación geográfica de sus participantes. Como Redcult, AnonGhost o la española La9deAnon. Ramificaciones locales o nacionales, que no siempre comparten la ideología, la metodología o los objetivos del resto de Anónymous. Anónymous Venezuela es un excelente ejemplo.

Pero los une algo: saben moverse en la red. Ese, y no el de las bombas o los AK-47 de los hermanos Kouachi, es su campo de batalla.

«Je Suis Charlie» vs. «Je Suis Ahmed»

Louis, que hablaba tanto español como yo francés, fue sin embargo de gran ayuda para ubicar los lugares donde todo ocurrió, y también para conseguir un buen número de ejemplares atrasados de *Charlie Hebdo.*

El lugar donde comenzó la tragedia es el número 10 de la Rue Nicolas-Appert, en el Distrito XI de París. Situada en la orilla norte del Sena, y no demasiado lejos de la Plaza de la Bastilla. Mide exactamente 137 metros de largo por 15 de ancho, y a mí me inspiró una agobiante sensación de tristeza. En muchos de los comercios de las calles colindantes, fundamentalmente oficinas, todavía colgaban los carteles de *Je Suis Charlie*, la campaña de apoyo a las víctimas que inundó Francia y buena parte del mundo tras el ataque. El edificio donde se produjo la matanza está al final de la calle, haciendo esquina con Allee-Verté. La redacción del semanario satírico *Charlie Hebdo* solo llevaba en aquella ratonera un año.

Estar allí, sobre el terreno, era muy diferente a ver las noticias del ataque en los informativos. Me impresionó el silencio. A pesar de encontrarse a solo un par de calles del transitado Boulevard Richard Lenoir, la calle Nicolas-Appert no parece la típica del centro de París, sino más bien un suburbio industrial de la periferia de Barcelona o Valencia. Ignoro si siempre fue así, o todavía permanecía en el ambiente el duelo por las víctimas, pero reconozco que la sensación era muy desagradable. Como si el aire continuase enrarecido por el olor a pólvora de los Kalashnikov que los hermanos Kouachi utilizaron en el ataque. Conozco el arma. Aprendí a usarla, montarla y desmontarla durante mi adiestramiento paramilitar en Venezuela. Un arma ideada para matar de forma eficiente, y una de las más utilizadas en el mundo. Por eso es más fácil conseguir munición para alimentarla.

Durante la siguiente hora recorrí los alrededores, desde el sitio donde se había detenido el Citroen C3 II negro de los Kouachi —y donde regresarían de nuevo tras el atentado, entre gritos de «Hemos matado a *Charlie Hebdo.* Allah es el más grande»—, hasta la altura del número 62 de Richard Lenoir, donde respondieron con ráfagas de los AK-47 al fuego de las pistolas de los agentes. El mismo sitio donde remataron en el suelo y de un tiro en la cabeza a un policía herido. Su nombre era Ahmed Merabet. Tenía cuarenta años y era musulmán.

Me paro en el lugar exacto donde murió. Alzo la vista y tampoco me resulta difícil identificar la ventana desde la que se grabó el vídeo de su ejecución. Jordi Mir, un ingeniero de cincuenta años, escuchó los disparos, se asomó a la ventana y grabó los últimos 42 segundos de vida de Merabet antes de que lo rematasen y luego subió el vídeo a su perfil de Facebook. Se arrepintió a los quince minutos y lo borró… Demasiado tarde. Todo lo que sube a la red se queda en la red.

Mir tenía 2.500 amigos agregados en su cuenta y para cuando se lo pensó, varios de ellos ya se lo habían descargado y ya estaba replicado en cientos de páginas y perfiles. El hermano de Ahmed le reprocharía posteriormente que hubiese divulgado

la ejecución de su hermano. Supongo que a ninguno nos gustaría que un vídeo con la muerte de un ser querido se convierta en *trending topic* de Twitter, y encontrarnos esas imágenes cada vez que encendemos la televisión o abrimos el ordenador.

Desde allí los Kouachi iniciaron su fuga, aunque les quedaban solo unas horas de vida a ellos también. Tras su muerte, Al Qaeda en Yemen reivindicaría el atentado contra *Charlie Hebdo.*

Me quedo unos minutos observando la calle. Sin duda es el lugar que aparece en el vídeo de Jordi Mir. Saco la tablet y visito una página que conozco bien. La consultaba casi a diario mientras estudiaba árabe porque ofrecían un curso *online* que me resultó de ayuda. Compruebo que el artículo que tanta desconfianza me generó todavía está en línea. Y siento lástima.

MusulmanesAndaluces.org fue una de las miles de webs que se hicieron eco de las teorías conspiranoicas según las cuales el ataque a *Charlie Hebdo* era un atentado de falsa bandera. Que las calles que aparecían en el vídeo ni siquiera eran de París. Que es imposible disparar un AK-47 con una sola mano y otras frivolidades parecidas. Están equivocados. Todo ocurrió allí. Y obviamente quien afirma cosas como esa ha disparado poco con un AK-47.[113]

Era una respuesta emocional lógica. Tras el atentado, muchos miserables, que se autodenominaban musulmanes, celebraron el ataque en las redes sociales. En diferentes países árabes los vídeos del ataque fueron replicados bajo el *hashtag* en árabe «París brûle», calificando de «héroes» a los Kouachi. Un cretino llamado Najam (@ 35njm) escribió: «#París arde. Oh Allah, mátalos, Alá, atácalos». Uno de tantos.

Más daño hicieron en Francia los tuits en francés de los defensores del ISIS, como Abu Hafs (Ansar_Al_Ouma) «El honor del profeta fue lavado». Abu-Talhal (@ Abu-Talhal) lamenta que los tiradores no tuviesen cámaras montadas en sus armas, para tener mejores imágenes de la matanza. Más radical un tuitero llamado El Kheyrad (Kheyradine) llama a la lucha: «Ármate y no le des la espalda. Sed soldados de Allah!», antes de amenazar a Hollande y elevar a rango de mártir y héroe a los terroristas.

Se me revuelve el estómago. La lista de ejemplos es tan extensa como vomitiva. Con cada uno de esos tuits, absolutamente antimusulmanes, anticristianos y antihumanitarios, los descerebrados que los escribían estaban polarizando todavía más a la opinión pública contra el islam. Quizá, en su manifiesta ignorancia, creían que lo que escribían en Twitter solo podían leerlo sus amigos de confianza… Sus cuentas fueron las que animaron en buena medida a Louis y a sus amigos de Anónymous a iniciar la campaña #OpCharlieHebdo. Y fueron las primeras en ser atacadas. Por gilipollas.

Lo que yo ignoraba, y me confesó Louis, es que algunos cristianos ultraconservadores también se habían alegrado del ataque. Me sorprendió. Hasta que me facilitó algunos ejemplares atrasados de la revista *Charlie Hebdo.*

Otro simpatizante del ISIS, Hamel Al-Liwa (@ blue964), había tuiteado: «El miedo reina entre los periódicos y periodistas que odian el islam», pero @ blue964 se equivocaba. Los dibujantes de *Charlie Hebdo* no odiaban al islam. En el mejor de los casos odiaban —o sería más justo decir que no respetaban— todas las religiones. Abogaban por una sociedad laica. Y estaban en su derecho, aunque quizá, al no compartir ningún sentimiento religioso, no podían comprender que algunas de sus viñetas eran una agresión a quienes sí lo sentían.

Hasta ese momento yo solo conocía las caricaturas del profeta Muhammad (saas) que habían generado la polémica. De hecho, a mí me había pillado en plena infiltración, viviéndola desde el lado musulmán.[114] Pero *Charlie Hebdo* había ido más allá que los daneses *Jyllands-Posten* o *Politiken*. Es cierto que algunas de sus portadas a mí me parecieron un ejercicio magistral de sátira, lanzando un mensaje contundente y razonable a través del humor. Por ejemplo, el número 712, en cuya portada el profeta Muhammad (saas) se lamenta: «Es difícil ser amado por idiotas». Los Kouachi hicieron real, una vez más, esa reflexión.

Puedo comprender la genialidad de la portada del número 1.163, donde bajo la leyenda «Si Mahoma regresara» se representa a un yihadista decapitando al fundador del islam mientras este le dice: «Yo soy el profeta, atontado» a lo que un *mujahid* responde «Jódete, infiel». O la del número 1.011, en la que se le representa sonriente y diciendo: «100 latigazos si no te estás muriendo de risa». Aquella inocente portada motivó uno de los primeros ciberataques sufridos por la revista, el 2 de noviembre de 2011, en que sus servidores fueron hackeados. Ojalá todo se hubiese quedado ahí.

Puedo entender el mensaje del número 1.012: un musulmán besándose apasionadamente con uno de los dibujantes de la revista bajo la leyenda «El amor es más fuerte que el odio». Incluso la del número 1.099, donde un musulmán es acribillado a balazos mientras interpone un ejemplar del Corán, atravesado por los proyectiles, y exclama «El Corán es una mierda, no detiene las balas».

Sin embargo, la elegancia, el ingenio y la brillantez de una crítica satírica tan lúcida como esa se veía empañada por viñetas más soeces, facilonas y de cuestionable buen gusto, que yo no había visto antes. Y que se encontraban en el interior de las revistas. Caricaturas del fundador del islam teniendo sexo anal con sus seguidores, o practicando felaciones… No conseguía encontrar el mensaje constructivo en aquellos dibujos. De la misma forma en que no encontraba el sentido de otras viñetas donde se representaba a líderes del judaísmo o del cristianismo, en actitudes sexuales obscenas y gratuitas, a mi juicio prescindibles.

Supongo que no soy un bicho raro si no consigo encontrar ni el buen gusto ni la necesidad de una cubierta así. E imagino que a ese tipo de portadas de *Charlie Hebdo* se refería el papa Francisco al hablar del límite de la libertad de prensa.[115]

En España ya no nos acordamos, pero algunos números de *Charlie Hebdo* despertaron grandes críticas entre intelectuales, políticos y funcionarios, por su frivolización de los atentados de ETA. Por ejemplo, en el número 503, publicado en julio de 1980, año en que ETA asesinó a cien personas —entre los cuales había mujeres y niños—, los dibujantes del semanario representaron, bajo el titular «Bombas en España», a una mujer desnuda que exclama con alegría sobre la onda expansiva de la detonación «Qué bien, esto me levanta los senos».

Pero nada. Ni el humor negro sobre ETA, ni Jesús sodomizado, ni las caricaturas del profeta Muhammad (saas), absolutamente nada, en ninguna circunstancia, justifica el uso de la violencia. El mismo fundador del islam lo dijo, en uno de los hadices compilado por Muslim: «La tinta del sabio es más sagrada que la sangre del mártir». Los tuiteros que celebraron los atentados contradecían al profeta: o

pretendían saber más que el fundador del islam, o lo consideraban un incompetente. En cualquiera de ambos supuestos no pueden considerarse musulmanes.

Inmediatamente después del ataque a la redacción de *Charlie Hebdo,* la batalla se trasladó a la red. Mientras un puñado de cretinos celebraba el atentado, y los hacktivistas de Anónymous ponían en marcha la #OpCharlieHebdo, un *hashtag* se convirtió en *trending topic* mundial: #JeSuisCharlie.

En todo el planeta millones de personas se solidarizaron con las víctimas diciendo: «Yo soy Charlie» en sus redes sociales. Ese fue el lema de la multitudinaria manifestación que se congregaría cuatro días después en París, con los líderes de diferentes gobiernos en cabeza. Supuestamente. Solo que era mentira. Los jefes de Estado no estuvieron en la manifestación. Se concentraron para la foto [(@lemondelive) enero 11, 2015], aislados de los manifestantes y rodeados por un férreo control de seguridad, cosa razonable dado el nivel de alerta terrorista que se había establecido en París. Lo que resulta triste es que pretendiesen hacernos creer que se habían unido a los dos millones de manifestantes que acudieron allí, desde todo el mundo, por un sentimiento honesto y sincero.

El 7 y 8 de enero el lema #JeSuisCharlie traspasó la red para imprimirse en camisetas, pancartas, estandartes, carteles, etcétera. Pero ese día, el jueves 8 de enero de 2015, un conocido activista de origen libanés, afincado en Bélgica, subió a su perfil en Twitter un mensaje demoledor.

«Yo no soy Charlie, soy Ahmed, el policía muerto. Charlie ridiculizó mi fe y cultura, y él murió defendiendo su derecho a hacerlo. #JesuisAhmed»

El autor de aquella dura reflexión era un viejo conocido, Dyab Abou Jahjah, exdirigente de la Liga Árabe Europea (AEL) y comparado por la prensa con Malcom X por su enérgica defensa de los inmigrantes a través del Movimiento X.

Puede compartirse o no su reflexión. Yo lo hice y esa frase fue la portada de mi perfil de Facebook hasta el Ramadán de 2015, pero lo que no puede cuestionarse es que reflejaba un hecho empírico: Ahmed Merabet era un verdadero musulmán; los

hermanos Kouachi no. Y Ahmed murió en acto de servicio, intentando proteger a los civiles del ataque terrorista.

La conexión española

Por una macabra paradoja del destino, la pequeña calle Rue Albert Willemetz desemboca en una plaza llamada Square de la Paix, la plaza de la Paz. Allí, justo en la esquina, se encuentra el Hiper Cacher donde se resguardó Amedy Coulibaly tras disparar contra la agente Clarissa Jean-Philippe y el funcionario municipal. Allí asesinó a otras cuatro personas e hirió de gravedad a cuatro más antes de ser abatido ante las cámaras de televisión por los agentes de Operaciones Especiales.

Antes del fatal desenlace Coulibaly habló por teléfono con la cadena BMF TV declarándose fiel al Estado Islámico, y confesando haberse coordinado con los hermanos Kouachi para ejecutar los ataques. Tras su muerte, el vídeo en el que Coulibaly se responsabilizaba de los ataques se hizo público: en él posa con un Kalashnikov y con la bandera del ISIS. Lo había grabado en un piso de Gentilly (Val-de-Marne) alquilado unos días como escondite para sus armas. La policía dio con él el mismo día de la difusión del vídeo, y allí descubrieron documentos de identidad a nombre de Coulibaly, cuatro pistolas Tokarev, un revólver, munición, teléfonos, bombas lacrimógenas, detonadores, un chaleco táctico, dinero y banderas del Estado Islámico.

Para entonces Hayat Boumeddiene, su esposade origen argelino, ya estaba muy lejos. Entre el 31 de diciembre 2014 y el 2 de enero 2015, ambos habían estado en Madrid. Luego, el día 2, ella había tomado un vuelo en el Aeropuerto de Barajas rumbo a Estambul, y habría pasado la frontera entre Turquía y Siria el 8 de enero. Según los servicios de Inteligencia franceses, una vez allí Boumeddiene se habría unido al Estado Islámico: apareció con traje de campaña y un subfusil de asalto en las manos, con un grupo de yihadistas, en un vídeo divulgado por el ISIS un mes más tarde.[116]

Y con esa conexión española, el 15 de enero 2015, el juez Eloy Velasco decidió abrir una investigación sobre la estancia en Madrid de Amedy Coulibaly y su esposa. Un juez con quien me he cruzado ya en alguna ocasión.

Cuando el 25 de mayo de 2010 *El Palestino* llegó a las librerías, nadie sabía dónde había estado metido durante los seis años que duró la infiltración, y las imágenes de Arturo Cubillas que grabé con cámara oculta en el Ministerio de Agricultura y Tierras donde trabaja como funcionario del Gobierno Bolivariano de Venezuela cogió a los servicios de información por sorpresa. Antes de esa grabación, no existían imágenes actuales de Cubillas —ni tampoco han vuelto a conseguirse hasta la fecha, a pesar de los reiterados intentos de muchos compañeros—, y siempre se utilizaban las mismas fotos antiguas para ilustrar las noticias sobre el supuesto jefe de ETA en Venezuela. Ahora se usan las mías, aunque ningún compañero se moleste en citar la fuente.

Los servicios policiales y/o de Inteligencia acogieron con entusiasmo aquellas

nuevas informaciones, obtenidas sobre el terreno, sobre la infraestructura de ETA en América Latina, y su relación con otros grupos armados, como las FARC o el ELN y me llegaron a pedir que echase un vistazo a un álbum con fotos de otros etarras que tenían localizados en Venezuela para ver si me había encontrado con alguno de ellos durante mis meses de estancia en la República Bolivariana. Y así era.

Seis meses más tarde, en octubre de 2010, el juez Velasco pedía la extradición de Arturo Cubillas.[117] Ahora, años después, mi trabajo y el del juez coincidían de nuevo.

Nuestros servicios de información controlan la red, y vigilan atentamente las redes sociales. Por eso, cuando se produjo el atentado contra *Charlie Hebdo* y se descubrió la conexión española de Coulibaly la mecánica judicial y policial se puso en marcha.

Como suele ocurrir en estos casos, las presiones de los políticos a los mandos policiales se tradujeron en presiones de dichos mandos a sus funcionarios. Como resultado se redactaron dos informes confidenciales basados en las tendencias de Twitter tras los atentados. El objeto de aquella ciberinvestigación confidencial era averiguar si podía detectarse en las redes sociales alguna amenaza hacia España tras la visita de Coulibaly y su esposa a Madrid unos días antes.

El primer informe (5 páginas), más precipitado, dibuja una imagen general de lo que había ocurrido en internet, en relación a España, tras el ataque a *Charlie Hebdo.* El segundo, más extenso (32 páginas), profundiza en cómo, cuándo y quién dijo qué.

Según dicho informe, las etiquetas #CharlieHebdo y #JeSuisCharlie «se convirtieron en dos de las más mencionadas en la historia de Twitter. #Jesuischarlie generó en sus primeras 36 horas un total de 997.470 comentarios a nivel mundial. Los momentos de más difusión en España fueron en torno a las 00:00 del día 7 de enero, con 4.640 tuits aproximadamente. En porcentajes, Francia fue el país con más comentarios con un 34,17 %, España tuvo un 3,73 % en el total de mensajes».

Los agentes localizaron varios tuits de apoyo a los terroristas escritos en castellano, pero no desde España, sino desde Chile —«No les gustó mofarse del profeta Mahoma? Ahora asuman»—, desde Argentina —«Me van a tener que perdonar, pero los de Francia se merecían lo que les pasó… Que se jodan»— o desde Venezuela —«Francia apoyó al Estado Islámico para asesinar a Gadafi, que era su contención, ahora rescaten lo que generaron»—. A partir de ahí sigue una investigación profunda y fascinante, realizada por los agentes españoles, rastreando las etiquetas escritas en árabe que celebraban el atentado.

La primera identificada en Twitter fue:

الدولة_الإسلامية_تكبر_وسط_باريس

«El Estado Islámico se hace fuerte en el centro de París»

Ese mensaje apareció, según el informe confidencial, a las 13:34 del 7 de enero.

Solo dos horas después del asalto a la revista. Inmediatamente los funcionarios españoles investigaron ese perfil y su presencia en las redes, así que no seré yo quien revele su identidad, porque no hace falta ser muy inteligente para intuir que ese malnacido puede ser una pista útil para investigaciones posteriores.

Otras etiquetas analizadas al detalle en el informe fueron:

#ثأرنا_لرسول_الله
«Nuestra venganza del profeta»

#غزوة_شارلي_إبدو
«La batalla de Charlie Hebdo»

#الجبهة_الإعلامية_لنصرة_الدولة_الإسلامية
«Frente de la prensa para apoyar al ISIS»

Lo interesante, para nosotros los ciudadanos, son las conclusiones del informe:

> Independientemente de la amenaza que existe en España por el significado que tiene para el islam integrista, con los datos analizados en este informe no se puede afirmar que esta haya crecido en intensidad tras los atentados terroristas de Francia.
>
> También se han actualizado los análisis de todos los perfiles de corte yihadista a los que se tiene en seguimiento en esta Unidad, muchos de ellos judicializados, observando cómo los más radicales apoyan lo acontecido en Francia y los menos justifican la acción, si bien no han aludido a España ni a ningún interés español en ninguno de sus mensajes posteriores al atentado.
>
> Por lo tanto, no se ha encontrado amenaza real o fiable tras estos hechos que pudieran representar un peligro añadido al nivel de amenaza que había antes de estos atentados.

Los asesinos de París no habían conseguido nada. Mataron y murieron por ser *trending topic* durante unas horas en Twitter. Y nada más. Todo el dolor, la angustia y el miedo que sembraron en París quedaron sepultados a las pocas horas por la marcha de la actualidad. Y otros *hashtag* les adelantaron como tendencia inmediatamente. En España al día siguiente, ni siquiera eran tendencia en Twitter. Los *hashtag* #htcmaniacos, #N1CanalFiesta2, #EstamosContigoPaula o #EliminaUnPiropo eran los temas más comentados por los tuiteros. Ni rastro de los asesinos en los diez primeros puestos de Twitter.

Ni siquiera consiguieron terminar con *Charlie Hebdo.* Volvió a publicarse, y de nuevo con el profeta Muhammed (saas) en la portada. Sosteniendo un cartel con el mensaje «Je Suis Charlie», bajo el titular: «Todo está perdonado». Vendió 7 millones de ejemplares en seis idiomas. Antes del ataque no pasaban de los 60.000. Los terroristas no habían conseguido nada. Porque con la violencia jamás se consigue nada.

Antes de abandonar París intenté contactar con Anna Erelle, la periodista francesa que en la primavera de 2014 contactó a través de Facebook con Abu Bilel, un mando del Ejército Islámico y durante meses le sacó una información valiosísima sobre el ISIS haciéndose pasar por una conversa dispuesta a casarse con él y viajar a Siria,

como otras muchas jóvenes europeas. Y chateando por Facebook y Skype Erelle consiguió introducirse como nadie en la mentalidad del ISIS a través de la red.

Pero ahora Anna es testigo protegido del Ministerio del Interior francés, y a pesar de mis ruegos a su editorial, no me permitieron entrevistarla. Creo que puedo comprender la fase en la que se encuentra mi colega. Tras la publicación de su interesantísimo libro[118] llegaron las amenazas, y el miedo. Un miedo que puede llegar a paralizarte. Las noches largas, pobladas de pesadillas. Ojalá consiga superarlo.

Así que en vez de reunirme con ella como pretendía, visité el Museo del Louvre. Tenía un interés especial por ver si encontraba dos cuadros sobre el mismo suceso negro de la historia de París. Louis me había asegurado que estaban allí, pero a Louis no le interesa demasiado el arte analógico y esta vez me guio mal…

En la noche de San Bartolomé de 1572, Catalina de Medici y su hijo Carlos IX ordenaron a los parisinos católicos que marcasen sus casas. Después lanzaron a sus fieras a una orgía de sangre histórica. Miles de protestantes fueron degollados esa noche, en el nombre de Jesucristo y de la única religión verdadera: el catolicismo. Aquella masacre la inmortalizaron François Dubois primero, y Édouard Debat-Ponsan después. Ambos cuadros reflejan el dramatismo de aquella noche siniestra en que las calles de París se regaron con la sangre de otros inocentes, en el nombre de otro Dios.

La masacre de San Bartolomé y la de *Charlie Hebdo* son igualmente blasfemas.

ENERO DE 2015
EL ARREPENTIMIENTO DE MARKOSS88

«Todo cruzamiento de razas provoca tarde o temprano la decadencia del producto híbrido, mientras el elemento superior del cruzamiento sobreviva en puridad racial. Cuando se ha bastardeado hasta el último vestigio de la unidad racial superior, es cuando desaparece para el producto híbrido el peligro de extinción.»

Adolf Hitler, *Mein Kampf,* parte segunda, cap. 2

El 22 de enero de 2015, Markos subía una nueva entrada a su blog. La tituló «Eso pensaba…», y en ella, sin citar mi nombre, reflexiona sobre la circunstancia que cruzó nuestros destinos.

Pensaba que jamás me iba a arrepentir de haber intentado matar a una persona por el hecho que fuera, pero desde hace días e incluso meses, me arrepiento de haberlo intentado con la persona que hoy en día, después de confesarle toda la verdad, me quiere ayudar a más no poder y que sin él saberlo, me está ayudando ya.

Sé reconocer cuándo me equivoco y esa fue una de las veces que me equivoqué. Todos creemos lo que nos dicen antes de intentar comprobarlo, lo siento, pero todos somos humanos, debí hacer lo correcto y haber investigado desde mi punto de vista, como siempre hago, pero esa vez se me anuló la mente y comencé a creer todo lo que me decían, caí en lo que odio, caí en las mentiras en las manipulaciones, a día de hoy, si le hubiera llegado a matar jamás habría sabido la verdad, habría caído en la mentira en la que caemos todos, cosa que no debemos hacer. Invito a leer, a comprobar, si lo que se dice de cierta persona es verdad y entonces podremos decidir por nosotros mismos. Si yo he abierto los ojos, vosotros no sois menos, al revés, yo sé que vosotros no caéis en la misma piedra que yo, juzga por ti mismo y no por lo que digan los demás, conoce la verdad. Sinceramente no sé si un día esa persona me perdonará por hacer lo mismo que el resto, pero espero que al menos comprenda mi error.

En el texto se presentaba como alguien que reconocía su error, y lo importante es que lo hacía ante sus lectores, los cachorros, jóvenes aspirantes al NS dispuestos a absorber las enseñanzas de alguien con tanto recorrido como MarkoSS88. Lo consideré un triunfo. Tal vez por ahora no había conseguido que Markos renunciase totalmente a la violencia, pero aquel *mea culpa* entonado ante los cachorros era esperanzador. Al menos aquellos adolescentes, que devoraban los textos de Markos como si fuesen revelados por un discípulo directo del Führer, recibirían ese día un mensaje diferente.

Volvía a equivocarme. El supuesto arrepentimiento de Markos encerraba otras intenciones. Un mensaje de Álex, el policía nacional, me advirtió del peligro.

—Tenemos que vernos. Markos te está engañando. Hemos geolocalizado

sus tuits. No está en Mallorca. Ten mucho cuidado…

Capítulo 13
Perfiles falsos para ligar en la red

«¡Qué sabios son aquellos que solo son tontos en el amor!»

James Cook

«La traición la emplean únicamente aquellos que no han llegado a comprender el gran tesoro que se posee siendo dueño de una conciencia honrada y pura.»

Vicente Espinel

La estrategia del miedo

Vivimos con miedo. Nos lo inculcan desde que nacemos. Y a lo largo de toda nuestra vida, por si se nos olvida, una, y otra, y otra vez más, nos obsequian con nuevos peligros, alertándonos de terribles amenazas y convenciéndonos de nuestra infinita vulnerabilidad como individuos. Solo en la masa, debidamente tutelada por los gobernantes, podremos sentirnos a salvo.

Yo sé algo sobre el miedo. Nos conocemos desde hace muchos años. No nos gustamos, pero nos respetamos. Hemos hecho muchas cosas juntos. Como ese compañero que te han asignado en la empresa, con el que no tienes nada en común, pero con el que funcionas bien en equipo. Ambos sois profesionales y juntos la rentabilidad es mayor. Quizá por eso el jefe os ha emparejado. Sé que el miedo —como la ambición, la humildad, o la rabia— en el fondo no es mala gente, si lo tratas en su justa medida y no se impone y te paraliza. Pero solo en las distancias cortas, es decir, en tu trato íntimo y personal con cada una de esas emociones. No cuando te los imponen desde arriba. Y el miedo, sobre todo desde el 11-S, nos lo imponen. Otra vez.

Una ingenua pero bienintencionada sentencia, atribuida a Cicerón, afirma que «el pueblo que no conoce su historia está condenado a repetirla». Yo no tengo tan claro que esté en manos del pueblo escribir su historia. Porque la historia, y perdón por la osadía, se repite una y otra vez, la conozcamos o no. Es cíclica.

Al consultar las hemerotecas para documentar cualquiera de mis libros, al visionar los viejos informativos, al repasar las crónicas periodísticas de los años cincuenta, sesenta o setenta, no puedo evitar sentir una cierta familiaridad con aquellos titulares.

En aquella época era la amenaza comunista la que arrasaría de forma inminente la sociedad occidental. La caza de brujas del macarthismo norteamericano de los cincuenta con sus juicios públicos, detenciones e interrogatorios, o su propaganda mediática contra los malditos comunistas asentados en suelo americano, intentando imponer a la gente de bien sus creencias e ideas fanáticas, me parece una parodia de la islamofobia actual.

El terror que inspiraba el nombre de Carlos el Chacal en un titular de prensa en los años setenta o primeros de los ochenta —avistado simultáneamente en una punta del mundo y la opuesta, preparando un nuevo atentado contra las vidas de inocentes ciudadanos o de tal o cual presidente del Gobierno— me resulta una copia del rastro que durante años dejó en las hemerotecas la amenaza del jeque Osama Ben Laden o ahora del «califa» Abu Bakr al-Baghdadi.

EL DIARIO DE CARACAS

Viernes 11 de diciembre de 1981

Washington urgió a los norteamericanos para que salgan de Libia

En USA temen que "Carlos" trate de matar a Reagan

Los servicios de inmigración advirtieron a la policía fronteriza que un grupo de 15 pistoleros busca entrar a Estados Unidos para matar al presidente, por orden de Kadafi. En México, país por donde deberían entrar los pistoleros se burlaron de la información.

San Isidro. Los servicios estadounidenses de inmigración (INS) advirtieron a la policía encargada de la vigilancia fronteriza sobre la posibilidad de que "un comando de seis asesinos liderados por (el terrorista) "Carlos" penetre en territorio norteamericano.

Los servicios suministraron una descripción de Carlos y una fotografía suya realizada por la policía canadiense. Se trata del venezolano Carlos Ilich Ramírez que habla perfectamente castellano, árabe y ruso y "es extremadamente hábil en cambiar de identidad y de apariencia".

Asimismo, la información del INS identifica a tres de los miembros del "equipo asesino" como ciudadanos sirios. Uno de ellos sería un oficial del Ejército sirio, mientras que otros tres serían libios.

El objetivo del comando, precisan los cartuchos colocados en el puesto fronterizo de San Isidro, California, consiste "en matar al presidente Reagan y a altos funcionarios".

El INS solicitó a los servicios fronterizos que vigilen también la posible llegada de un segundo equipo de tres iraníes, un libanés, un palestino y un estrasalemán, cuyas identidades y algunos rasgos físicos son conocidos por la policía.

Reacción contra Libia

El gobierno de Reagan, tomando la primera de una posible serie de medidas contra Libia, urgió ayer a los ciudadanos norteamericanos a que salgan de ese país y condenó a Estados Unidos y limitó los viajes de los norteamericanos a esa nación de Africa del Norte.

La medida, tomada a raíz de lo que en la opinión del Departamento de Estado es "un peligro inminente", fue anunciada por William Clark, a cargo del departamento en ausencia de Alexander Haig.

Agregó que Reagan debía actuar a causa de los esfuerzos de Kadafi para "minar los intereses de Estados Unidos y sus amigos" y por su "apoyo al terrorismo internacional".

El anuncio de que "el clima de seguridad ha empeorado" para los ciudadanos norteamericanos en Libia se produjo después de [illegible] entre el gobierno de Reagan y el régimen del coronel Moammar Kadafy, acusado por Estados Unidos de ser el principal promotor del terrorismo internacional.

También se dio a conocer una lista de 14 terroristas, que estarían actualmente en México, supuestamente enviados por Libia para asesinar a Reagan y a otros altos funcionarios norteamericanos.

"Estados Unidos reconoce la gravedad de la situación, pero cree que estas acciones de Libia nos obligan a tomar medidas. En verdad, sería una irresponsabilidad para el Gobierno de Estados Unidos no hacer algo", dijo [illegible]. Añadió que se había puesto en contacto con algunos ejecutivos de empresas norteamericanas con personal en Libia, para discutir los "conocidos esfuerzos" de Kadafi por minar los intereses estadounidenses y apoyar el terrorismo.

La mayoría de los norteamericanos en Libia son empleados de seis empresas petroleras. Una de ellas, Exxon, está preparándose para salir de Libia, pero Amerada Hess, Occidental Petroleum, Mobil, Conoco y Marathon todavía están operando allí.

Marathon indicó ayer que está retirando a sus empleados y a sus familiares en respuesta a la exhortación gubernamental estadounidense.

En Trípoli, la agencia oficial libia Jana calificó hoy de "pretensiones sin ningún fundamento" las declaraciones del presidente Ronald Reagan, según las cuales "un peligro inminente amenaza la seguridad de los norteamericanos que se encuentran viajen a Libia".

Como primera reacción ante la decisión de Reagan de repatriar a los norteamericanos que se encuentran en ese país, la agencia libia afirmó que "los norteamericanos que trabajan en Libia viven en paz y seguridad".

En México dudan

Un diplomático estadounidense en México expresó su [illegible] sobre [illegible] libio, preparado para matar a funcionarios de su país, estaría oculto en México.

"No tengo razón para creerlo", dijo un diplomático cuando se le pidió que comentara sobre el informe".

José Rodríguez, portavoz de la oficina mexicana de la agencia internacional policíaca Interpol, se burló del informe y dijo que sonaba "como un aviso para colegiales".

Funcionarios de la división federal de seguridad mexicana dijeron que nadie que llevase un pasaporte del Medio Oriente ha entrado en México en las últimas 48 horas. (AFP-UPI)

Reagan, el hombre más poderoso de Occidente, siente la amenaza del terrorista "Carlos, el chacal".

Siguen estallando bombas en el Líbano

Tras once años, habrá una nueva cumbre internacional

Y no apostaría a que el terror que nos inspiró el 11-S, la consternación, angustia y miedo que generó en millones de hogares de todo el mundo, sean mayores que la catarsis apocalíptica, la angustiosa desesperación y el pavor a una inminente Tercera Guerra Mundial que impuso en todo el planeta la crisis de los misiles de Cuba en octubre de 1962. Yo ni había nacido pero mis padres y abuelos sí. Y no están seguros de cuándo sintieron más miedo.

Son nuestras víctimas las que nos duelen. Y sin entrar en un absurdo ranking de muertos, lo cierto es que el terrorismo no lo inventó el ISIS. Ni Al Qaeda. Ni siquiera Carlos el Chacal. El terrorismo forma parte de nuestra historia. Porque la letra con miedo entra.

Vivimos unos tiempos convulsos, en los que la amenaza yihadista nos obliga a levantarnos una hora antes para salir de viaje, a desprendernos de nuestros botes de desodorante o perfume antes de subir al avión, o a soportar colas, cacheos y situaciones denigrantes. Nos fuerza a convivir con dispositivos policiales, o militares, armados hasta los dientes en nuestras calles. Nos impone restricciones en nuestros derechos y libertades. Lo aceptamos todo porque tememos que la amenaza yihadista

pueda alcanzarlos «así sea, en nuestras casas».

Pero hubo un tiempo en que nuestros padres y abuelos aceptaron las mismas restricciones por un miedo similar, o mayor, a otras amenazas inminentes. Antes del 11-S, el 11-M o el 7-J, otros terroristas escogieron aviones, trenes o autobuses para lanzar su mensaje de terror.

¿Quién se acuerda hoy del Boeing 747 que sesgó 329 vidas en Irlanda, el 23 de junio de 1985? ¿O la masacre de Lockerbie, el 21 de diciembre de 1988, con 270 muertos de veintiuna nacionalidades distintas? ¿Quién recuerda hoy a los casi 300 muertos de los cuarteles de Beirut en 1983? ¿O los 168 muertos y más de 500 tullidos, mutilados y heridos de Oklahoma City? ¿O los más de 100 muertos y 500 heridos en la AMIA y la embajada de Israel en Buenos Aires?

El miedo caduca. Por eso debe ser renovado.

Durante la Transición española, nuestros padres aprendieron a temer la amenaza filofascista de los nostálgicos del franquismo, que segaron vidas, violaron y torturaron, y sembraron el terror, en el nombre de unas ideas antagónicas al yihadismo… pero los extremos se tocan. Hoy nadie teme a organizaciones como el Batallón Vasco Español, la Alianza Apostólica Anticomunista (Triple A), los Grupos Armados Españoles, los Comandos Antimarxistas o los Guerrilleros de Cristo Rey. [119]

Sin embargo, nuestro padres y abuelos si les temieron. En aquellos años setenta y ochenta, otras víctimas abrían los informativos, generaban manifestaciones y ocupaban las tertulias. Pero hoy nadie recuerda a José Luis Alcazo, Ana Teresa Barrueta o Yolanda González. Nadie rememora la bomba del bar Aldama, o la que arrasó la redacción de *El Papus*, o la Matanza de Atocha, que llenaron de miedo la Transición. Como antes y después de ella fueron los atentados de ETA, GRAPO, Terra Lliure, MPAIAC, Comandos Autónomos Anticapitalistas, FRAP, EGPGC, GAVF**,** Andecha Obrera, DRIL, etcétera. Hoy tenemos otros miedos.

Tengo razones para creer que alguno de aquellos atentados fueron una falsa bandera, aunque no puedo demostrarlo (por ahora). Pero ¿y los actuales?

Durante los seis años que duró la investigación de *El Palestino*, aprendí que el terrorismo ha sido, entre otras muchas cosas, un arma política de alto calibre. Perdí mucho tiempo y dinero intentando contrastar informaciones que se publicaban en los diarios, se exponían en congresos y cursos especializados, y aparecían reseñadas en la Wikipedia o en Google. Mentiras, mentiras y mentiras, estratégicamente insertadas entre otras muchas verdades. Que es como resultan más eficientes.

Por eso suelo desconfiar del alarmismo y de los titulares sensacionalistas cuando se habla de grandes amenazas. Y mi experiencia personal no ha hecho más que reafirmarme en esa conclusión. La última vez, el 28 de enero de 2015.

Hackeando las mentiras de Roi en FITUR

Blanca fue la primera víctima de Roi a la que entrevisté. Y fue ella quien me puso al corriente de que otras víctimas se habían unido, coordinadas por una tal Gloria, para compilar toda la información posible sobre el estafador emocional en serie. Un modo, suponían, de alertar a otras mujeres para que no pasasen por lo que ellas habían pasado.

—Toni, soy Blanca —me dijo mi amiga en cuanto atendí su llamada al móvil—. Te confirmo que Gloria estará en FITUR. Lo inauguran el próximo 28 de enero, y ella solo va a estar ese día, pero igual hay mucho follón porque van los Reyes y un montón de políticos.

—No te preocupes. Si solo está ese día, merece la pena. Preparo la maleta y salgo mañana mismo para Madrid. —Acordamos reunirnos el día 28 en la puerta de acceso al pabellón principal del IFEMA.

La Feria Internacional de Turismo, que alcanzaba su 35 edición, se había convertido ya en una plataforma promocional extraordinaria. Y además del rey Felipe VI y la reina Letizia, acudieron a la inauguración los presidentes autonómicos Paulino Rivero (Canarias), Susana Díaz (Andalucía), Alberto Núñez Feijóo (Galicia) o María Dolores de Cospedal (Castilla-La Mancha), así como numerosos alcaldes, embajadores y políticos relevantes. El coto de caza que soñaría cualquier terrorista. El dispositivo policial era extraordinario.

Tardé un rato en localizar a Blanca entre aquella legión de policías, guardias civiles y escoltas. Hola. Hola. Dos besos, muac, muac. ¿Qué tal el viaje?… Entonces Blanca me explicó que había quedado con Gloria en el interior. Ella ya se había acreditado para acceder al pabellón, pero yo no tenía la menor intención de hacerlo.

—Vaya por Dios, me he olvidado la documentación en el hotel —mentí—. He tenido que salir con prisa y olvidé recogerla en recepción.

—No te preocupes. Una amiga mía trabaja aquí, voy a darle un telefonazo y ella nos pasa.

Accedimos al vestíbulo del pabellón donde se agolpaba una legión de policías y periodistas, y su amiga nos hizo una señal desde el otro lado de uno de los tornos, rodeado por detectores de metales. Llevaba colgado del cuello una credencial del IFEMA que al parecer la autorizaba a moverse por todo el pabellón libremente… Pretendía que, aunque sin registrarme, cruzase por aquel detector, pero si lo hacía, aquello se pondría a pitar como loco.

—Ostras, Blanca, me olvidé de comentártelo. No puedo pasar por ahí… Un marcapasos —improvisé—. No me gusta hablar de eso…

Blanca me miró con una mezcla de sorpresa, curiosidad y escepticismo. No se esperaba algo así. Yo tampoco.

—¿Tu amiga no podría colarnos por otro lado? —insistí.

Dudó unos instantes, aunque supongo que al final concluyó que no había de qué

preocuparse, se acercó a su amiga, cuchichearon unos segundos mientras me dirigían miradas de reojo, y por fin mi cara de tipo inofensivo o las dotes de persuasión de Blanca convencieron a la trabajadora del IFEMA, que me hizo una seña para que me desplazase hacia la derecha del pabellón.

Blanca y yo entramos en el recinto a pocos metros de los reyes de España y aquella peregrinación de políticos y presidentes, sin acreditación alguna, y sin que nadie se hubiese cerciorado de que no portábamos nada peligroso. Supongo que cualquier terrorista, con muchos más recursos y experiencia que yo, podría haber atentado allí aquella mañana. Y me disculpo por adelantado, porque no es mi intención hacer una crítica a los responsables de seguridad del evento, pero así fue como ocurrió.

Gloria nos esperaba en una de las cafeterías.

Lo primero que me impresionó de ella fue su enorme sonrisa, su transparencia, su cercanía y su irresistible cordialidad. Costaba creer que alguien quisiese hacer daño a aquella mujer.

—Glory, este es Toni. Toni, Glory. —Blanca hizo las presentaciones, y a partir de ese instante permaneció casi todo el tiempo en silencio. Gloria tenía mucho que contar, y nuestra común amiga no quería interrumpirla.

—¿Os importa? Es mejor que tomar notas —le pregunté a las dos mientras les mostraba la grabadora.

—No, en absoluto. Además, la historia es larga y compleja —respondió Gloria sonriendo con un punto de amargura.

—¿Tú también conociste a Roi en la web de Adoptauntio?

—No. A mí me captó en FetLife. Es que yo soy sumisa… ¿Conoces FetLife?

No tendría que ser así, no a estas alturas, pero me sorprendió la naturalidad con la que Gloria se definió como sumisa a los pocos segundos de conocernos. Y me avergüenza aquella primera sensación de sorpresa, y cierta incomodidad, porque Gloria no estaba desnudando su preferencia sexual, era algo mucho más profundo: era su filosofía de vida. Una entrega total y absoluta, de la que Roi se aprovechó. Y ella sabía que para que yo pudiese comprender el trauma que infligió en su vida, debía empezar por conocer su condición.

No, yo no conocía FetLife. A pesar de que el BSDM[120] siempre me despertó una profunda curiosidad, sobre todo desde que mi amiga Valérie Tasso se introdujo varios años en ese mundo para documentar su libro *El otro lado del sexo* (Plaza y Janés, 2006), y yo viví de cerca sus primeros contactos con Other World Kingdom en la República Checa. Un pequeño «país», de 3 hectáreas de extensión, creado en 1996 en torno a una antigua fortaleza reconvertida en palacio del BDSM, con moneda, Gobierno, pasaporte y Policía propia. Y donde, como dice el primer artículo de su código: «La mujer es un ser superior a todas las criaturas masculinas en el OWK, y tales criaturas actuarán en consecuencia».[121]

En cuanto a FetLife, se trataba, como averigüé después, de una red social creada

en 2008 por el ingeniero de software canadiense John Baku, frustrado por no encontrar mujeres que compartiesen sus preferencias sexuales. Y aunque FetLife nació como un punto de encuentro entre los practicantes del BDSM, Gloria puso mucho empeño en aclararme que estaba abierto a todas las opciones sexuales, porque no solo era un portal para buscar sexo, sino que el mayor interés de la web estaba en sus foros sobre filosofía.

Con más de cuatro millones de usuarios en todo el mundo, en FetLife convivían dominants y dommes, masters y mistress, slaves, kajiras y kajirus, pets, daddys, brats, primals, fetischists, babygirls, switchs… y todo el sorprendente abanico de roles imaginables en las fantasías del BDSM. Pero también había depredadores. Depredadores emocionales. Que en su dedicada patrulla por las redes sociales habían incluido FetLife en su coto de caza. Gloria tuvo la mala suerte de encontrarse con uno.

—Yo soy megafriki de la secularización del pensamiento filosófico. Y FetLife es una comunidad en la que sobre todo nos une la secularidad en el sexo. Hay dóminas, sumisas, kinkster… pero también hay asexuales. Sería un error que pensases que solo se trata de sexo. FetLife es como un embudo. Arriba están los que simplemente entran por el sexo, pero a medida que vas bajando escalones, vas encontrando gente superinteresante. De sexo es de lo que menos se habla. Mira, esta soy yo.

Gloria había abierto el navegador de su teléfono móvil y me mostró su perfil en la red social. En las fotos aparecía con el atrezo característico de la cultura BDSM. Cuero, correas, tacones, cadenas…

—¿Ves? Estas son mis fotos, y aquí están los foros de debate. Yo pertenezco a uno de humor satírico, este de aquí, muy transgresor, aunque hablamos mucho de filosofía. A veces ponemos dilemas, para poner a prueba nuestro ingenio. Yo había dejado una respuesta a uno, y es cuando Roi me abrió un privado. Conmigo utilizó el nombre de Shrapnel 77. Yo al principio no le di ni los buenos días, pero este tío tiene una inteligencia emocional brutal. Yo no he visto a nadie escribir tan bien, con tanto gancho, con tanta coherencia. Me pidió que le agregase al Skype, y empezamos a hablar. A mí se me presentó con la identidad de un programador de videojuegos que trabajaba para EA Entertainment, que además era tatuador. Me contó que había nacido en Malmö, enSuecia, pero que ahora estaba en España porque un amigo suyo, Daniel, un cocinero gallego, le había pedido ayuda en un proyecto que había abierto en Pontevedra. Porque él también era cocinero. Todo era supercoherente. Lo tenía todo estudiado.

Gloria y Roi comenzaron a charlar por internet, como hacen millones de personas todas las noches. Él, un ejecutivo de origen sueco, tatuador, programador de videojuegos, pianista, aventurero… presentaba un perfil diferente al que había utilizado con Blanca, pero igual de blindado. Tenía todo un cargamento de «pruebas» para reforzar su identidad digital ante la nueva víctima. Todo un profesional.

—Al principio me mandaba fotos de sus diseños de tatus, piezas de música épica

de las que componían para los videojuegos, y unos textos y poemas maravillosos. Te envuelve en su mundo y te hace sentir especial. Y además, manipula muy bien tu instinto maternal, porque te cuenta una historia muy dramática: que sus padres habían muerto en un accidente de tráfico, que su hermana se había suicidado, que él había estado meses solo en un hospital por un accidente de moto. Todo muy dramático. Y él, ya sabes, era un poeta, un artista, un alma errante… Y las que somos del verbo *to be stupid* caemos… Hasta que un día me dice que me quiere conocer. Y el 21 de marzo se planta en Bilbao.

Gloria y Roi comenzaron una relación. Hasta ahí todo normal.

—En mi mundo todo era de color y gominolas, te lo juro. Roi consigue ilusionarte. Siempre está pendiente de ti, mandándote emails, mensajes… Aquella primera semana yo tenía un viaje a Chile, pero después él me invitó a pasar un fin de semana en Aranda de Duero, acuérdate de este detalle. Nos quedamos en el piso de un amigo, según él, y bueno… Debes saber que en nuestro mundo, cuando tú aceptas a un Dom, le entregas todos tus juguetes sexuales, y el collar, que es lo más sagrado para nosotros… Y yo se lo entregué todo. Y cuando ya estoy de vuelta en Bilbao, me llama y me cuenta que su amigo de Pontevedra le había sacado todo el dinero del banco. Que él estaba en Madrid, en un piso que le habían dejado en herencia sus padres, pero que no tenía dinero porque le habían robado también las tarjetas, y claro, tenía que volar a Suecia para hacer un duplicado porque su banco no trabajaba en España. De nuevo todo muy coherente. A ver, yo no soy muy lista, pero la historia sonaba rara. Lo que pasa es que él se adelanta a tus movimientos. Cuando me dio el nombre de su banco, lo busqué en Google y es verdad que solo tiene oficinas en Suecia. Todo cuadraba, al final todo cuadraba siempre. Incluso me mandó fotos de su piso en Madrid…

—Que eran de mi casa —apuntó Blanca para mi sorpresa.

—¿Cómo? ¿O sea, que mientras estaba viviendo contigo, a Gloria le decía que esa era la casa que le dejaron sus padres?

—Espera, mejor vamos por partes o te vas a liar —añadió Gloria—. El caso es que lo vi tan apurado que yo me bajé a Madrid para llevarle dinero en efectivo. Me dijo que en su casa no nos podíamos quedar, porque tenía un problema con la luz, así que alquilé un apartamento. Y como me dijo que tenía que terminar unas piezas para EA Entertainment, pero su piano, su portátil y todas sus cosas se habían quedado en Pontevedra, le dejé dinero, mi ordenador y preparé el traslado de sus cosas a Madrid. Yo quería hacerlo a través de una empresa conocida, pero me dijo que tenía un amigo transportista que se lo hacía más barato… Total, que también le di dinero para él.

Sin embargo, la mudanza nunca terminaba de completarse. Probablemente por culpa del piano, que es una pieza tan delicada que requiere una atención especial. Aun así, la relación de Gloria continuó. Tanto a través de internet, como con encuentros esporádicos en otras ciudades.

—Tienes que entender que Roi es… mágico. No sabes cómo, pero te envuelve de

tal manera que te atrapa. Su música, sus poemas, sus dibujos, porque también es calígrafo. No importa lo enrevesada que sea la historia que te cuente; siempre tiene a mano las pruebas para demostrarla. El caso es que a mí me había prohibido que volviese a entrar en FetLife, y yo confiaba ciegamente en él. Además, yo soy cero celosa. Y así estuvimos unos meses. Yo volví a bajar a Madrid, o nos veíamos a medio camino. Pero su piso de Madrid (o sea, el de Blanca), siempre tenía alguna avería y no podíamos ir. Recuerdo que también le arreglé cita con un médico amigo, para que le ayudase con el tema de los dientes —resulta que a Roi le faltan casi todos —, que al final era seborrea y no culpa de un accidente en moto…

Una de las características físicas de Roi es que le faltan casi todos los dientes, circunstancia que aprovechó para justificar con un dramático accidente.

—¿Cómo en moto? —interrumpió Blanca—. A mí me dijo que fue en coche.

—No, no, a mí me contó que padeció ocho meses de angustiosa soledad en un hospital por el accidente de moto.

—¡Qué hijo de puta! A mí me contó exactamente la misma historia, pero en coche.

Supongo que cuando las diferentes víctimas de un estafador en serie tienen la oportunidad de encontrarse para contrastar sus respectivas historias, se producen muchas escenas como esta. Pero en esta ocasión yo era testigo.

—Y un día me escribe una amiga de FetLife, y me dice que ella no quiere meterse en mi vida, pero que una dómina que también estaba en la red, Victoria, había subido un escrito al foro y a ella le sonaba a Roi. Yo no sé por qué, te lo juro, pero le escribí un email a Evasión, diciéndole simplemente que creía que teníamos un amigo en común, Roi… Me respondió al instante. Y solo me dijo que llevaba dos meses esperando ese email, que ese no era un tema para hablar por la red y que me esperaba el domingo siguiente en Aranda de Duero. Y me mandó una dirección.

De pronto un pequeño revuelo en la entrada de la cafetería de IFEMA llamó mi atención. Una secuencia de flashes fotográficos, como el resplandor de un AK-47 escupiendo una ráfaga del calibre 7,62, iluminó las cristaleras. Supusimos que sería alguna de las autoridades políticas, quizás los reyes de España, en el recorrido que estaban haciendo por FITUR seguidos de una legión de fotógrafos. Estaban a menos de 20 metros. Un terrorista suicida lo habría tenido fácil. Y hasta un tirador torpe también. Pero yo estaba allí por otra razón…

—Perdona, y supongo que acudes a esa dirección…

—Sí, claro… —De repente, por primera vez, la voz de Gloria se quiebra. Como si el mero recuerdo del día en que descubrió la verdad abriese viejas heridas en el corazón, y arrojase dentro un puñado de sal—. Yo… cuando estaba llegando reconocí el sitio. Era la casa donde había estado un fin de semana con Roi, y que supuestamente era de un amigo… No entendía nada… Me abrió Victoria, me invitó a entrar, y me preguntó qué relación tenía yo con Roi. Le respondí que era mi amo… y ella me dijo que Roi era su sumiso, que llevaban cinco meses de relación… Me llevó

a su dormitorio, abrió un arcón y… y allí estaban todos mis juguetes, que eso me da igual, pero el collar… el collar en nuestro mundo es sagrado… y lo estaba usando él con ella…

Blanca, que es muy inteligente, se percató, igual que yo, que los ojos de Gloria habían comenzado a humedecerse, y que le costaba seguir con el relato, y la interrumpió para darle unos segundos de respiro y permitir que se recompusiese.

—No te quedes en la forma, Toni. Aunque la historia de Gloria empezase en el contexto de una página web de BDSM, en mi caso fue en otra. Y lo importante de que Gloria y Victoria sean una sumisa y una dómina es que Roi es capaz de adaptarse a papeles totalmente antagónicos. Podría ser socialista o pepero, judío o palestino, merengue o culé. Puede convertirse en cualquier personaje en la red para atrapar a la víctima. Quédate con eso.

La red creó el problema, y también la solución

—Bueno… —Gloria se secó las lágrimas, se recompuso un poco y continuó su relato—. Victoria me dijo que conocía su identidad real, y ya con su nombre real buscamos y encontramos el blog de Xanfarín y el de Zor,[122] y entonces la historia empezó a cobrar sentido.

Xanfarín, un aventurero que sí vivió en Suecia, y Zor, autor de prosas tan profundas como seductoras, eran dos de las fuentes de inspiración de Roi, que había robado sus vidas para utilizarlas como propias en el ataque a sus víctimas. Ahora uno y otro habían puesto en marcha un altavoz para desenmascararle, y en sus blogs analizaban paso a paso las estrategias de Roi en la red. En el blog de Zor, por ejemplo, podemos encontrar copiados, casi literalmente, algunos de aquellos versos tan hermosos y profundos con los que Roi había seducido a Gloria… y a varias docenas de mujeres antes, durante y después de su relación. Duele a la vista, y al alma, que unas palabras tan hermosas hayan sido utilizadas como vector de ataque para crackear las defensas de una mujer e introducir un virus en su sistema emocional. Pero en este caso internet, que había dado a Roi las herramientas para perpetrar sus engaños, también ofreció la solución a sus víctimas.

—En la época del IRC, te hablo de los años noventa, Roi ya se dedicaba a contactar chicas en los chats, y plagiaba los escritos de Xanfarín y de Zor, como si fuesen suyos. Y claro, a ti te enviaba algo así, diciendo que lo había escrito solo para ti, y te hacía sentir la chica más especial del mundo…

El *modus operandi* de Roi no había cambiado mucho en años. Buscaba la materia prima en los blogs y páginas de otras personas, y robaba todo el material que podía serle útil para crearse una nueva vida, hecha a medida de la víctima seleccionada en la red.

—Imagínate lo que sentí cuando descubrí esto, Toni. Ni era sueco ni había estado en Suecia, ni tocaba el piano, ni escribía versos, ni nada. Era un estafador profesional. Joder, y encima era sumiso… Igual piensas que estoy loca, pero para nosotros es muy importante el respeto. Cuanto tú cedes el liderazgo, es lo único que pides, porque te entregas totalmente. Y cuando vi sus fotos como sumiso… No, no, no te puedo explicar, es la traición más grande, y encima con mi collar… Yo salí de Aranda que no sabía si estrellarme con el coche, o hacer algo con esta información, porque no podía saber cuántas chicas más habían sido estafadas.

—Por suerte, veo que escogiste la segunda opción.

—Sí, pero yo no tenía absolutamente ninguna referencia real de Roi, todo era inventado. Solo tenía un número de teléfono prepago y un correo de Gmail, nada más. Entonces me acordé de Daniel, su amigo cocinero. Localicé su número y le llamé. Y aluciné. A Daniel le había contactado en Badoo haciéndose pasar por gay. Se había metido en su casa, había vivido allí unos meses y después, coincidiendo con

su primer viaje a Bilbao, salió de casa de Daniel sin avisar y nunca más volvió. Daniel pensaba que estaba muerto, que lo habían asesinado, porque lo dio de baja en WhatsApp, borró la cuenta de Gmail que usaba con él, y nunca más dio señales de vida. Le había hecho lo mismo que a nosotras. Yo le decía: «Pero si yo soy la chica que ha pagado la mudanza». Y él me decía: «¿Qué mudanza?» «Del piano.» «¿Qué piano?» Pensé que me volvía loca. Pero cuando hablé con Xanfarín fue peor. Él le seguía la pista desde hacía catorce años, porque un día empezó a recibir emails en su blog de chicas diciéndole que por qué les había hecho eso, que por qué las había seducido y luego había desaparecido, y claro, el pobre alucinaba. Y empezó a hacer una lista de víctimas. Ya sé que te parecerá increíble…

Pero no, no me parecía increíble. A menor escala, lo que le había ocurrido a Xanfarín me había pasado a mí. Yo también había recibido varios correos de chicas que habían sido seducidas por falsos Antonio Salas que luego habían desaparecido, así que la historia me resultaba de lo más creíble. Además, Gloria no ganaba absolutamente nada desnudándose de aquella manera.

—Xanfarín me envió los emails de las últimas víctimas que le habían escrito, y a partir de ahí empecé a componer la historia. Claro, las pobres estaban destrozadas. Con cada una había usado una identidad distinta. Se había metido en sus casas, les había sacado dinero, ordenadores, cámaras… siempre se llevaba algo electrónico. El *modus operandi* es que contacta a una chica por internet, da igual la red, foro o páginas en las que esté. Te estudia y se monta una identidad en función de tus gustos y así se gana tu confianza, te seduce y se mete en tu vida o incluso en tu casa ya sea como amigo, futuro socio, pareja… Allí está un tiempo parasitándote, sacando todo lo que puede. No solo dinero y cosas físicas, roba toda tu vida y la utiliza para crear la siguiente identidad. A otras les mandaba mis informes, presupuestos, todos los documentos de mi empresa, como si fuesen suyos. Y en cuanto escoge a la siguiente víctima, desaparece. De la manera más cruel. O sea, se hace humo. Y tú te quedas superenamorada de un tío que de repente ha desaparecido y del que no tienes el menor rastro.

Gloria abrió su portátil y me señaló algunos nombres en el documento de Excel que ya había visto en casa de Blanca.

—Hay historias terribles. Esta chica intentó suicidarse. Mira, esta es Bea: le hizo abortar porque le dijo que tenía un cáncer terminal. Yo no me suicidé porque descubrí todo esto antes de que desapareciera… pero si no…

Gloria se queda un momento en silencio. Blanca la abraza. Yo empiezo a sentir un profundo odio hacia ese hijo de puta y me pregunto cuántos miserables parecidos estarán en estos mismos instantes rastreando internet en busca de nuevas víctimas.

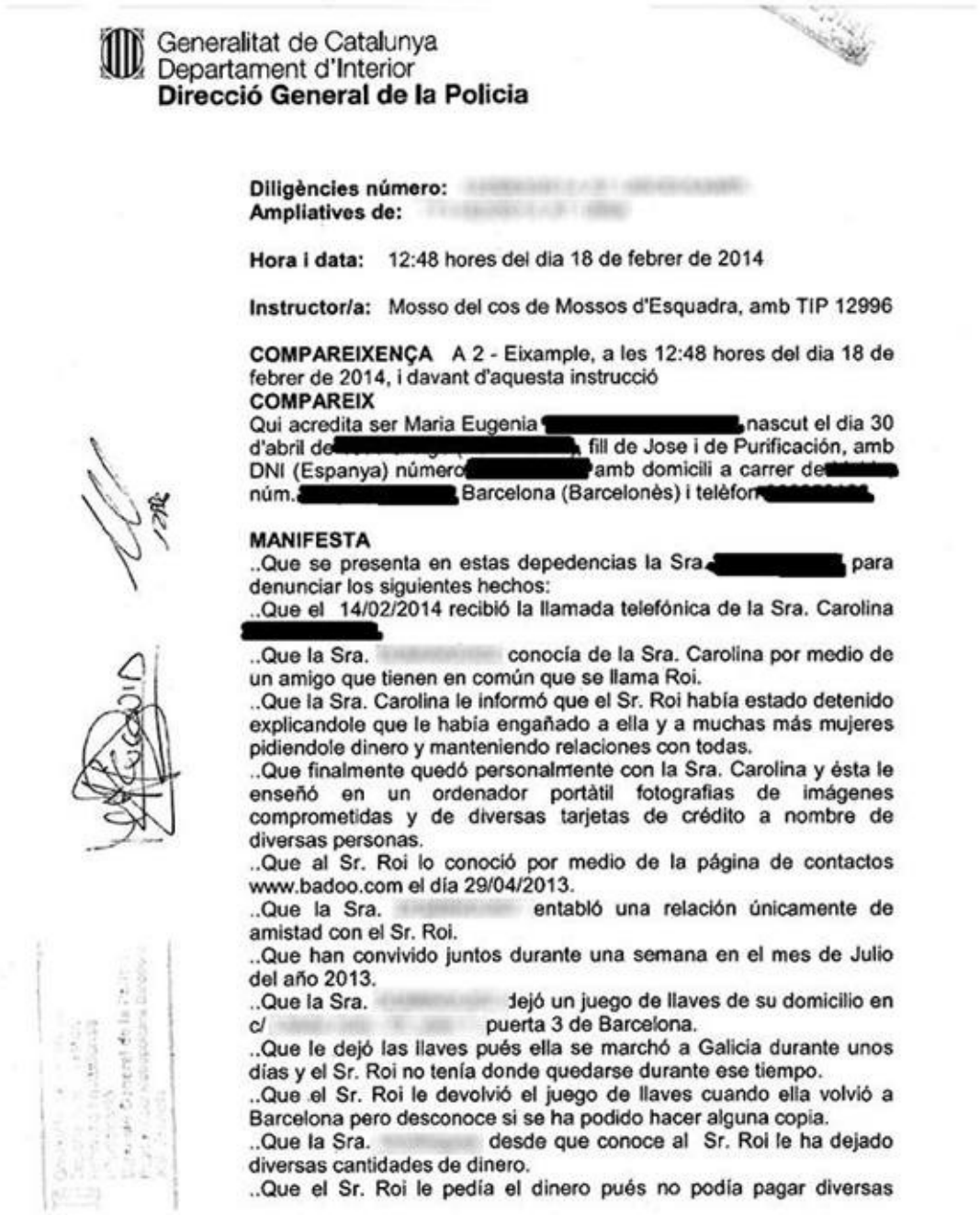
—Xanfarín me pasó el mail de Álex, y en cuanto recibió mi correo me dijo: «Sé por lo que estas pasando, es un horror, sé cómo te sientes, no estás sola…».

En Barcelona se había creado un grupo de víctimas: Álex, Mariona, Paula, Olga, Natalia, Geni, Nina —«Ella es una de las más perjudicadas, su psiquiatra todavía no

le ha permitido unirse al grupo»—. Todas del 2013. Una de ellas dio con Xanfarín y gracias a la información que ya tenía, al final se juntaron varias víctimas de Barcelona. En ese momento él vivía en casa de Nina, aunque estaba al mismo tiempo con las demás. Entonces se pusieron de acuerdo entre ellas, lo denunciaron a los Mossos d'Escuadra, porque se había llevado el ordenador de una de ellas, y le prepararon una encerrona.

Gloria abre uno de los documentos de su ordenador y me muestra varias denuncias. Entre ellas la presentada ante los Mossos que motivó la primera detención de Roi.

—Cuando estaba en Marbella con esta —añade Gloria mientras señala a una de las víctimas en su listado—, Alexandra, ahí vendía las cosas que se llevaba en Cash Converters. Su caso es de hace dieciséis años, de 1998. Ahora los vende en páginas web de segunda mano. El día de San Valentín de 2013, que había quedado con tres, le esperaron en casa de una de ellas y le detuvieron. Pero nada, a las setenta y dos horas estaba en la calle. Entonces hablé con Aaron, un amigo mío que colabora con las Fuerzas y Cuerpos de Seguridad del Estado, y decidimos descubrirlo todo. Intentamos pillarle la geolocalización del móvil, pero el tío es muy hábil. Lleva veinte años dedicándose a esto. El dinero hace que se lo mandes por Hal-Cash, por ejemplo, porque no deja rastro, y siempre por debajo del límite legal. Pero yo me dedico al marketing *online* y mi mundo es internet.



Generalitat de Catalunya
Departament d'Interior
Direcció General de la Policia

Diligències número:
Ampliatives de:

Hora i data: 12:48 hores del dia 18 de febrer de 2014

Instructor/a: Mosso del cos de Mossos d'Esquadra, amb TIP 12996

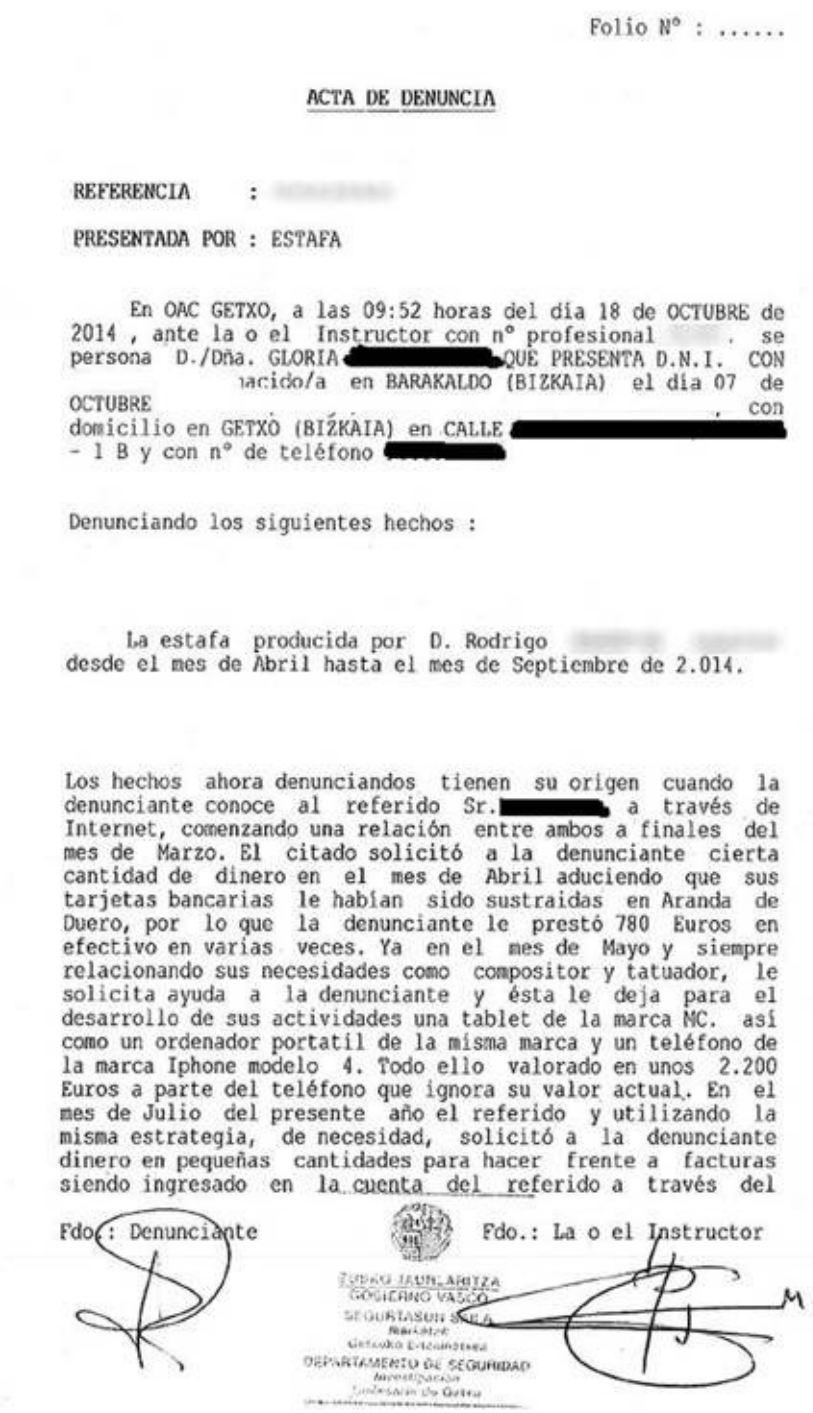
COMPAREIXENÇA A 2 - Eixample, a les 12:48 hores del dia 18 de febrer de 2014, i davant d'aquesta instrucció
COMPAREIX
Qui acredita ser Maria Eugenia [redacted] nascut el dia 30 d'abril de [redacted] fill de Jose i de Purificación, amb DNI (Espanya) número [redacted] amb domicili a carrer de [redacted] núm. [redacted] Barcelona (Barcelonès) i telèfon [redacted]

MANIFESTA
..Que se presenta en estas depedencias la Sra. [redacted] para denunciar los siguientes hechos:
..Que el 14/02/2014 recibió la llamada telefónica de la Sra. Carolina [redacted]
..Que la Sra. [redacted] conocía de la Sra. Carolina por medio de un amigo que tienen en común que se llama Roi.
..Que la Sra. Carolina le informó que el Sr. Roi había estado detenido explicandole que le habia engañado a ella y a muchas más mujeres pidiendole dinero y manteniendo relaciones con todas.
..Que finalmente quedó personalmente con la Sra. Carolina y ésta le enseñó en un ordenador portàtil fotografias de imágenes comprometidas y de diversas tarjetas de crédito a nombre de diversas personas.
..Que al Sr. Roi lo conoció por medio de la página de contactos www.badoo.com el día 29/04/2013.
..Que la Sra. [redacted] entabló una relación únicamente de amistad con el Sr. Roi.
..Que han convivido juntos durante una semana en el mes de Julio del año 2013.
..Que la Sra. [redacted] dejó un juego de llaves de su domicilio en c/ [redacted] puerta 3 de Barcelona.
..Que le dejó las llaves pués ella se marchó a Galicia durante unos días y el Sr. Roi no tenía donde quedarse durante ese tiempo.
..Que el Sr. Roi le devolvió el juego de llaves cuando ella volvió a Barcelona pero desconoce si se ha podido hacer alguna copia.
..Que la Sra. [redacted] desde que conoce al Sr. Roi le ha dejado diversas cantidades de dinero.
..Que el Sr. Roi le pedía el dinero pués no podía pagar diversas

Entonces Gloria me muestra varios registros telefónicos. Eran las facturas de uno de los teléfonos que utilizaba Roi, y de donde partió una de sus líneas de investigación.

—Él había desviado su teléfono al de Victoria, la chica de Aranda de Duero, y en la factura tenía un montón de números de teléfono. Hice un Excel con los más recurrentes y empecé a investigar. Y un amigo informático, ya sabes, tenía la manera de asociar cada número al nombre del titular. Después solo tenía que buscar sus perfiles sociales y así localicé a muchas otras víctimas. Y otro amigo consiguió meterse en el Servicio de Salud gallego, y por ahí localizamos a su hermano y hablamos con él. Yo me quedé en 48 kilos, pero quería llegar al final. Al final, te lo resumo porque la historia es larga, conseguí localizar a cientos de víctimas, pero seguro que hay muchas más. Algunas intentaron denunciar su desaparición, pero como solo tenían un nombre falso, en la Policía las tomaban por locas, porque esa

persona no existía. No nos juzgues, Toni, no estamos locas. Cuando te enamoras de un espejo, porque él crea una personalidad espejo a la suya, eso engancha mucho.



Folio Nº : .....

ACTA DE DENUNCIA

REFERENCIA :

PRESENTADA POR : ESTAFA

En OAC GETXO, a las 09:52 horas del día 18 de OCTUBRE de 2014 , ante la o el Instructor con nº profesional . se persona D./Dña. GLORIA [redacted] QUE PRESENTA D.N.I. CON nacido/a en BARAKALDO (BIZKAIA) el día 07 de OCTUBRE , con domicilio en GETXO (BIZKAIA) en CALLE [redacted] - 1 B y con nº de teléfono [redacted]

Denunciando los siguientes hechos :

La estafa producida por D. Rodrigo desde el mes de Abril hasta el mes de Septiembre de 2.014.

Los hechos ahora denunciandos tienen su origen cuando la denunciante conoce al referido Sr. [redacted] a través de Internet, comenzando una relación entre ambos a finales del mes de Marzo. El citado solicitó a la denunciante cierta cantidad de dinero en el mes de Abril aduciendo que sus tarjetas bancarias le habían sido sustraidas en Aranda de Duero, por lo que la denunciante le prestó 780 Euros en efectivo en varias veces. Ya en el mes de Mayo y siempre relacionando sus necesidades como compositor y tatuador, le solicita ayuda a la denunciante y ésta le deja para el desarrollo de sus actividades una tablet de la marca MC. así como un ordenador portatil de la misma marca y un teléfono de la marca Iphone modelo 4. Todo ello valorado en unos 2.200 Euros a parte del teléfono que ignora su valor actual. En el mes de Julio del presente año el referido y utilizando la misma estrategia, de necesidad, solicitó a la denunciante dinero en pequeñas cantidades para hacer frente a facturas siendo ingresado en la cuenta del referido a través del

Fdo.: Denunciante

Fdo.: La o el Instructor

EUSKO JAURLARITZA
GOBIERNO VASCO
SEGURTASUN SAILA
DEPARTAMENTO DE SEGURIDAD

Rodrigo, ese es su nombre real, aunque jamás lo utiliza, nació en 1976 en Marín (Pontevedra). Creció con una madre dominante y siendo el moñas de la clase. Quizá por eso decidió vengarse de las mujeres. Roi parecía haber hecho un máster en el polémico «Sex Code» de Mario Luna. Aprendió a seducir y convirtió la seducción y la estafa en su *modus vivendi.*

Gloria también le denunció. El 18 de octubre de 2014, en la comisaría de la Ertzaintza en Vitoria. Pero su denuncia solo vino a sumarse a la lista de denuncias

presentadas contra Roi, y que recorren el mapa de España de Málaga a Barcelona. El problema es que como los delitos son menores, Roi siempre sale de nuevo. Así que en 2014 alguien, cansado de que la Policía no consiga frenarlo, sube un blog a internet contando toda la historia: https://moiestafa.wordpress.com.

Con un Máster de Marketing *online* por la Universidad de Londres, Gloria cuenta con un currículo profesional impresionante y que la ha llevado a trabajar en Dubái o Sudamérica. Directora de una empresa de Social Media Manager, es la organizadora de varios eventos de Seguridad Informática en las universidades del País Vasco, a los que acuden algunos de los primeros espadas del hacking español. Pero a pesar de que internet es su hábitat natural, ella también cayó en las redes del estafador, pero ahora sus conocimientos sobre internet podían ayudar a que nadie más cayera.

—Cuando vi el blog —puntualiza Gloria—, hice una estrategia de posicionamiento en Google, para que tuviese enlaces entrantes y subiese en los buscadores. Taggeé [etiqueté] todas las fotos y lo indexé en Google Webmaster Tools. Y empezaron a aparecer más víctimas que iban contando sus experiencias. Hay casos terribles…

Lo que le ocurrió a Gloria, Blanca y a todas las demás le podía haber ocurrido a mi madre, a tu hija, a nuestras primas, vecinas, hermanas o amigas. Quizá les ha ocurrido y nunca se han atrevido a confesarlo.

Con la historia de Roi, la Providencia me estaba lanzando a gritos una advertencia, pero yo no la escuché.

FEBRERO DE 2015
GEOLOCALIZANDO A MARKOSS88

«Ante Dios y el mundo, el más fuerte tiene el derecho de hacer prevalecer su voluntad […] ¡Al que no tiene la fuerza, el derecho en sí no le sirve de nada! […] Toda la naturaleza es una formidable pugna entre la fuerza y la debilidad, una eterna victoria del fuerte sobre el débil.»

Adolf Hitler, discurso «El enemigo de los pueblos» (13 de abril de 1923), párrafo 3

Creepy Data es una aplicación de geolocalización, que hasta no hace mucho podía utilizarse en redes sociales como Twitter o Flickr, para averiguar desde qué punto geográfico se habían actualizado las cuentas. En otras palabras, era posible saber en qué punto del mapa estaba una persona cuando enviaba un tuit a su cuenta.

Durante algún tiempo, y hasta que Twitter restringió su uso, se convirtió en una de las herramientas «de botón gordo» favoritas de los hackers. Incluso Chema Alonso, «el Maligno», le dedicó una entrada en su blog «Un Informático en el Lado del Mal», probablemente el blog sobre hacking más consultado en habla hispana[123]:

La idea es tan sencilla como recoger la información de posicionamiento que se puede sacar de los tuits o fotos publicadas que publica una persona. En el caso de Twitter, recoge información de posicionamiento de tuits con:

— Información GPS cuando se hace desde determinados clientes para teléfonos móviles.
— Tuits asociados a una ubicación.
— Triangulación basada en la IP desde la que se hizo el tuit.

—No fue idea mía —me dijo Álex cuando nos reunimos para ver lo que habían averiguado—, sino de Rafa. Dale las gracias a él.

Rafa, compañero de Pepe y como él destinado en el Grupo de Actuación con Menores, era probablemente el más callado y reservado en nuestras comidas-tertulia. Quizá porque siempre estaba cavilando sobre algún caso abierto. Y para él, como para todos los amigos que se comprometieron con mi problema, MarkoSS88 era un caso.

—Hemos rastreado la cuenta de Twitter de Markos, y cometió un error. Muchos de sus tuits están enviados desde un móvil al que no había desactivado la opción de geolocalización, así que tenemos un mapa de sus movimientos.

Ante mis ojos, Rafa colocó los gráficos del programa Creepy, posicionando en un mapa los lugares donde se encontraba físicamente

MarkoSS88 a la hora de enviar aquellos tuits.

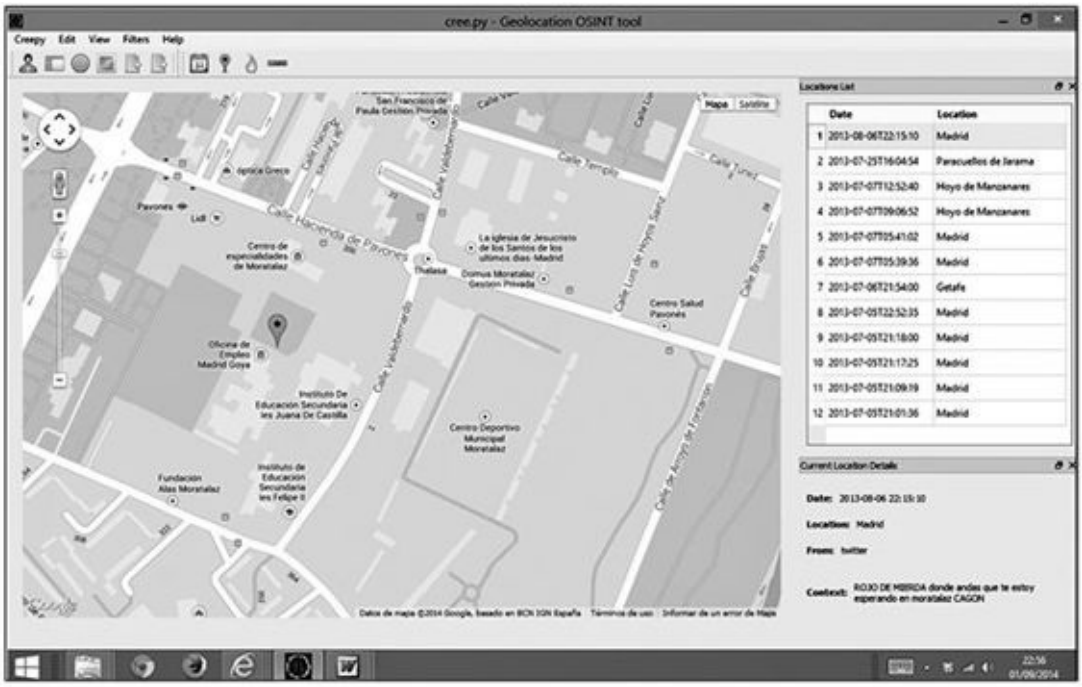
MarkoSS88 había reaparecido en Twitter el 17 de julio de 2013. Y digo «reaparecido» porque él mismo hacía alusión a una cuenta anterior, que sin embargo no nos consta. Curiosamente, en su primer mensaje hace alusión a los hackers… No podía ser más oportuno. Y durante un tiempo habla solo. Como si nadie le conociese. Se limita a subir comentarios que nadie retuitea ni comenta.

Pero Markos es tenaz. Día tras día va ganando seguidores a fuerza de echarle horas y utilizar los *hashtag* con más tirón. Así es como se consiguen seguidores en Twitter. De hecho, su cuenta comienza a recibir seguidores por dos razones. Anuncia que va a publicar la identidad real de Antonio

Salas, y la dirección de Alfon.

En cuanto a la primera, él sabe que es falsa, y en los comentarios de su blog varios skins le reprochan que ha vendido humo al limitarse a repetir teorías publicadas en 2003, cuando apareció *Diario de un skin,* y detalladamente aclaradas ya entonces.[124] Pero da igual, ya había conseguido más *followers* skin en Twitter, que es lo que pretendía con el engaño. En cuanto a la segunda, el anuncio de divulgar el domicilio de Alfon, también sabía que era falso, pero le supuso muchos seguidores antifas. Quizá no era su intención, aunque a nosotros nos vino genial…

Al final, su cuenta se convirtió en una mina. Durante meses, MarkoSS88 había protagonizado acalorados debates, cuando no un simple intercambio de insultos, con numerosos antifas. Y esos enfrentamientos, puro troleo, suelen generar mucho tráfico de mensajes. Eso jugaba a nuestro favor, porque en el fragor del enfrentamiento, incluso alguien tan celoso de su identidad como Markos había olvidado desactivar la geolocalización de su teléfono.



Lo sorprendente es que su cuenta en Twitter no solo había nacido con una alusión a los hackers en el primer tuit, sino que en sus enfrentamientos con los antifas constantemente hacía gala de unos conocimientos informáticos desconcertantes…

—Este tío no es un skin normal —concluía Rafa, que se había empollado sus perfiles sociales como ninguno de nosotros—. Fíjate en sus discusiones con Halcón, por ejemplo. Hablan de doxeo, de hacking, se descubren las IP… Este tío es informático, te lo digo yo…

—Perdona, ¿qué es doxeo?

—El doxing es una técnica para obtener información de una persona a través de la tecnología. No se trata de hackearle la cuenta, sino de saber utilizar las herramientas que ya existen, por ejemplo para averiguar la IP, y a partir de ahí vas tirando del hilo…

Realmente, al volver a leer los viejos tuits, y descubrir sus acalorados debates con los antifas, daba la sensación de que Markos tenía unos conocimientos informáticos desconcertantes para el skinhead de diecinueve años, sin formación universitaria, que pretendía ser.

Rafa, además, había analizado otros elementos de su perfil en Twitter: regularidad, horas de conexión, interrelación con otros perfiles, características lingüísticas, etcétera. No sé si me impresionó más la profundidad de su análisis, o las horas de su tiempo libre que había invertido en aquella investigación, solo por ayudarme. No tengo palabras para agradecérselo.

—Fíjate en esta semana —me dijo, mientras me señalaba una serie de tuits en la cuenta de MarkoSS88—. El 10 de agosto manifiesta desconectarse de las redes sociales por problemas de salud; el mismo día manifiesta comenzar la rehabilitación sin comentar cuál es el motivo. Nadie le pregunta. No hay conversaciones. Esto último lo RT @alvaro88toledo, pero sin comentarios. El 14 de agosto: tercer día de rehabilitación. «Tengo que estar al 100% para hacer de las mías.» Esto lo RT @alvaro88toledo. Del 14

al 22, desaparece. En los días anteriores observo que habla solo, no hay conversaciones, y solo le retuitean un par de tipos, @alvaro88toledo, @andreeaGG98, uno del Frente Atlético NS. Hasta ahora solo ha hablado de UltraSSur una vez, el 7 de agosto. A primeros de agosto se cita con varios rojos en Moratalaz, no veo conversaciones, habla solo… Su lenguaje no es el de un chaval. Juan88, por ejemplo, es de Murcia, comete muchas faltas de ortografía, y usa mucho la k, MarkoSS88 no usa la k.

Cuando los expertos en seguridad informática hablan de toda la información inconsciente que dejamos en la red, se refieren justo a esto. En especial cuando en el fragor de una discusión, en Twitter, Facebook o en cualquier foro, tecleamos rápido, enfadados, con prisa por responder al oponente. Ahí es donde se cometen errores… como no desactivar la geolocalización.

—Con el Creepy tenemos localizado a Markos en varios puntos de Madrid. No hay ninguno desde Mallorca. Lo tenemos en Getafe, en Hoyo de Manzanares, uno en Paracuellos del Jarama, pero sobre todo en la zona de San Blas y Moratalaz. Ahí se repiten la mayoría de los tuits. Este tío vive en el sureste de Madrid. ¿Dónde decías que estaba el campus de la universidad donde intentó ir a por ti?

—En Vicálvaro —respondí intentando recomponer mi cara de asombro.

—Justo. Entre San Blas y Moratalaz… No puede ser casualidad.

—No es posible. Mira, fíjate en las fotos que sube —argumenté mostrándole a Rafa las fotos que Markos colgaba en su Facebook—. Estas playas, estas calas… Joder, esto es Mallorca. Se le ve a él en lugares tan reconocibles como en las que está en el Bernabéu o en el Retiro. ¿Cómo puede hacerse una foto en Mallorca e inmediatamente subirla a internet desde Madrid? No tiene sentido…

Rafa se quedó en silencio, observándome. Estaba buscando una respuesta a mi pregunta. Y no pararía hasta encontrarla.

Capítulo 14
Los hackers del Estado Islámico

«En verdad, te hemos revelado el Libro con veracidad para el bien de los hombres. Así pues, quien sigue la guía la sigue a favor de su propia alma; y quien se extravía se extravía únicamente en su perjuicio. Mas tú no eres su guardián.»

El Sagrado Corán (39:41)

La caída del Temible Pirata Roberts

En febrero de 2015, la comunidad hacker recibió con asombro una noticia que esperaban con impaciencia. Tras un proceso judicial de once días, tan angustioso para la comunidad como mediático, el jurado dictó su veredicto: culpable de los siete cargos de los que era acusado. El joven programador Ross Ulbricht se pasará el resto de su vida en prisión tras ser oficialmente identificado con el nick en internet del Dread Pirate Roberts,[125] propietario y moderador de Silk Road, una web cifrada que surgió en febrero de 2011 en la Deep Web —y por tanto no indexada en buscadores como Google, Bing, Yahoo, etcétera—, en la que era posible comprar casi cualquier tipo de sustancia ilegal. El primer gran supermercado de la droga del mundo. (*El País*, 30-v-2015).

Nacido el 27 de marzo de 1984, Ross William Ulbricht creció en Austin, la capital tejana, con cara de no haber roto un plato en su vida. Mantuvo esa aparente inocencia durante sus años de primaria y secundaria en la West Ridge Middle School primero, y la Westlake High School después, y disfrutó de una beca académica completa para licenciarse en Física en la Universidad de Texas, antes de sacarse un Máster en Ciencias de los Materiales e Ingeniería en la Universidad Estatal de Pensilvania. Nadie dudó nunca de lo privilegiado de su cerebro.

Allí, en la Universidad de Pensilvania, tomó contacto por primera vez con las teorías económicas liberales de Ludwig Heinrich Edler von Mises, el genial economista y filosofo austríaco que dijo: «Todo el mundo, sin importar lo fanáticos que sean a la hora de difamar y luchar contra el capitalismo, lo homenajea de manera implícita al demandar apasionadamente sus productos» o «Lo único que cuenta es el innovador, el que disiente, el que proclama cosas que nadie ha oído antes, el hombre que rechaza los estándares tradicionales y busca sustituir los viejos valores e ideas por otros».

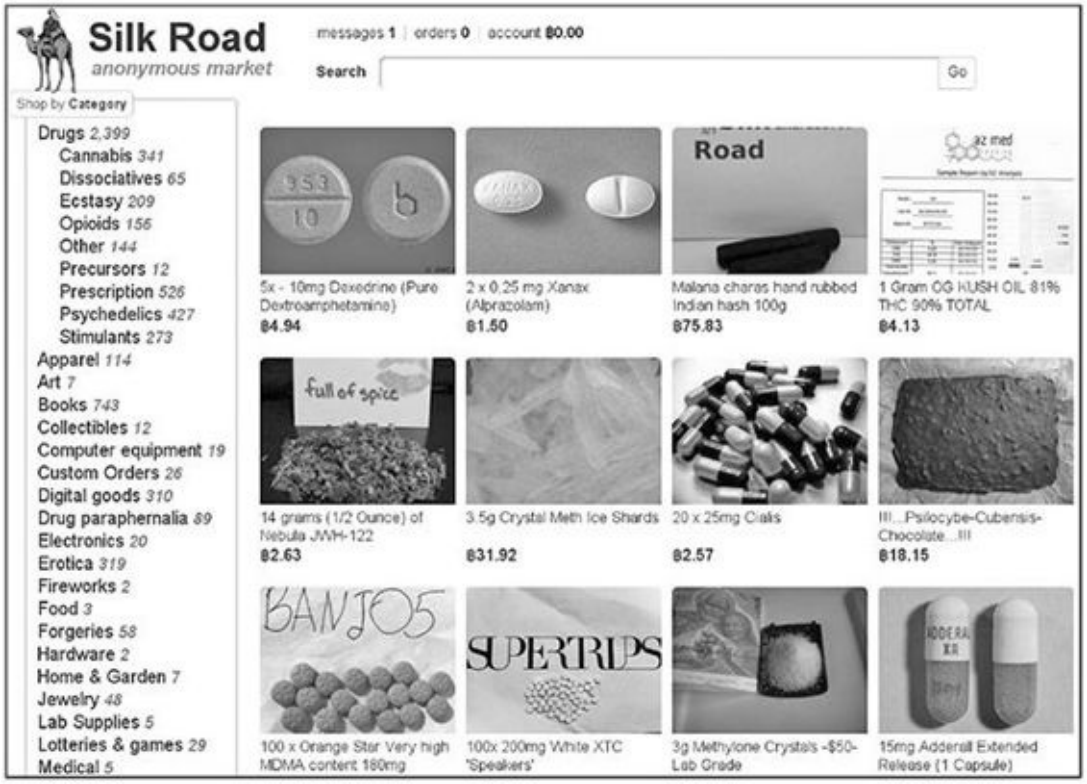
Ulbricht se entusiasmó con el pensamiento de Von Mises, y hasta su graduación en 2009 participó en foros y debates políticos, defendiendo el liberalismo del economista austríaco. De regreso a su Austin natal, montó su primera empresa de venta de libros, sin mucho éxito. En 2010 descubrió el Bitcoin, la criptomoneda de Satoshi Nakamoto, de uso más popular en internet, y escribió en su perfil de Linkedin que quería «usar la teoría económica como un medio para abolir el uso de la coerción y la agresión entre la humanidad».

El 9 de abril de 2012, Ulbricht pregunta a sus amigos en su perfil de Google+ si alguien está familiarizado con los envíos de paquetería postal… El FBI utilizaría este mensaje en el juicio, al interpretarlo como una evidencia de que Ulbricht estaba gestionando un negocio de venta por internet. Y una vez más, todo lo que alguien sube a la red, hasta un mensaje tan inocente como este, puede volverse en su contra algún día.

En octubre de 2013, el FBI lo detiene en San Francisco acusado de ser el responsables de Silk Road: entre otros, Ulbricht se enfrentará a cargos de blanqueo de capitales, piratería informática, conspiración para tráfico de drogas, proxenetismo y asesinato, aunque este último fue posteriormente retirado.

Según el FBI, Ulbricht había amasado una fortuna de más de 3 millones de dólares conSilk Road. Y no lo ganó solo con su comisión en cada venta de comida, libros o herramientas de jardinería. O de hachís o marihuana. Después llegaron la cocaína, el crack, la heroína… Todo valía en la «ruta de la seda» del Temible Pirata Roberts, así que no tardaron en plantarse en sus foros pedófilos, sicarios, traficantes de armas… Lo mejor de cada casa.

El FBI y la ATF dedicaron dos años y muchos recursos a infiltrar en Silk Roada docenas de agentes, disfrazados de vendedores y compradores. Lo llamaron «Operación Marco Polo». Y habría sido sencillo detener a miles de usuarios que navegaban por el anárquico supermercado de lo prohibido confiados en que el protocolo TOR protegía sus identidades, pero el FBI quería ir a por el pez gordo. El creador y moderador de la web. Así es como rastrearon las conexiones cifradas del Temible Pirata Roberts que, como yo, siempre utilizaba cibercafés para conectarse.



A las 3:15 del 2 de octubre de 2013, el FBI cerró la web y detuvo a Ulbricht delante de un ordenador público de la biblioteca de Glen Park, en San Francisco. Creyó que los cibercafés y TOR borraban su rastro. Se equivocó. Dos meses antes, Edward Snowden había gritado al mundo, desde su escondite en Hong Kong, que todas las comunicaciones a través de internet estaban a disposición de la NSA, pero Ulbricht, que sin duda era un genio, creyó que había encontrado la forma de

engañarles. Pues no.

El agente del FBI Christopher Tarbell aseguraba haber identificado el *captcha* del servidor, y que siguiendo esa pista habían localizado los ordenadores en Islandia. Sin embargo, los hackers, que conocían la meticulosidad de Ulbricht con el cifrado, recibieron con escepticismo esa versión oficial, y algunos sugirieron que el caso Silk Road fue la primera prueba de que Snowden decía la verdad. Y la NSA tenía acceso a todo.

Tras el veredicto del jurado en febrero de 2015, la jueza se retiró a deliberar, adelantando que Ulbricht pasaría no menos de treinta años en prisión. El 29 de mayo se haría pública la sentencia definitiva: cadena perpetua. Ulbricht nunca confesó. Poco después de su cierre, la web de Silk Road reapareció durante un tiempo, liderada por otro Dread Pirate Roberts, pero volvieron a cerrarla. Algunos investigadores sugirieron que habían existido más «piratas Roberts» que Ulbricht, pero no importó. Algunas estadísticas sugirieron que Silk Road contribuyó a un descenso de la violencia en relación al comercio de drogas en tanto que la venta *online* elimina al vendedor de los callejones oscuros, los tiroteos, los navajazos… Eso tampoco convenció al tribunal. La condena era definitiva.

Para el fiscal, Silk Road había minado los cimientos de la sociedad norteamericana convirtiendo internet en un arma de destrucción masiva. Ahora podemos fabricar pistolas en nuestra casa con una impresora de 3D, podemos utilizar un dinero (Bitcoins) no rastreable por ningún banco del mundo, podemos comprar drogas a domicilio… Ya no basta con que una madre vigile las amistades que frecuenta su hijo, o sus compañeros del colegio, o sus amigos de Facebook… Con Silk Road, nadie necesitaba salir siquiera de casa para recibir una dosis de cocaína, metanfetamina o heroína: se la llevaban a domicilio oculta en un DVD con una peli de dibujos animados.

El abogado de Ulbricht presentó una moción pidiendo que se anulasen todas las pruebas relacionadas con el material incautado en los servidores de Islandia, porque vulneraban los derechos de su defendido en base a la Cuarta Enmienda. La jueza desestimó su moción. La madre del joven Ross aprendió, en pocos meses, todo lo que pudo, no solo sobre el sistema de justicia norteamericano, sino sobre internet y las nuevas tecnologías. Se convirtió en una inmigrante digital por pura necesidad y en tiempo récord. Y aunque sé que a algunos les sonará atroz, al ver a la madre de Ulbricht peleando con uñas y dientes por defender a su hijo, no podía evitar recordar a doña Elba Ramírez, la madre de Carlos el Chacal, mandando un mensaje al presidente Hugo Chávez ante mi cámara de vídeo para defender el honor de su hijo. O a su hermano pequeño Vladimir, asistiendo a eventos, recogiendo firmas, dando conferencias, para defender la inocencia de su hermano.

La comunidad hacker se dividió con aquella sentencia. Cuando el 4 de febrero de 2015 se conoció el veredicto de culpabilidad contra Ross Ulbricht, muchos lo interpretaron como un aviso a navegantes. Una advertencia a los hackers que

creyesen que podían saltarse las reglas en la red. Para ellos, la sentencia contra Ulbricht era un mensaje.

Otros sin embargo, y aun admitiendo la genialidad de la estructura informática de Silk Road,reconocían que no puedes crear un centro de distribución de drogas, armas o pornografía, y esperar salir airoso. Pero incluso estos últimos consideraban la sentencia desproporcionada. Hablaría de todo esto con David R. Vidal, el «agente Juan», apenas unos días más tarde.

Historia del espionaje

Del 13 al 23 de febrero de 2015, el Museo del Espía[126] celebraba en Sarria (Lugo) una de sus exposiciones temáticas y unas jornadas sobre Inteligencia. El título del congreso era muy atractivo: «Las nuevas amenazas*:* el terrorismo islamista y la seguridad informática», y aunque yo ya había cedido al Museo del Espía alguna de mis «reliquias» para exposiciones anteriores, esta vez pretendían algo más. Querían que participase en el congreso. Por supuesto, me negué. Y seguí negándome un tiempo.

Una cosa es que pudiese cederles la cazadora bomber que utilicé para *Diario de un skin;* una placa de la federación de burdeles ANELA *(El año que trafiqué con mujeres);* el Corán que escribí a mano en árabe durante la investigación de *El Palestino;* o mi chaleco del motero de *Operación Princesa.*… y otra muy distinta que participase físicamente en unas conferencias abiertas al público.

Sin embargo, Peter, un guardia civil amigo vinculado a aquel congreso, puede llegar a ser insistente hasta el agotamiento. No envidio a los detenidos que caigan en su sala de interrogatorios… Durante semanas insistió e insistió, y continuó insistiendo en que participase en el evento. Sin embargo, lo que al fin me hizo claudicar fue el programa de actos. Entre los conferenciantes estaban algunos amigos, como Fernando Rueda y David R. Vidal, cuya opinión sobre la reciente condena a Ross Ultricht me interesaba conocer. A otros, no me los habían presentado formalmente, como el juez Vázquez Taín, de quien fui alumno en un curso sobre blanqueo de capitales mientras preparaba la investigación de *Operación Princesa*, y aquella podía ser una buena oportunidad para tener un contacto más directo y averiguar si había llevado algún caso de cibercrimen. Taín fue el instructor de casos muy mediáticos, como el robo del *Códice Calixtino* o el crimen de Asunta. Y por si todo eso no fue bastante, los policías Pepe y David Madrid también participarían en las jornadas, aunque la presencia de David Madrid, por razones de seguridad, no sería incluida en el programa de actos, y hasta el último momento él no subiría al escenario, sin advertencia previa al público asistente.

—Y si voy yo, puedes venir tú, Toni —insistía David Madrid, mientras Pepe asentía con la cabeza—. Vas a estar protegido. Nosotros nos vamos a quedar en la Comandancia de Lugo, con un amigo guardia civil de allí. Y el jefe de la Comandancia ha mandado una circular a todos los cuarteles de la provincia recomendándoles asistir. Aquello va a estar lleno de policías, no tienes que preocuparte.

—También estaba lleno de policías el auditorio de la Rey Juan Carlos el 5 de marzo, David. Vosotros estabais allí. Y ya ves lo que cuenta MarkoSS88. Eso no me garantiza nada.

Finalmente acepté la invitación de Peter con una condición: yo intervendría por

videoconferencia, y en ningún momento se revelaría que, en realidad, yo estaba en la sala.

Viajé a Sarria solo. Nunca había estado allí, pero durante la investigación de *Operación Princesa* sí había hecho tres viajes a Lugo para visitar los burdeles implicados en la Operación Carioca, y para seguir la pista de algunas de las testigos protegidos, las prostitutas victimizadas en los clubs Queens, Eros, Colina, etcétera, que protagonizan una de las tramas del libro.

Aproveché para regresar a los mismos lugares que había recorrido bajo la identidad del falso *free-biker* de *Operación Princesa*, y aunque todo había cambiado mucho, el paisaje me produjo la misma sensación de honda tristeza. Algunos de los principales clubs de la trama habían cerrado, o literalmente ardido, otros habían reabierto sus puertas a los puteros gallegos disfrazados bajo un nuevo nombre…

El congreso fue un éxito. El salón de actos de la Casa de la Cultura de Sarria estaba repleto de público. Miles de personas llegadas de toda España visitaron la exposición «Historia del Espionaje» del Museo del Espía, y la organización fue extraordinariamente amable y discreta con todos los ponentes, aunque yo no estaba allí como tal.[127]

Y al fin pude saber qué opinaba David R. Vidal, como informático y como trabajador del CNI durante doce años, sobre la sentencia contra Ulbricht.

—Me parece una sentencia en gran medida acorde a las leyes estadounidenses. Puede que tenga algo de ejemplificante, pero que le iba a caer una pena elevada estaba cantado. Es difícil opinar sobre las penas relacionadas con drogas, ya que hay países más permisivos que otros. En cualquier caso, si tienes un portal donde ofreces desde drogas duras hasta órganos infantiles es evidente que acabarás mal. El problema es justo al revés, es decir, que hay muchos delitos informáticos que son difíciles de tipificar y eso hace que los criminales se aprovechen. Entiendo que si eres un traficante, aunque te vistas de seda y te escudes en lagunas legales, te tienen que juzgar como a tal y condenarte en consecuencia.

Fueron días de tensión, esquivando las cámaras de la prensa que cubría el evento, y noches de tertulia hasta altas horas de la madrugada. Rodeado por amigos como David Madrid, Fernando Rueda, David R. Vidal, David Castillo, Pepe, Peter y otros me sentía relativamente seguro, pero después del susto con MarkoSS88 me resulta imposible relajarme en un evento público. Siempre en tensión. Atento a las cámaras de fotos y los teléfonos móviles. Pendiente de quién entra y sale de la sala. Por eso la vi…

Fue durante la conferencia del juez José Antonio Vázquez Taín. Ella estaba sentada a solo un par de metros de mí. La reconocí por las fotos de la prensa, pero lógicamente ella no tenía forma de conocer mi rostro. Era la jueza Pilar de Lara. La instructora del sumario de la Operación Carioca. Más de 160 tomos. Más de 75.000 folios. Y yo los estudié todos. De hecho, tras hablar con varios implicados en el caso, creo que solo De Lara y yo nos lo leímos entero.

Al parecer De Lara y Vázquez Taín habían sido compañeros de promoción en la carrera judicial. Cuando el juez terminó su conferencia, se reunieron en la parte de atrás de la sala y se fundieron en un abrazo. Evidentemente había confianza. Decidí no interrumpirles. Me hubiese gustado acercarme a la jueza y presentarme, solo para agradecerle el coraje y la valentía con que había llevado la instrucción del mayor caso de corrupción policial, política y empresarial de la región, pero concluí que no era el momento. Y además, justo después del juez Taín, me tocaba hablar a mí.

Mi charla cerraba una primera jornada que se había abierto de manera magistral, con una conferencia del informático Juan José Sánchez-Oro, dedicada al uso de internet por parte del ISIS. De nuevo el yihad sobrevolaba la red…

ISIS: terrorismo en línea

Hasta ese mes de febrero, la alianza de sesenta países contra el Estado Islámico había lanzado más de dos mil ataques aéreos sobre sus posiciones (catorce de esos países participaron directamente en la ofensiva). Pero el ISIS seguía creciendo. Y había empezado a encontrar un uso propagandístico a internet. Un fenómeno que jamás se había dado en la historia del terrorismo con tal eficiencia e intensidad.

«Para el terrorismo, nosotros somos el arma. Y las víctimas, la munición.» Así de fuerte arrancó la conferencia, que enunciaba la estrategia del ISIS en las redes sociales. Un blog o una cuenta en Twitter puede llegar aún más lejos que un periódico, radio o televisión por varios motivos. De entrada, permiten la colaboración e interactuación de los simpatizantes en cualquier punto del planeta, y eliminan los intermediarios y la censura de los medios convencionales. Saben que es efectivo, de modo que compiten con otros contenidos en la red por aumentar la espectacularidad y estética. Además, los contenidos digitales son más baratos que una producción televisiva o cinematográfica, permiten la fabulación —la noticia ni siquiera debe ser real, solo espectacular—, minimizan los riegos de ser capturados y están disponibles en todo momento porque no dependen de una programación. Y si encima pueden llegar hasta tu teléfono móvil…

El Ejército Islámico había aprendido de los errores y aciertos de predecesores como Al Qaeda, y había conseguido gestionar internet como ninguna organización terrorista de la historia. Convirtieron un conflicto local en una guerra global. Deslegitimaron a los gobiernos adversarios para justificar la ocupación de territorios. Transfirieron la responsabilidad del atentado o ejecución en el enemigo «diabólico», como Israel, los Estados Unidos u Occidente en general. Potenciaron las redes de reclutamiento en todo el mundo. Denunciaron los crímenes de guerra del enemigo, justificando los propios. Y por último nos inculcaron el efecto panóptico: ISIS está en todos lados, puede verlo todo, y llegar hasta ti, estés donde estés.

Para conseguir transmitir ese demoledor efecto en la opinión pública internacional, el ISIS contaba con organizaciones especializadas en nuevas tecnologías, como el as-Sahab Institute for Media Production, o el Frente Islámico Mediático Global. Además de miles de cuentas en diferentes redes sociales. A través de ellas convocaba concursos *online* de lectura de Corán, u ofertaba puestos de trabajo para editores de vídeo, cámaras, diseñadores gráficos, traductores… y hackers.

El ISIS llegó a internet como a Siria, con evidente vocación de conquista. Y lo cierto es que sus primeras batallas resultaron tan exitosas en la red como sobre el terreno.

A mediados de enero, poco después de la matanza en *Charlie Hebdo,* los hackers del ISIS habían atacado el Mando Central de Estados Unidos, crackeando sus cuentas en Twitter y YouTube para lanzar un mensaje al mundo: «Soldados estadounidenses,

vamos por vosotros, vigilad vuestras espaldas», «Lo sabemos todo sobre vosotros, sobre vuestras esposas, vuestros hijos». Y para demostrarlo, los atacantes filtraron una lista con las direcciones, números de teléfono y nombres de varios generales y soldados del Mando Central con sede en Florida. Entre ellos el jefe del Estado Mayor Conjunto, el general Martin Dempsey.

Los hackers yihadistas habían cambiado la foto de perfil de su Twitter por una de un *mujahid* del ISIS con la leyenda «Amo al Estado Islámico», y se habían hecho con el control total de las cuentas en internet del Mando Central, utilizándolas para continuar lanzando sus mensajes: «El CiberCalifato, bajo los auspicios del ISIS, continúa su CiberYihad. Mientras Estados Unidos y sus satélites asesinan a nuestros hermanos en Siria, Irak y Afganistán, nosotros ingresamos en vuestras redes y aparatos personales y sabemos todo sobre vosotros». «ISIS está aquí, en vuestros PC, en cada base militar. Con el permiso de Allah estamos ahora en el CENTCOM». Daba un poco de miedo.

Los informáticos del ISIS habían estudiado en las universidades occidentales que ahora querían destruir. Aprendieron diseño gráfico, programación, seguridad informática, etcétera, con los mejores, y además, como todos los hackers, poseían una capacidad asombrosa para el pensamiento lateral.

Buena prueba de su capacidad de inventiva fueron las primeras apps del Estado Islámico, como Farachar, un sistema de mensajería telefónica vía Bluetooth. O The Dawn of the Glad Tidings («El amanecer de la Buena Nueva»): una aplicación para el control y sincronización de cuentas en Twitter.

No solo eso, además desarrollaron sus propios videojuegos. En una cultura tecnológica en la que los jóvenes crecen frente a las pantallas del ordenador, los yihadistas les ofrecieron cambiar el papel de héroes y villanos en sus videojuegos. Y además, les brindaban la posibilidad de sacarlos de la pantalla y jugar en la vida real. Matando, decapitando, masacrando, como hacían en los juegos de ordenador, pero en el mundo físico. En el frente de combate. El *meme* popularizado en las cuentas del ISIS, con la leyenda «Este es nuestro Call Of Duty y nosotros reencarnamos en el Paraíso» lo expresa perfectamente.

Para un público menos violento, desarrollaron además toda una estrategia de captación «blanda» a través de páginas como Jihad Matchmaker, que buscaba emparejar con fines matrimoniales a jóvenes musulmanas con guerreros del ISIS. O la campaña CatsOfJihad, protagonizada por tiernos y entrañables gatitos, ataviados como *mujahidin* o posando con los guerreros del Estado Islámico. Adorables.

¿Cómo enfrentarnos a esta amenaza? Sánchez-Oro hacía una reflexión muy interesante. Como profesional de la informática, entendía que era posible responder a la propaganda del ISIS en su propio terreno: la red. Y sugería, como otros especialistas, una táctica psicológica, compatible con otras herramientas de lucha antiterrorista simultáneas: deslegitimar a los propagandistas ante sus seguidores.

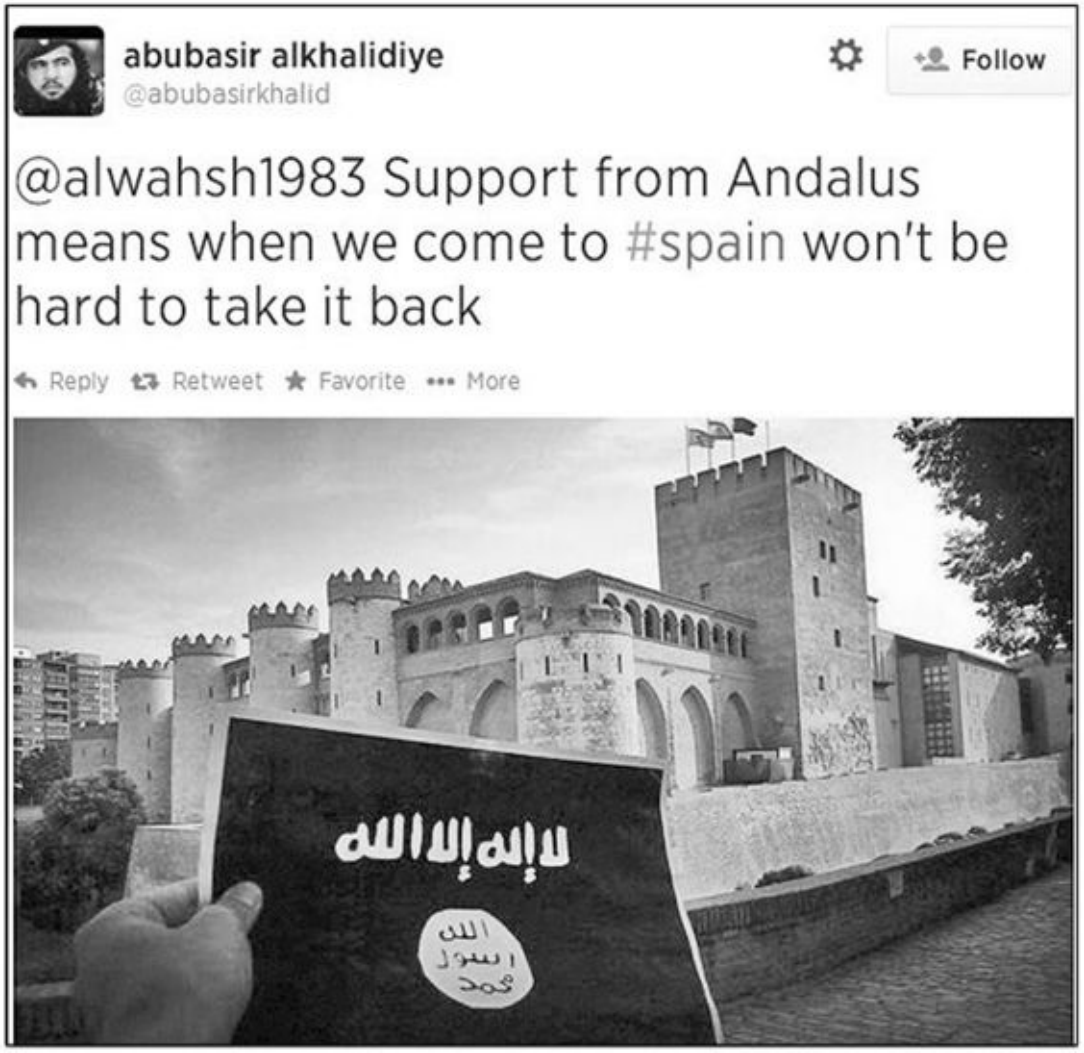
¿Qué responderían los gestores del ISIS en las redes sociales ante preguntas tan incómodas como?:

- ¿Ofrecerá la organización algún tipo de compensación a la familia de los inocentes muertos? Si la respuesta es negativa, ¿ha contemplado la organización la posibilidad de ofrecer una disculpa y condolencias a las familias de manera pública?
- ¿Cuál es la mujer que posee el mayor rango dentro de la estructura de Al Qaeda y cuál es su función?
- ¿Por qué no hay palestinos en el liderazgo del yihad global?
- ¿Por qué los *mujahidin* en Irak matan a las Fuerzas de Seguridad locales y no se centran en los soldados americanos?
- ¿Por qué los activistas de Al Qaeda matan soldados argelinos y no luchan en Irak o Somalia?
- ¿Por qué Al Qaeda no ataca el territorio israelí o las embajadas israelíes a lo largo del mundo?

«Y para ello —sugería— tenemos armas poderosas.» Por ejemplo, llamaba nuestra atención sobre el hecho de que el Twitter del Cuerpo Nacional de Policía, con más de 700.000 seguidores, era el segundo cuerpo de Policía con más *followers* del mundo. Solo aventajado por el FBI con 722.000. Eso era en febrero, cuando se celebró el congreso. En abril, el perfil de Twitter de la Policía española ya había duplicado sus seguidores para convertirse en el perfil de una Policía con más *followers* del planeta. Y eso significa un poder de actuación muy importante en esa red social.

La ciberguerra contra el terrorismo ya era una realidad objetiva. Ese mismo mes de febrero, la Armada británica presentó en sociedad al Batallón 77, también conocido como Chindits:[128] 1.500 especialistas formados como soldados digitales cuyo campo de batalla serán las redes sociales. Pero el ISIS no iba a quedarse de manos cruzadas, y acentuó el efecto panóptico de su estrategia pidiendo a sus seguidores que tomasen fotos de la bandera blanca y negra del Estado Islámico ondeando en lugares estratégicos de todo el planeta.

En España, algunos cretinos cayeron en el juego, imprimiendo en un simple folio la bandera del ISIS y fotografiándola mientras la sostenían ante algún lugar emblemático, para luego subirlo a Twitter. La primera, ante el Palacio de la Aljafería (Zaragoza), la subió a su Twitter un tal abubasir alkhalidiye, que utilizaba como foto de perfil la de otro viejo conocido: Samir Salah Abdullah, alias Ibn Al Jattab, el «Che Guevara musulmán», a cuya historia dedico un capítulo en *El Palestino.*



Después, otros estúpidos hicieron lo mismo en la playa de La Concha en San Sebastián, en una calle de Madrid, etcétera. Simples hojas de papel… Pero el efecto mediático fue brutal. El alarmismo se desató en los medios, como si doce divisiones acorazadas del Estado Islámico hubiesen desembarcado en Gibraltar para reconquistar Al Andalus. Y eso es lo que ellos querían, sembrar el terror con un simple trozo de papel.

Más tarde otros miserables irían más allá, realizando grafitis con la bandera y mensajes del ISIS en Melilla (también viajé allí).[129] Y después otros los imitaron en ciudades como Lepe, Ceuta… Sin duda algunas de esas pintadas fueron obra de imitadores. Jóvenes musulmanes fascinados por el efecto mediático de aquellos primeros selfis. Pero ojo, otras las hicieron islamófobos que solo pretendían generar más odio contra el islam. En los grafitis que aparecieron en Lepe, por ejemplo, y que tanta alarma generaron en su población, el ignorante autor escribió «Lo de Charlie fue poco. Lo peor está por llegar. Alá es grande».[130] Y es tan improbable que un musulmán cometa ese error (Alá en lugar de Allah) como que un cristiano escriba Gexus en lugar de Jesús.

Los autores de las falsas pintadas yihadistas en Lepe probablemente se parecen más a los autores de las pintadas vandálicas, proclamando «muerte a los

musulmanes», que desde entonces me encontré en las mezquitas de media España, convirtiendo la islamofobia en el principal delito de odio perseguido en el país.[131]

Concienciados con el enorme poder propagandístico de la red, algunos especialistas españoles —como Manuel R. Torres Soriano, de la Universidad Pablo de Olavide en Sevilla— se han puesto manos a la obra para estudiar académicamente el fenómeno del ISIS como antes se había hecho con Al Qaeda.

En enero de 2014, Torres Soriano publicaba, directamente en Amazon, *Al Andalus 2.0.: La ciber-yihad contra España*,[132]donde desarrollaba la evolución del yihad en internet desde donde lo había dejado en su tesis doctoral, antes comentada, y en el libro que se inspiró en ella *El eco del terror (Cultura de Inteligencia).*

Yihad 2.0

Pero si algo impactó a los especialistas reunidos en Sarria fueron los vídeos que Sánchez-Oro había recopilado durante su investigación. A pesar de que la grabación se había realizado un mes antes, el 3 de febrero el ISIS dio a conocer el vídeo de la ejecución del piloto jordano Muaz Kasasbeh, capturado el 24 de diciembre cuando su avión fue abatido en Al Raqa, durante uno de los ataques de la alianza, y quemado vivo dentro de una jaula. Doce días después, el ISIS lanzaba otro vídeo estremecedor: la ejecución de veintiún prisioneros, cristianos coptos capturados en Libia, decapitados a la orilla del mar.

Como explicó el informático, en aquellas imágenes nada era casual: amparándose en una antigua *fatwa,* el ISIS reservaba la ejecución con cuchillo o sable a los infieles, y la muerte en la hoguera a los herejes que —según su fanática, irracional y blasfema interpretación del islam (digna del KKK «cristiano»)— habían traicionado la religión. Exactamente lo mismo que la Santa Inquisición católica hacía con heresiarcas, y continúa haciéndose en algunos países de África con las personas acusadas de brujería.

Y llamó nuestra atención sobre la edición de los vídeos. Magistral. Los asesinos no se habían limitado a grabar una *snuf movie*. Al contrario. La realización de los vídeos era absolutamente profesional. Juraría que habían utilizado una *steadycam*, y una grúa para los planos cenitales, o drones. De cualquier forma, el despliegue técnico en la realización de las grabaciones solo se veía superado por el mimo y la dedicación puesta en la posproducción. Algo que quienes hemos trabajado en televisión sabemos apreciar. La música, los tempos… Todo estaba cuidado al milímetro para convertir la barbarie en una obra de arte.

Tanto durante su conferencia como después en las tertulias de la cena, pudimos ver muchos vídeos del ISIS, efectuados con evidente profesionalidad. Los realizadores del Estado Islámico habían decidido utilizar las armas de los propagandistas occidentales para convertir sus acciones en películas de Hollywood y que internet fuese la mayor de las salas de cine. Los conspiranoicos que argumentaban que los vídeos eran falsos «porque estaban demasiado bien hechos» no sabían todo lo que había detrás. Pero el islam no tiene nada que ver con eso.

En los meses sucesivos el ISIS continuó realizando ciberataques y produciendo vídeos de sus atrocidades, para ilustrar su «yihad» en las redes sociales. Pero en agosto se publicó una noticia que era previsible. Yunaid Hussain, hacker británico que se había alistado en el Ejército Islámico y había liderado su presencia en la red, moría abatido por un dron estadounidense. El hacker era un objetivo prioritario de la CIA, y sus cifrados PGP, sus VPN o su encebollado en la red TOR podían protegerle de un virus troyano o un gusano, pero no de un misil teledirigido hacia su asiento ante el ordenador.[133] Que los hackers del ISIS, como Eng Islamic State, Mogahed

Alictronic, Hacker Aldamar o Dr Islamic State se hayan convertido en objetivos prioritarios de Washington, autorizando su ejecución selectiva, ilustra perfectamente la trascendencia de la guerra *online* en un conflicto bélico.

No en mi nombre

Estoy seguro de que cualquiera de los miles de turistas que visitan en la población cántabra de Santillana del Mar el Museo de la Inquisición y la Tortura se estremecerán al contemplar piezas como el potro, la rueda, la cigüeña, la doncella de hierro, la turca o la horquilla del hereje, el toro de Falaris, la cuna de Judas, la zarpo del gato, la pera, la silla o cualquiera de los demás artefactos ideados para infringir dolor, incluidas en este museo o en otros museos de la tortura similares. Estremece pensar que estas abominaciones fueron imaginadas, diseñadas, fabricadas, perfeccionadas y empleadas por hombres que decían ser cristianos.

Estoy seguro de que hasta el último lector coincidirá conmigo en que esos torturadores, vistiesen o no hábitos católicos, anglicanos o protestantes, no representan el mensaje de Jesús de Nazaret ni de la Biblia. Incluso a pesar de que justificasen cada uno de sus actos con ella.

Estoy seguro de que todos coincidimos también en que las violaciones, torturas y asesinatos cometidos por el Ku Klux Klan en los Estados Unidos o el IRA en Irlanda, mientras blandían un arma en una mano y una Biblia en la otra, no tienen nada que ver con el cristianismo.

Y estoy seguro también de que nadie legitimará las mutilaciones, violaciones en grupo, y la perversión de miles de niños convertidos en soldados en África, realizados por el Ejército de la Resistencia del Señor, por mucho que su líder, el psicópata Joseph Kony, afirme hablar por boca de Jesucristo, con el mismo derecho con que Abu Bakr se erigió en califa del islam…

Como no merecen ser llamados cristianos los narcotraficantes mexicanos que decapitan, descuartizan, mutilan y violan, mientras llevan al cuello una medalla de la Virgen de Guadalupe o rezan a la Santa Muerte.[134]

La historia nos ha legado suficientes ejemplos de asesinos, violadores y psicópatas que han pretendido justificar sus actos con la Biblia. Pero todos sabemos que esas acciones no representan al cristianismo… Pues lo mismo ocurre con Al Qaeda o el ISIS en relación al islam.

Una de cada cinco personas en el planeta Tierra es musulmán. Y la natalidad de las familias musulmanas, y las conversiones, hacen que el número de creyentes en el islam crezca de forma exponencial cada año. Sin embargo, y a pesar de las *fatwas* emitidas por las autoridades islámicas contra Ben Laden o Abu Bakr al-Siddiq y sus seguidores, a pesar de las manifestaciones y concentraciones realizadas en todo el mundo, donde millones de musulmanes abominaban de las atrocidades del ISIS, determinados medios de comunicación occidentales prefieren seguir jugando a la ambigüedad, generalizando el fanatismo irracional de un puñado de dementes e identificándolo con todos los musulmanes. Y lo que es peor, fomentando noticias falsas en internet para aumentar la crispación entre religiones. Y es un error.

Declaraciones tan radicales, como las que hizo el alcalde de Venelles, Robert Chardon, proponiendo prohibir el islam en Francia —país en el que ya hay más mezquitas que iglesias— son aberraciones tan fascistas, como las afirmaciones de los imames yihadistas sugiriendo que todos los cristianos maltratan a sus mujeres, violan niños, y son sucios e ignorantes.[135]

Legitimar al ISIS o a cualquier grupo yihadista, colocándolo al mismo nivel que el islam, es tan contraproducente como sentir miedo por una hoja de papel con la bandera yihadista, sostenida por un imbécil ante el Palacio de la Aljafería. No merecen nuestro miedo. No aquí.

FEBRERO - MARZO DE 2015
LA PISTA POLICIAL

«El jefe de un ejército debe vivir con la misma simplicidad que los hombres a quienes manda.»

Adolf Hitler, citado por su secretaria Christa Schroeder en sus memorias

«¡L tnemos! Pro no t lo vs a creer… :-o».

El sms de David me cogió desprevenido. No acababa de entender a qué se refería. Le respondí utilizando la misma contracción de caracteres habitual en los mensajes de sms o WhatsApp, que según algunos autores está mermando los conocimientos ortográficos y lingüísticos de las nuevas generaciones, porque ganamos rapidez en la comunicación a costa de destrozar la noble lengua de Cervantes: «Q tnems?». Respondió: «A MkSS88».

En cuanto nos reunimos, mis amigos los policías me pusieron al corriente del descubrimiento. Y aunque no todos eran tan entusiastas como David, lo cierto es que el candidato a ser MarkoSS88 tenía muchas posibilidades. Aunque las implicaciones de esa teoría eran muy turbadoras.

—Rafa pilló la geolocalización de un par de tuits de MarkoSS88 en la zona de Buitrago de Lozoya. Vale, es verdad, la mayoría están en Madrid, y estos pudo mandarlos un día que se fue de paseo, pero buscando la presencia del nick MarkoSS88 en páginas más antiguas, anteriores a la creación de su blog, nos encontramos con esto…

David me mostró un foro de paintball, un juego de estrategia militar en el que los equipos combaten con armas marcadoras que imitan a las reales. En 2010, alguien con el nick MarKoSS88 se había dado de alta en dicha web, que prefiero omitir, y participaba activamente en el foro.

—Accediendo a su perfil descubrimos un email de usuario y siguiendo el email llegamos a otros foros de paintball y tunning, donde también tiene perfil. El tipo es muy activo en los foros. En uno de ellos se dio de alta con el nick MarKos, a secas, el 4 de octubre de 2006, y estuvo activo hasta el 1 de enero de 2008. En otra de las páginas de paintball encontramos una foto suya…

En la foto aparecía un joven vestido con un traje mimetizado, boina negra y gafas de sol reflectantes. Parecía más un paramilitar que un skinhead. Pero es lo previsible en una página de paintball —un juego que consiste en reconstruir o improvisar batallas sobre el terreno, utilizando armas

marcadoras—. Me llamó la atención su mandíbula. Muy marcada. Angulosa. La foto no era definitiva, podría ser el mismo chico que aparecía en las fotos de MarkoSS88 apretando los dientes, o podría no serlo. Yo no lo tenía claro, y mis amigos tampoco.

—Así que seguimos buscando. Y nos lo volvemos a encontrar en una red social antigua. Su perfil es de 2002. Míralo. Por desgracia, la foto del perfil tampoco es buena. Pero el nick es el mismo MarKoSS88. Con la K en mayúscula.

El joven que posaba en la foto del perfil había cubierto la casilla «Acerca de mí», diseñada en la plantilla para presentarse a los otros usuarios, con el siguiente texto:

> Bueno, soi un xikillo rubio (más o menos :-D) ajos azules, bajito, simpatico…
> Me encantan las motos y coxes y lo k mas: HARDCORE de PONTAERI, CENTRAL, MASIA, PIRAMIDE…venga saludiss y besazos pa las ninias!!!

El tipo aportaba mucha información en su perfil. Fecha y lugar de nacimiento, ciudad de residencia, lo que buscaba, aficiones, etcétera. Y lo que es más importante, incluía su nombre real y sus dos apellidos. A partir de ahí, el resto fue sencillo. Y sobre todo sorprendente.

Rastreando su nombre en las publicaciones oficiales, nos lo encontramos en la lista de admitidos en la Escuela de Cabos y Guardias del Cuerpo de la Guardia Civil, el 10 de mayo de 2011.

—¿Guardia civil? —exclamé incrédulo—. ¿Me estáis diciendo que MarkoSS88 es un guardia civil?

—No, Toni —puntualizó David Madrid—, te estamos enseñando lo que hemos descubierto. Estos son los datos, ahora tú interprétalos como quieras.

—No, joder, no puedo creerlo. Es imposible. No puedo creer que un guardia civil intentase asesinarme, no me entra en la cabeza.

—No nos consta que intentase asesinarte, solo que él dice que lo intentó. Pero no sé por qué te extraña tanto. ¿Ya no te acuerdas de mi jefe?

David tenía razón. En 2002 pudo haber concluido mi historia como periodista encubierto, antes incluso de haber publicado mi primer libro.

Él fue quien me salvó la vida al advertirme de que su superior y responsable del grupo de tribus urbanas de la Policía de Madrid me había delatado a los Hammerskin: «Toni, no vayas hoy al Bernabéu… Los de UltraSSur te están esperando. Saben que eres un periodista infiltrado. Estoy avergonzado. Mi jefe te ha delatado…».

Los periodistas, especialmente los *freelance*, siempre hemos sido prescindibles. Simples peones en el tablero de las investigaciones policiales o de Inteligencia. La mayoría de las veces intentan utilizarnos como propagandistas de las versiones oficiales, y a veces somos una pieza

sacrificable en aras de objetivos más ambiciosos. Pero cuando lo conocí, David era un joven agente de policía que se había infiltrado en los ultras antes que yo —él mismo narró su aventura en *Insider. Un policía infiltrado en las gradas ultras*—[136] y supongo que de todos los policías destinados en el grupo de violencia en el deporte, David era el único que podía comprender el miedo, la angustia y la soledad que experimenta un infiltrado. El único realmente capaz de entender lo que yo sentí durante los meses que conviví con los NS. Por eso, cuando descubrió que su superior había querido apuntarse un tanto con los Hammerkins, advirtiéndoles de que tenían a un periodista grabándoles con cámara oculta, me avisó para que aquel fin de semana no acudiese al estadio. Y ahora iba a necesitar de nuevo de sus consejos.

—¿En serio te parecería tan raro? —insistió él—. Imagínate que alguien quiere hacer méritos delante de los skinhead para ganarse su confianza. ¿Qué es lo primero que tendría que hacer?

—Odiar mucho a Tiger88…

—Exacto. Si te diese una paliza, o una puñalada, o al menos convenciese a la comunidad nazi de que lo había intentado, se convertiría en un héroe.

—Y no solo para los nazis —apuntó Pepe con cierta amargura en el tono.

—Yo no había leído a nadie escribir con tanto odio hacia ti como MarkoSS88. Es irracional. La mejor prueba de que no tiene ni idea de quién eres es que te atribuyó una identidad antigua que sacó de Google, pero es posible que haya intentado utilizarte para ganar puntos delante de los nazis. Como hizo mi jefe.

La posibilidad de que MarkoSS88 fuese un policía no hizo más que acrecentar mi angustia. Soy muy cuidadoso, y pago un precio altísimo por mi anonimato. Más de lo que nadie podría imaginar.

Cuando, este mismo año 2015, acudí a Intervención de Armas de la Guardia Civil para renovar mi licencia, uno de los funcionarios que me acompañaba, buen amigo desde el juicio a Hammerskin, me hizo un comentario jocoso, que refleja mi empeño por no dejar pistas que pudiese rastrear, ni siquiera un policía corrupto: «No sé cómo lo haces, Toni, pero desde 2005 no hay nada sobre ti… Ni cuentas bancarias, ni registros legales, ni padrón municipal… No existes en nuestras bases de datos».

El precio que he de pagar para borrar todas esas huellas es muy alto. La vida se vuelve extremadamente complicada. Pero ante la posibilidad de que MarkoSS88 fuese un guardia civil, resultaba un consuelo. Si ni siquiera sus compañeros en el servicio de Información habían conseguido romper mi *firewall,* para rastrearme, él tampoco podría hacerlo. Sin embargo, yo sí podía rastrearle a él.

No me sentía cómodo investigando a un guardia civil, pero dadas las

circunstancias lo consideré más que justificado. Averigüé que Marcos N. estaba destinado en el cuartel de Buitrago de Lozoya, adonde se había mudado desde su pueblo natal manchego, donde aún vivían sus padres. Localicé su casa, muy cerca del cuartel de la Guardia Civil, y me las apañé para averiguar muchas cosas sobre el nuevo candidato a ser MarkoSS88. Desde sus gustos y aficiones, hasta su número de cuenta bancaria. Todo está en la red si sabes cómo buscar. Por eso es tan urgente que nos concienciemos sobre el riesgo de subir tanta información personal a internet. Las instituciones oficiales ya lo hacen por nosotros y, como me demostraba una vez más esta investigación, todo lo que aquel joven guardia civil había subido a la red antes de entrar en la Benemérita seguía estando allí, proporcionándonos datos sobre su vida personal que no deberíamos conocer.

Localizamos su perfil en Facebook. Este Marcos era más prudente. Lo tenía restringido, pero aun así su foto de perfil y de cabecera eran accesibles para cualquier usuario. Y también sus «me gusta».

La actividad de Marcos N. en Facebook casi siempre estaba relacionada con la Guardia Civil, armas, Sniper, diversas Fuerzas Especiales, aviones caza, motos, boxeo…

Marcos, por ejemplo, manifestaba su solidaridad en páginas de Facebook que homenajeaban a guardias civiles caídos. Pero alguno de mis amigos en Facebook también. Lo descubrí al seguir su rastro en la red. Teníamos amigos comunes…

En su foto de perfil posaba con una moto de color verde, que parecía la misma que encontramos en una de las fotos subidas por Marcos Santos Navarro a uno de sus perfiles de Facebook y de Twitter. Pero después de un meticuloso análisis de ambas descubrimos que eran máquinas distintas. Falsa alarma.

Además, había olvidado utilizar las aplicaciones de Facebook que permiten ocultar tus amigos, así que teníamos una larga lista de contactos de Marcos N. a los que investigar. Cuarenta y cinco, para ser exactos. Todos con su nombre y apellidos.

Fue una labor ardua, pero por suerte la mayoría de los contactos de Marcos N. no había restringido sus páginas de Facebook. Formaban parte de esa masa de personas confiadas que creen que nadie puede estar interesado en sus vidas, en sus fotos o en sus contactos… Así localizamos a un hermano de Marcos, y a su novia, con la que posaba en una de las fotos visibles en su perfil, tomada en la Plaza Mayor de Salamanca… No era Silvia Hierro.

El rastreo de los contactos de Marcos N. implicó la inversión de una cantidad de horas impagable por parte de mis amigos. Uno a uno aquellos

contactos fueron cruzados con otros perfiles neonazis, bases de datos, listados de emails, etcétera. Nada. Salvo las coincidencias atribuibles al azar, no había nada. Incluso yo tenía más coincidencias de amigos comunes en Facebook…

Marcos N., el guardia civil de la mandíbula cuadrada, tampoco era MarkoSS88. Habíamos perdido energía y un tiempo precioso siguiendo una pista falsa. Otra más. Nuestro Markos resultaba mucho más escurridizo de lo que jamás habríamos sospechado. Ya no bastaba con investigar perfiles sociales en internet. Había que subir la apuesta.

Capítulo 15
Espionaje y Ciberdefensa

«¿Cómo es que, siendo tan inteligentes los niños, son tan estúpidos la mayor parte de los hombres? Debe ser fruto de la educación.»

Alejandro Dumas

Mauro, el pequeño espía

Conocí a Chus en unas condiciones absolutamente inusuales. Después de nuestro encuentro en la CyberCamp, Berto intentó encontrar el momento oportuno en nuestras respectivas agendas y por puro azar, o quizá por los secretos designios de la Providencia, ese día llegó semanas después, el 11 de marzo de 2015, y a la carrera.

—Toni, soy Berto, lo de Chus tiene que ser hoy.

—¿Hoy? No jodas. Hoy me viene fatal… ¿No podría ser mañana?

—Me temo que no. Chus tiene una agenda supercomplicada. No te imaginas lo solicitado que está en el servicio. Solo él puede hacer ciertas cosas con los ordenadores, así que si no es hoy, ya no sé cuándo podrá verte. Pueden pasar meses.

En ese instante la respuesta de Berto me pareció exagerada. No lo es. Hoy sé que el torrente de casos que llega a ese departamento de la Guardia Civil casi siempre implica análisis informáticos forenses, y Chus es el mejor en su oficio. Ahora me consta que pueden pasar meses, literalmente, hasta que el hacker de la Benemérita pueda responder tu email o devolverte las llamadas. Y no porque se desentienda de ti, sino porque está desbordado de trabajo. Para entonces no tenía esa información, y Berto no me dejaba otra opción. Sería ese día o no sería.

—Entiendo… Déjame pensar un momento, quizás haya una posibilidad… ¿Os gustaría participar en una sorpresa a un niño enfermo?

Justo ese día, y no otro, se habían coordinado un montón de personas para dar una sorpresa a un niño de nueve años enamorado del mundo de los espías.

A mí me reclutó Fernando Rueda. El veterano periodista y maestro de periodistas, especializado en espionaje, había recibido la llamada de la Fundación Pequeño Deseo[137] para solicitar su colaboración en uno de sus proyectos. Esta Fundación se dedica a hacer realidad los sueños de los niños que sufren enfermedades graves. Su objetivo no es recaudar dinero para costosos tratamientos, ni dirigir campañas para ayudar a las familias… Es algo mucho más sencillo, en apariencia. Pequeño Deseo solo quiere hacerles sonreír, y para ello averiguan cuál es el mayor sueño, la mayor ilusión de esos niños, y mueven cielo y tierra para materializarla.

Y resulta que la mayor ilusión del pequeño Mauro era ser espía. Su enfermedad impedía jugar con las fechas. Los médicos estaban al corriente y habían dado la autorización. Y su madre, abuela y hermano lo acompañarían a la «oficina del servicio secreto» que se ideó para él en el escenario perfecto: el Museo del Espía había organizado una nueva exposición —«Mujeres espía: el lado femenino de los servicios secretos»— en el Teatro Auditorio Adolfo Marsillach de San Sebastián de los Reyes y la responsable, Carmen Bances, había cedido amablemente una de las oficinas de juntas, donde se habilitó la decoración acorde con un servicio secreto como Dios manda.

Allí quedé con Berto y Chus. Si la montaña no va al Profeta…

—No hay tiempo para explicaciones, te lo cuento allí —le dije a Berto—. A las cuatro en punto. No os retraséis. Ah, y traed el arma y los grilletes…

Todo fue como la seda, un día mágico, y no solo para Mauro, que alucinaba cuando se unió a nuestro *planning* de operaciones secretas… El hecho de que Jesús Reina, destinado durante años en el norte de África, y yo chapurreásemos un rato en árabe confirió a la escena aún más verosimilitud. Eso y la imponente Magnum que portaba al cinto el detective.

El pequeño recibió una visita guiada por la exposición del Museo del Espía de la mano de Juan Rando, un espía de verdad, que en su día formó parte de los grupos operativos del CESID, y más tarde el agente Mauro recibió su primera misión… Alguien se tomó la molestia de ocultar por todo el edificio diferentes mensajes ocultos, unos en clave, otros escritos con tinta invisible, etcétera, y Mauro debía descifrar, solo y sin la ayuda de los mayores, cada uno de ellos para avanzar hacia el siguiente. Creo que todos nos sentimos asombrados de la inteligencia y habilidad del pequeño espía, que supo descifrar cada mensaje sin ayuda de ningún adulto.

Una de sus pruebas más difíciles fue la identificar a un agente enemigo (el genial fotógrafo Ignacio Pérez Crespo, que también se prestó a colaborar con Pequeño Deseo), y avisar a la Guardia Civil. Chus y Berto, reclutados precipitadamente para aquella sorpresa, derrocharon generosidad y profesionalidad, y siguiendo las indicaciones del pequeño espía identificaron, cachearon, detuvieron y engrilletaron al agente enemigo, mientras Mauro vivía el día más intenso de su vida. Salió de allí con su carné y su diploma expedidos por el Museo del Espía, y un montón de regalos. Sin duda, el más valioso, la fotografía dedicada que Mikel Lejarza, «Lobo», le envió desde algún lugar del mundo, a través de Fernando Rueda.[138]

Yo, por mi parte, por fin pude conocer a Chus. Berto no había sido el único de sus compañeros en hablarme de sus sorprendentes capacidades. Y nuestro primer encuentro, en unas circunstancias tan especiales y emotivas, sin duda allanó el camino. Chus aceptó iniciarme en algunas técnicas de hacking, y las clases darían comienzo inmediatamente… en su propio domicilio.

Pero el día no había terminado. Al fin, meses de gestiones burocráticas habían dado sus frutos. Conseguir el email y el teléfono personal del jefe de operaciones del Mando Conjunto de Ciberdefensa fue complejo. Pura ingeniería social. Convencer a sus superiores en el Ministerio de Defensa para que autorizasen a grabarle en una entrevista fue difícil. Pero entrar en las instalaciones del MCCD sin identificarme y sin pasar por el arco de metales fue imposible. Lo cual me tranquiliza. Así que cuando el capitán de navío Cubeiro me dijo que pensaba pasarse por la exposición del Museo del Espía justo el mismo día en que habíamos preparado la sorpresa al pequeño Mauro, y aceptó grabar la entrevista rodeados del atrezo de cámaras, micrófonos y dispositivos espía del Mosad, la CIA, el KGB o el MI6, me pareció que me había tocado la lotería.

Ciberdefensa

> El Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) es el órgano de la estructura operativa, subordinado al Jefe de Estado Mayor de la Defensa (JEMAD), responsable de realizar el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Así es como se define a sí mismo el MCCD en su página web oficial,[139] y yo me había citado con su jefe de operaciones a última hora de la tarde. Me esperaba a un tipo aparentemente distante, serio… militar. Capitán de navío equivale a coronel en los demás ejércitos, con el tratamiento de «usía», aunque a mi generación, que ya no vivió el servicio militar obligatorio, se nos hace raro el tratamiento a mandos militares.

Al igual que el Grupo de Delitos Tecnológicos de la Guardia Civil, y a diferencia de la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, el MCCD ha comprendido que sus mejores aliados en su misión por salvaguardar la integridad digital del Ministerio de Defensa son los hackers. Por eso participa activamente en numerosas conferencias, convenciones y reuniones sobre hacking y seguridad informática. Y el de Enrique Cubeiro es el rostro público del MCCD en esas conferencias. CyberCamp, Securmática, HOMSEC… Yo había asistido a algunas de ellas y doy fe de su profesionalidad y rigor en las exposiciones. En las distancias cortas, sin embargo, y ya sin el uniforme militar, Enrique resulta mucho más accesible, cordial y didáctico. Muy alejado de la imagen que me habían dado de él los hacktivistas.

El capitán de navío Cubeiro no es tampoco un desconocido para la prensa, fuera del ámbito informático. Nacido en Madrid, en 1962, Enrique Cubeiro Cabello es hijo y esposo de ferrolanos, quizá de ahí su afición al mar. Y aunque su pasión secreta es la pintura, y en su viejo blog maresybosques.blogspot.com.es todavía podemos admirar algunas de las obras que ya ha expuesto, toda su carrera militar, al menos hasta 2012, está vinculada a la Armada. Por esa razón, a las 03:30 horas del 12 de enero de 2012 era el oficial al mando del buque de aprovisionamiento para el combate (BAC) *Patiño*, cuando un grupo de piratas somalíes intentaron abordarlo, confundiendo sus 166 metros de eslora y 17.000 toneladas con un barco mercante.

Los piratas abrieron fuego con sus AK-47. Más de una decena de proyectiles impactaron contra el casco, muy cerca de los infantes de marina, que no daban crédito a la estupidez de los somalíes. Respondieron al fuego de los Kalashnikov con ráfagas de una MG de 7,62 milímetros. Antes de que los atrapasen, uno de los agresores falleció en el tiroteo y tres fueron heridos. El juicio a los piratas somalíes, un año después, catapultó al comandante del *Patiño* a las portadas de la prensa, como testigo clave en el juicio. Pero poco después Enrique Cubeiro recibiría un nuevo

destino en las Fuerzas Armadas: cambiaba a los piratas somalíes por los piratas informáticos. Un trabajo poco envidiable, dada la carrera por descubrir nuevas vulnerabilidades en los sistemas informáticos militares.

Nos acomodamos en la sala dedicada a la Guerra Fría de la exposición «Mujeres espía». Tras él, durante la entrevista, un maniquí ataviado con el uniforme femenino de la Stasi, la siniestra policía secreta alemana. No fue intencionado, lo prometo, pero tiene su gracia que el interrogatorio al jefe de operaciones del Mando de Ciberdefensa se realizase ante la atenta mirada de la Stasi, conocida por su obsesiva captura de las comunicaciones

—En 2013 ganaste el Premio Álvaro de Bazán por un trabajo sobre el origen, causa y situación actual de la piratería en Somalia basado en tu propia experiencia personal… ¿Cómo se pasa de los piratas somalíes a los piratas informáticos?

—Si te digo la verdad, realmente fue un poco de carambola. Cuando yo dejé el mando del *Patiño* estaba a punto de ascender a capitán de navío y tenía que buscarme un nuevo destino, pero no me apetecía mucho meterme en uno aburrido después de lo bien que me lo había pasado en el *Patiño*. Yo ahí había sido primero segundo comandante y luego comandante, y antes de tomar el mando había tenido de comandante al almirante que mandaba la división CIS del EMACON, el Estado Mayor Conjunto, que es donde nace el embrión de Ciberdefensa. Él fue quien me llamó y me propuso venirme al MCCD.

Dicen que el sentido del humor es un síntoma de inteligencia. Y en el caso del capitán de navío Cubeiro está sobrado de ambas. Sin uniforme y en las distancias cortas no había rastro de su rictus distante y militar.

—¿Y no te atemoriza un poco tener a tus órdenes a verdaderos hackers con una formación mucho más técnica?

—El otro día, por ejemplo, en la conferencia de HOMSEC… cuando leían mi currículo y el de otros participantes, la verdad es que me daba un poco de apuro. Ves a técnicos con montones de cursos, másters, con años de experiencia en seguridad informática… y la verdad es que yo tengo muy poco de todo eso. Pero estoy en un destino de mucha responsabilidad y creo que no lo estoy haciendo mal de momento.

Según me explicó Cubeiro, el MCCD se crea por orden ministerial en 2013, pero lo que había entonces era solo un embrión en la división CIS del EMACON que se encargó de planificar su nacimiento. «En realidad, nosotros nacemos como unidad el 27 de septiembre de 2013, que es cuando llegamos a la base de Retamares. Éramos unos quince. Teníamos un despacho con mesa y silla y poco más. A los pocos días nos pusieron los teléfonos, unos días después los ordenadores, luego los teclados…»

—¿Y antes qué? Porque los ciberataques existen desde hace más de año y medio…

En enero de 2010, *El País* había llevado a su portada los cuarenta ataques informáticos recibidos por el CNI y el Centro Criptológico Nacional antes de esa fecha.[140]

—Antes de la seguridad informática ya existía la seguridad en la información y después el *information assurance,* que era algo más que lo puramente técnico, también se ocupaba de la resiliencia y de la recuperación de los sistemas… Y de ahí se evolucionó a la ciberdefensa, que es *information assurance* y algo más: el combate en el ciberespacio.

—Combate en el ciberespacio —repetí rememorando el clásico *Juegos de guerra.*

—Sí. Obtener inteligencia sobre ciberamenazas y lo que nosotros llamamos con el eufemismo de «respuesta». Le llamamos *respuesta* a lo que en realidad es un ataque, pero un ataque que con nuestra normativa se interpreta como de legítima defensa tras una agresión previa. La respuesta tiene que ser oportuna, legítima y proporcionada, y somos una de las pocas unidades de ciberdefensa a nivel mundial que hacemos respuesta.

—Es decir, convertiros vosotros en hackers…

—Exactamente. En el ciberespacio se combate con ciberarmas. Y las ciberarmas son las mismas para el crimen organizado, que para el hacktivismo o para el ciberespionaje… Unos buscan obtener dinero, otros publicidad y otros información.

—Entiendo que todo esto es la actualización de la guerra asimétrica.

Enrique Cubeiro sonrió con un rictus de satisfacción en el rostro. La pregunta le había sorprendido. El concepto de «guerra asimétrica» no solía entrar en el vocabulario de los periodistas que le entrevistan tras cada intervención del MCCD en una conferencia de hackers, e intuí que había despertado su curiosidad. Durante mi experiencia con las guerrillas y los movimientos revolucionarios en América Latina, para *El Palestino,* el concepto de «guerra asimétrica» era recurrente como justificación de lo que otros llaman terrorismo. E inspiró a Jorge Verstrynge su libro *La guerra periférica y el Islam revolucionario,* editado por las Fuerzas Armadas Bolivarianas de Venezuela, muy influenciado a su vez por la obra *El Islam revolucionario,* de mi mentor en dicha investigación, Ilich Ramírez, «Carlos el Chacal».

—Así es. Estamos ante el paradigma de la guerra asimétrica, donde un solo individuo puede causar grandes daños. El problema es que para defendernos de esa persona necesitamos unos recursos ingentes. La superficie por defender es cada vez más grande. Nosotros comenzamos defendiendo nuestros sistemas de información, sistemas muy securizados, en los que hacen falta contraseñas, claves, estar en locales con seguridad física a los que se accede tras muchos controles… Venimos de una etapa en la que se dio una gran importancia a la conectividad permanente: la telefonía móvil nos permite acceder a la red y a múltiples sistemas. Aparecen las redes sociales, y los organismos oficiales comenzaron a crearse perfiles que hay que defender, porque la opinión pública cree erróneamente que si atacan el perfil del Ministerio de Defensa en Facebook o Twitter te han robado los secretos militares… A eso une que muchos dispositivos móviles ya vienen de fábrica con su dispositivo de espionaje incluido. Que los discos duros también. Que los USB no son de fiar…

—Vale, yo entiendo que tengáis mucha relación con el CNI o el Centro Criptológico Nacional (CCN), pero me ha sorprendido vuestra vinculación con el Ministerio de Industria…

—Claro, pero verás, nosotros lo que tenemos es mucha relación con los CERT, los Centros de Emergencia y Respuesta a Incidentes Cibernéticos. Y en estos momentos, a nivel gubernamental, en España hay otros dos: el del CCN y el de Industria, que es INCIBE, que además trabaja como CERT para el Centro Nacional de Protección de Infraestructuras Críticas. CCN e INCIBE son dos organismos de referencia. Y nosotros tenemos muy buena relación con ambos, por cuestiones personales. En algunas cosas, como la estructura de un CERT, podemos aprender de ellos, pero en otras cosas, como la parte de ciberexplotación o de respuesta, estamos haciendo camino al andar. Con la sensación, te confieso, de que en realidad no podemos copiar de nadie porque estamos todos un poco perdidos. Mira, a veces nos visita la delegación de Suiza, o la de Portugal, y nos preguntan «¿Vosotros cómo habéis resuelto este tema?». Y tenemos que responderles: «Bueno, pues realmente seguimos trabajando en ello»…

En todo momento agradecí la sinceridad, humildad y transparencia del capitán de navío, aunque supongo que detectó un cierto desasosiego en mi expresión. Hasta este punto de mi viaje, ya era consciente de que los recursos, motivación y capacidades de los cibercriminales, o los terroristas, aventajaban con mucho los de nuestras Fuerzas Armadas, y más después de los enormes recortes de presupuestos a los que fueron sometidos tras el inicio de la crisis. Para un sector de la sociedad es fácil aplaudir los recortes cuando afectan a los militares, pero esas carencias no se limitan a la inversión en tanques, cañones o munición. Inevitablemente también menoscaban la capacidad del Ministerio de Defensa a la hora de proteger nuestro ciberespacio. Por eso valoré mucho la honestidad del jefe de operaciones del MCCD.

—Nos hemos traído lo mejor del Ejército de Tierra, de la Armada y del Ejército del Aire para formar nuestra unidad. Y un poco nos echan en cara que les hemos quitado lo mejor que tenían… pero todavía somos pocos.

En una de las conferencias de Enrique Cubeiro a las que pude asistir, mencionaba un argumento muy recurrente entre los menos alarmistas con la amenaza de conflictos cibernéticos. Cubeiro ponía como ejemplo la aviación. Los primeros bombarderos y aviones de combate revolucionaron la guerra, y algunos entusiastas sugirieron que, ante esta nueva tecnología capaz de sobrevolar las líneas enemigas para atacarlas desde el aire, se revolucionaría el «arte de la guerra», dejando obsoletos a otros ejércitos como la infantería o la armada. Pero la historia nos ha demostrado que no fue así. Ni la aviación, ni las bombas atómicas, ni los submarinos, ni ningún otro invento revolucionario aplicado a la guerra ha evitado que continúen existiendo los combates convencionales. Y en el siglo XXI el concepto *ciberguerra* viene a sumarse a esas nuevas tendencias, haciendo que algunos autores imaginen una futura guerra mundial sin fusiles, limitada a teclados de ordenador.

—Y no solo eso —añadió—. Nuestro Ejército del Aire, por ejemplo, se creó hacia 1940, pero existían aviones desde 1910. La Armada operaba sus propios aviones, el Ejército de Tierra también, y se cuestionaba la existencia de un ejército específico para la aviación. Hasta 1939 no se formalizó el Ejército del Aire. Ahora ocurre lo mismo. ¿Hace falta crear un ejército propio para el ciberespacio? Mi general siempre dice: en este campo no podemos prever más allá de cinco años, porque no sabemos dónde estaremos. Este mundo va tan rápido que lo que pensemos ahora igual dentro de cinco años no vale para nada.

—Por eso es tan importante la ciberdefensa…

—Es que tenemos la idea de que esto es un terreno más en el que se combate por la información. Se combate para robar la del enemigo o para evitar que use sus sistemas de información para comunicarse y transmitir órdenes al mando y control. Pero hay más. Te pongo un ejemplo. La gente piensa que un barco aislado, en alta mar, es ciberinvulnerable… Pues no es verdad. Un tipo en su casa, con un ordenador, podría interferir la conexión satelital de un barco. En lugar de tirarle un torpedo se le puede hacer un ciberataque a través de la actualización de la cartografía digital, por ejemplo, mediante el cual se puede alterar el funcionamiento de la planta propulsora del barco. Es muy complicado, pero teóricamente posible. Las unidades dependen cada vez más de lo cíber. Todo está interconectado. Además, cuando se desarrolla un sistema, se piensa en la funcionabilidad, en la conectividad, y en lo último que se piensa es en la seguridad.

Ya ha ocurrido. Eso y mucho más. En estos momentos se libra una guerra en el ciberespacio entre múltiples bandos, que intentan interceptar las comunicaciones, acceder a estructuras críticas o limitar la capacidad ciberoperativa de los contrarios, sin que la opinión pública apenas se entere de lo que está pasando. Una guerra secreta en la que fuerzas de distintos bandos firman alianzas temporales, para unir sus fuerzas contra otros objetivos. En mayo de 2015, por ejemplo, China y Rusia firman un tratado de no agresión cibernética.[141] Solo hay que echar un vistazo al mapa de los ciberataques en tiempo real,[142] para ver quién ataca a quién…

España llegó tarde al campo de batalla, y pagaremos el precio. Porque no solo nos unimos al encuentro hacia el final del segundo tiempo, sino que lo hacemos con unos recursos paupérrimos. Las austeras instalaciones del MCCD están a años luz del potencial, técnico y humano, con que cuentan grupos como el Batallón 77 británico.

—He leído un trabajo tuyo sobre la historia de los sistemas de mando y control…

—¡Ostras! Si eso lo escribí en el año 2000…

—Ya, ya, pero yo procuro prepararme bien las entrevistas —respondí halagado por la nueva expresión de sorpresa del capitán de navío—. Además, ganaste un premio por ese trabajo. Pues, tras leerlo, entiendo que internet agiliza mucho las comunicaciones con los Sistemas de mando y control… pero ¿no las hace mucho más vulnerables?

—Claro. Antes de llegar nosotros se daba mucha importancia a la conectividad

permanente, pero eso fue a costa de la seguridad. Y a medida que se descubren nuevas vulnerabilidades, se comienza una progresión de prohibir y prohibir, hasta un punto que ya casi nos faltaría solo prohibir la existencia de dispositivos electrónicos en el Ministerio de Defensa, y que volvamos al papel y lápiz… que tampoco son seguros. Y eso no puede ser. Lo que tenemos que conseguir es encontrar un equilibrio entre seguridad y funcionalidad. Esa es nuestra misión. Y es un auténtico dolor de muelas. Hay que sacar una copia en un ordenador aislado, firmarla, hacer el PDF, cargarlo en otro ordenador aduana… Con lo fácil que sería darle al botón y mandarlo… Pero es cuestión de disciplina.

—¿Qué sentisteis cuando Wikileaks filtró miles de comunicaciones facilitadas por un colega?

En respuesta, el capitán de navío me mostró el recién diseñado logotipo del Mando Conjunto de Ciberdefensa. Un águila azul que integra los símbolos de los tres ejércitos, sobre un código informático. Y, rodeándola, las iniciales MCCD y ESP, y el lema que les caracteriza…

—Lo de Wikileaks y el soldado Manning ocurrió cuando el Mando estaba naciendo. Mira, nuestro lema es: «Lealtad y Constancia. Ingenio y Destreza». Y lo de *lealtad* está puesto ahí precisamente por eso. Creemos que es fundamental que nuestra gente sea ante todo leal. No podemos permitirnos *insiders*, que el enemigo esté dentro. En toda organización hay un tanto por ciento de descontentos, gente vulnerable por temas de deudas, chantaje, drogas… Nosotros también tenemos que proteger los sistemas de ese enemigo, que es el que más daño te puede hacer. Ese siempre es el más peligroso, el *insider*. Hemos de tener medios para detectar esa amenaza. Ese que accede a sistemas clasificados, a los que no está autorizado, que extrae información, que se conecta a horas raras o a sitios raros. Hemos de tener medios para detectar ese tipo de cosas. Así que aprendimos de ese error.

—¿Y Snowden? ¿Cómo reacciona un Ministerio de Defensa cuando descubre que un supuesto país amigo está espiando sus comunicaciones?

—Hay un dicho en diplomacia: «No existen países amigos o enemigos, solo existen otros países». La historia demuestra que tu aliado de hoy es tu enemigo de mañana. Entendemos que eso va a ser así siempre, y que tu supuesto aliado puede estar interesado en tu información por razones que se te escapan, así que tenemos que prever también esa posibilidad y protegernos hasta de los amigos de hoy.

—Pero imagino que toda nueva herramienta de protección, también implica una nueva forma de ataque…

—Es un arma de doble filo. De hecho, Google iba a sacar un protocolo, el SPDY, que permitía las comunicaciones cifradas. Pero ¿nos interesa tener ese tipo de comunicaciones? Porque las van a tener también los malos. Y con eso los haces prácticamente invulnerables. No vas a poder escuchar las intenciones de los terroristas, por ejemplo… Cuando apareció el protocolo SPDY nosotros dijimos, qué estupendo. Tenemos un protocolo seguro, ya no van a poder interceptar nuestras

comunicaciones. Pero enseguida pensamos, anda, tampoco nosotros vamos a poder interceptar las de ellos. Y las mías son inocuas, pero las de ellos no… Esto es como lo de Hacienda, si no tienes nada que ocultar, no debería preocuparte que te investigase Hacienda…

Inevitablemente recordé el manual de hacking de ETA, y el uso del cifrado PGP que Arkaitz Landaberea había impuesto en las comunicaciones entre los comandos, por orden de «Thierry» en 2008. Cubeiro tenía razón. Los «malos» también pueden beneficiarse del hacking.

—Ya, pero yo todavía no he conocido a nadie que no tenga nada que ocultar en internet… —concluyó el jefe de operaciones del MCCD—. Aunque mira, saber que nos pueden pillar igual nos hace ser mejores…

En el momento de entrevistar a Enrique Cubeiro, España tenía desplazados a más de dos mil hombres y mujeres en misiones en el extranjero. 1.107 efectivos del Ejército de Tierra, 580 de la Armada, 265 del Ejército del Aire, 44 de la Guardia Civil y 46 de los Cuerpos Comunes de la Defensa.

La seguridad de esas 2.042 personas, desplazadas en Bosnia y Herzegovina, Afganistán, Líbano, Senegal, Somalia, Mali, Uganda, Senegal o Gabón y la tranquilidad de sus familias y amigos, hoy también es responsabilidad del Mando Conjunto de Ciberdefensa. Porque si alguien pudiese romper la seguridad de sus comunicaciones, los convertiría en objetivos mucho más vulnerables sobre el terreno. Por eso es tan importante el trabajo del MCCD.

Defensa del ciberespacio nacional

El MCCD, como me explicó el capitán de navío Enrique Cubeiro, es solo uno de los puntales de la ciberdefensa patria. Otra de las piezas clave de nuestra seguridad nacional en la red es el Centro Criptológico Nacional, organismo anexionado al Centro Nacional de Inteligencia y destinado al análisis criptológico de las amenazas a la seguridad del país, así como la investigación y formación de nuevos especialistas. [143]

El CCN nació en 2006 como CERT GubernamentalNacional español y tanto él como su organismo integrado, el Computer Emergency Response Team (CERT), están directamente integrados en el servicio de Inteligencia nacional. Lo que no impide que el CCN-CERT cuente con su propia página web pública y su propio perfil en Twitter,[144] ambos constantemente actualizados y fuente inagotable de información sobre las últimas vulnerabilidades, ataques, noticias, etcétera.

Aunque no llega al nivel de acceso de la NSA, denunciado por Snowden, el CCN-CERT firmó dos importantes acuerdos de colaboración con Microsoft, adhiriéndose al Programa de Seguridad Gubernamental (GSP). El primero en 2004, para tener acceso al código fuente de Windows. Y el segundo, en 2006, para acceder al código de Office.

«Su misión, por tanto —explican en su web oficial—, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes».[145]

Y junto con el CCN-CERT y el MCCD, otro organismo vela por nuestra ciberseguridad nacional: el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Y es que una cadena es tan fuerte como su eslabón más débil. Por ello la ciberdefensa española cuenta con un organismo dedicado exclusivamente a la protección de las estructuras vitales e imprescindibles para la sociedad, consideradas un objetivo prioritario en caso de conflicto o ciberconflicto.

En los últimos años el cine nos ha acostumbrado a la idea de que las estructuras críticas de un país —centrales nucleares, embalses de agua, centrales eléctricas y demás— pueden convertirse en objeto de sabotaje en un conflicto internacional, en una competencia económica o en un ataque terrorista. Pero por desgracia esa posibilidad no se circunscribe a la ficción. Ya existen casos documentados de ciberataques contra estructuras críticas en la reciente historia de la ciberguerra.

En España, la pesada responsabilidad de proteger los pilares fundamentales de nuestra sociedad recae precisamente en el CNPIC,[146] y yo estaba empeñado en que me lo explicase Juan José Zurdo, jefe del Servicio de Normativa y Coordinación de

ese centro.

Podría haber solicitado formalmente una entrevista con él, o podía haberlo interceptado en alguno de los eventos institucionales en los que participa, pero eso implicaría acreditarme con mi identidad real, pasar los controles de acceso, arcos de metales, etcétera, y mis circunstancias personales dificultan enormemente esa vía. Así que, como siempre, tuve que dar un rodeo por el sendero más largo. Un amigo, de un amigo, de un amigo…

Juan José Zurdo es policía. Durante años fue uno de los docentes que impartió cursos a las escalas que conforman el Cuerpo Nacional de Policía (comisarios, inspectores jefe, subinspectores y oficiales) en el Centro de Promoción de Carabanchel, ahora reconvertido en Centro de Altos Estudios Policiales. Antes de eso estuvo destinado en la Comisaría General de Información. Entre sus alumnos estuvo mi amigo el inspector jefe Rado, el jefe de Manu, dos de los «pata negra» que se dejaron más horas en ayudarme en la investigación de MarkoSS88. Ellos hicieron de cicerones para encontrar el día, la hora y el lugar donde pudiese producirse el encuentro.

Ocurrió en una cafetería muy cercana a las instalaciones centrales de la Guardia Civil en la calle Guzmán el Bueno. Donde se desarrollan algunos episodios fundamentales de *Operación Princesa.* Cuando Manu me envió la dirección, sonreí. Conocía bien la zona. Era una buena señal.

Compartimos desayuno: Manu y yo, un combinado de huevos fritos con patatas fritas, tortitas y sirope. Manu, que me conoce, me quita el beicon que acompaña los huevos y lo traspasa a su plato ante la mirada curiosa de Zurdo, que no entiende el gesto. Él y Rado coinciden en pedir un bocadillo y zumo de naranja.

—¿Qué hace un policía como tú en un centro como este? —empiezo—. ¿Cómo terminaste en el CNPIC?

—Supongo que son circunstancias de la vida. Conocía de su existencia por lo que había leído en revistas especializadas de seguridad. Un amigo me comentó la existencia de una plaza y no me lo pensé. Recuerdo cuando me hicieron la entrevista que me pareció un lugar muy interesante porque empezaban a desarrollar su trabajo en ese momento.

—Para que pueda entenderlo mi madre… ¿En qué consiste el trabajo del CNPIC, y cuál es vuestra relación con las diferentes Policías, Ejército o el CNI?

—El CNPIC es un centro que tiene como misión fundamental identificar las infraestructuras imprescindibles para garantizar la prestación de servicios esenciales a la sociedad (que nosotros llamamos críticas) y a partir de ese momento, articular un sistema de planificación que afecta tanto al operador crítico como a la administración a través del desarrollo de unos planes estratégicos y operativos. La Policía, el Ejército y el CNI son miembros imprescindibles del Sistema PIC, compuesto, como he dicho antes, por las administraciones públicas y los operadores privados, y todos ellos colaboran en la tarea de protección de infraestructuras críticas. Digamos que todos

forman parte de una gran orquesta que está dirigida por el CNPIC, en materia de infraestructuras críticas.

Rado y Manu escuchaban con interés, apuntando de vez en cuando algún comentario. Ambos, cada uno desde su trayectoria personal, han participado en operaciones que algún día alguien debería relatar…

—Hace un tiempo —proseguí con la entrevista— leí un artículo tuyo donde mencionas «el ataque terrorista perpetrado por ETA en junio de 1987 a la central petroquímica Enpetrol, ubicada tan solo a cinco kilómetros del centro urbano de Tarragona».[147] ¿Tan real y cercana es la amenaza?

—Nosotros hemos sufrido la amenaza terrorista durante muchos años. Conocemos bien la seguridad física y está muy desarrollada en prácticamente todos los sectores. El problema actual, por supuesto sin olvidar la seguridad física, es la ciberseguridad. Todas las infraestructuras son potencialmente vulnerables, unas más que otras en función de su propia naturaleza. Nuestra labor es identificar esas vulnerabilidades y minimizarlas. Debemos ser conscientes de que en materia de ciberseguridad, la amenaza está muy cercana, aunque el agresor se encuentre a miles de kilómetros de distancia.

—El ataque de ETA a Enpetrol es de 1987, y el CNPIC no nace hasta once años después… ¿Quién protegía las estructuras críticas antes?

—Las Fuerzas y Cuerpos de Seguridad y los propios operadores, pero no de forma organizada ni consensuada, al menos no al nivel que existe en la actualidad. Siempre han existido las infraestructuras críticas y nunca han dejado de protegerse. Los romanos protegían sus arterias principales y las infraestructuras que les daban servicios básicos como puentes, acueductos… La diferencia antes de la creación del CNPIC es que no estaban identificadas como tales y no existía un sistema de planificación que fuera capaz de movilizar las capacidades operativas tanto de la Administración, como de los propios operadores, posibilitando su acción conjunta y coordinada.

Como me había relatado el capitán de navío Enrique Cubeiro, antes de la implantación de internet en todos los sectores de la sociedad, ya existían las mismas amenazas, pero la evolución de la tecnología ha obligado a las Fuerzas y Cuerpos de Seguridad del Estado a adaptar sus sistemas de defensa al nuevo tablero de juego: la red.

—En vuestro organigrama, corrígeme si me equivoco, hay tres áreas: Normativa y Coordinación, Seguridad Física y Seguridad Lógica. Pero la mitad de vuestros recursos están destinados a la seguridad lógica, es decir, la ciberseguridad… ¿Significa eso que nuestras estructuras críticas corren mayor riesgo de sufrir un ciberataque que un ataque físico?

—No. Es relativamente fácil cometer un ataque físico, pero quizá el impacto que pueda tener en el funcionamiento de los servicios esenciales sea escaso, dada la buena resiliencia actual de nuestras infraestructuras ante este tipo de ataques. El

problema es que, como he dicho antes, no existe una cultura de ciberseguridad o, al menos, no hasta hace muy poco, y esto puede producir graves consecuencias con pequeños ciberataques. La gran aportación de este centro a la seguridad de las infraestructuras críticas es el concepto de seguridad integral; es decir, establecer desde un mismo prisma la seguridad física y la seguridad lógica, siendo gestionada desde un mismo departamento de seguridad. En la actualidad, la seguridad física en las infraestructuras críticas está muy consolidada, no así la ciberseguridad. Este es el motivo por el cual debemos desarrollar herramientas, como los CERT y otros organismos especializados (en el CNPIC tenemos además del CERTSI, la Oficina de Coordinación Cibernética) que permita a la ciberseguridad implantarse definitivamente en la seguridad corporativa de los operadores.

—Creo que en este momento estáis centrados en cinco de los doce sectores de nuestra seguridad. ¿En qué consiste el Plan Nacional PIC y los planes estratégicos sectoriales?

—El Plan Nacional PIC es la cúspide del sistema de planificación. De él emanan los demás planes. Este tiene por objeto establecer los criterios y las directrices precisas para movilizar nuestras capacidades operativas y para articular las medidas y las respuestas integradas necesarias para asegurar la protección permanente, actualizada y homogénea de nuestro sistema de infraestructuras críticas frente a amenazas tanto genéricas como específicas contra las mismas. En cuanto a los planes estratégicos, se han desarrollado hasta este momento cinco planes sectoriales (Energía, Industria Nuclear y Sistema Financiero, que fueron aprobados en junio de 2014, y Transporte y Agua que han sido aprobados en septiembre de este año).

Me quedé un momento observando a Zurdo, mientras Rado y Manu me miraban a mí. Sabía que me iba a quedar con las ganas, que la pregunta que iba a lanzar no tendría respuesta. Y que de tenerla, yo no debería publicarla, pero sentía curiosidad personal…

—Lógicamente, si te pregunto cuáles son esas infraestructuras críticas, me mandarás a paseo.

—Lógicamente. —Zurdo sonrió, y mis amigos también—. El catálogo de infraestructuras críticas está clasificado como SECRETO, por lo que no es posible conocerlas públicamente. Solo decirte que son aquellas que prestan servicios esenciales y cuya destrucción o inutilización puede tener un grave impacto en el servicio, las personas, la economía o el medio ambiente.

—Pero… por ejemplo, ¿podrían sufrir las centrales nucleares de España un ataque como el del gusano Stuxnet? —El gusano Stuxnet marcó un hito en la historia de la seguridad informática: alguien, se presupone que los servicios de Inteligencia israelíes y norteamericanos, consiguieron hackear una central nuclear iraní, retardando su programa nuclear, gracias a un sofisticado virus que viajó en un *pendrive* por medio mundo, hasta que alcanzó su objetivo, invulnerable desde la red —. Me refiero a que en ese caso se combinó una acción sobre el terreno, con un

ciberataque. Supongo que en vuestro caso la seguridad física y lógica se contemplan como algo simultáneo e interrelacionado… ¿o no?

—Sí, esa es nuestra filosofía. Las centrales nucleares en España gozan de una seguridad muy desarrollada en el campo físico. Hay que tener en cuenta que son muy herméticas, prácticamente aisladas del mundo exterior, lógicamente por motivos de seguridad. Sin embargo, ataques como el Stuxnet deben hacernos plantear si la configuración de la seguridad actual de la industria nuclear es 100% efectiva. Debemos tener en cuenta que de los casi 63 episodios de alto impacto que se registraron por el Ministerio del Interior en 2014, cuatro afectaban a la industria nuclear.

Le pegué un sorbo al café y continué con las preguntas:

—Con el caso de ISIS estamos observando un uso de la tecnología y la informática inaudito en la historia del terrorismo. Los hackers del ISIS ya han conseguido ataques con éxito contra la ciberdefensa de los Estados Unidos… ¿Debemos considerarlos una amenaza?

—Por supuesto. Este grupo terrorista está utilizando tecnologías emergentes, lo que hace que sean más difíciles de rastrear, por lo que nosotros no podemos quedarnos detrás. Si somos capaces de anticipar y desarrollar tecnología más avanzada que ellos, podremos tener éxito en la protección de nuestras infraestructuras. Si no, es posible que tarde o temprano podamos sufrir un ciberataque de consecuencias graves.

Algunos académicos, como el francés Eric Filiol, han demostrado que era posible inutilizar la red eléctrica estadounidense combinando un ataque físico y cíber, con «un grupo de tamaño reducido (menos de diez personas, que no se conocen entre sí), con medios reducidos disponibles en el lugar».[148] Y por eso la protección del sistema eléctrico fue el primer plan estratégico del CNPIC. Sobre él, y sobre otras vulnerabilidades de nuestras estructuras críticas, continuamos charlando durante el desayuno, que Rado y Manu enriquecían con sus aportaciones, fruto de trabajar para el servicio que más información privilegiada maneja. Pero probablemente no sea prudente ahondar más sobre esas materias en un reportaje público. Los ciberterroristas también leen libros…

MARZO DE 2015
EL SKIN QUE BORRA LOS METADATOS

«Las armas más crueles resultan humanitarias si consiguen provocar una rápida victoria.»

Adolf Hitler, *Mein Kampf*, cap. 6

Rafa tenía razón cuando sugería que MarkoSS88 era un hacker, o al menos alguien con grandes conocimientos informáticos. Lo comprobamos en cuanto revisamos las fotografías que me había enviado de las supuestas heridas, traumatismos, hematomas o puñaladas que había recibido durante sus enfrentamientos con los antifascistas.

La idea me la dio la actualidad. Unos meses antes se había producido el homicidio del hincha del Deportivo de La Coruña, Francisco Javier Romero Taboada, alias «Jimmy», durante un enfrentamiento con hinchas del Atlético de Madrid —una muesca más en el listado de víctimas de la violencia ultra— y a esas alturas de 2015 el tema aún coleaba. Jimmy y sus colegas de la peña ultra Riazor Blues, de ideología de ultraizquierda, acudieron a una cita con los ultras del Frente Atlético, de ideología de ultraderecha, para pegarse. Es lo habitual. No hace falta ser un hacker ni un agente de la Brigada de Información para encontrar en las redes sociales sus intercambios de insultos, amenazas, y sus citas para pelear. Y a MarkoSS88 le encantaba jugar a ese juego.

Tiempo atrás me había enviado varias fotografías de su cuerpo magullado tras alguna de esas peleas, o tras las palizas que le propiciaban los policías cada vez que lo detenían, siempre injustamente, claro. Desde que las recibí, me llamó la atención que en ninguna de ellas apareciese su cara. Eso sería comprensible en el caso de un ultra que oculta su identidad, como hacen la mayoría, pero Markos no tenía problema en mostrar su rostro en todas sus redes sociales. Había cientos de fotos suyas en la red. Solo, con amigos, o con su exnovia Silvia Hierro. Supuse que esa ausencia de su cara en las fotos era por una razón sencilla: se las había tomado él a sí mismo.

Daba igual. En este momento lo que nos interesaba era examinar los metadatos que se incluyen en todas las fotografías.

Los expertos en seguridad informática lo advierten constantemente. Debemos ser muy cautos a la hora de subir nuestras fotos a internet. Porque tanto en las tomadas con el teléfono móvil, como con las modernas cámaras digitales, se incluyen muchos metadatos de los que no somos conscientes: cuándo se tomó la foto, dónde, con qué tipo de dispositivo, etcétera.

Así que rescatamos las fotografías que me había enviado Markos en varios de sus

emails y… nada. No había nada. Markos había borrado todos los metadatos de las imágenes antes de subirlas a sus redes sociales o enviármelas a mí.

Ya no cabía lugar a la duda. MarkoSS88 estaba familiarizado con las técnicas de hacking y con la seguridad informática. Aquellas medidas preventivas a la hora de enviar unas fotos no las toma nadie que no esté familiarizado con el hacking.

Capítulo 16
Viaje a la Deep Web

«Cuando tenga la suerte de prestar algún servicio importante, si el agradecimiento le ofrece alguna retribución, nunca debe admitirla. El Guardia Civil no hace más que cumplir con su deber, y si algo le es permitido esperar de aquel a quien ha favorecido, es solo un recuerdo de gratitud. Este noble desinterés le llenará de orgullo, pues su fin no ha de ser otro que captarse el aprecio de todos, y en especial la estimación de sus jefes, allanándole el camino para sus ascensos tan digno proceder.»

Duque de Ahumada, La Cartilla del Guardia Civil, artículo 7

Hacker antes que guardia civil

Chus es un personaje absolutamente insólito. He conocido a muchos guardias civiles en mi vida, pero ninguno como él. A pesar de sus antecedentes familiares en las Fuerzas Armadas, Chus creció como un hacker, madurando al mismo tiempo que la tecnología. Probablemente aprendió a destripar discos duros antes que a bailar. Ensayando nuevos códigos de programación, buscando vulnerabilidades en los sistemas, aprendiendo Linux, Python, Php, al mismo tiempo que el castellano. Y haciendo «travesuras», como todos los hackers de su generación, que buscaban explorar nuevos horizontes en la red.

La muerte de su padre fue un duro golpe. El más duro de su vida. Y probablemente condicionó para siempre su futuro. Chus dejó de coquetear con el lado oscuro de la red e ingresó en la academia de la Guardia Civil. Hoy viste con orgullo el uniforme de la Benemérita, y sin duda es uno de esos funcionarios, como mis amigos del SAI, que todavía creen en esas cosas como la lealtad, el honor y La Cartilla.

Desde el día en que nos conocimos, actuando juntos en la sorpresa al pequeño Mauro, hasta mi primera clase de «hacking para novatos», pasaron varias semanas. Chus no está destinado en el Grupo de Delitos Telemáticos, ni tampoco en la UCO. Pero en la unidad donde presta servicio son perfectamente conscientes de su brutal cualificación, y la explotan a fondo. Me consta.

Él ha sido el responsable de rescatar todas las miserias de los ordenadores de algunos de los protagonistas de los escándalos de corrupción más mediáticos de los últimos años. Si los periodistas hemos podido llenar primeras páginas con los secretos, las fotografías, los emails y las cuentas bancarias de algunos de los corruptos más célebres de la moderna historia de España, ha sido gracias a la pericia, la persistencia y la brutal capacidad de trabajo de este joven hacker metido a policía.

No importa lo profundo que intentasen esconderlas. Porque Chus, entre otras muchas cosas, es un excepcional forense informático. «Yo puedo rescatar los datos de tu ordenador aunque lo formatees hasta cuatro veces —me dijo en una ocasión—. A partir de la cuarta ya me cuesta un poco más».

Durante el día, a veces durante semanas, el hacker trabaja intensamente operando las máquinas con la pericia de un cirujano. Después traduce sus logros para presentarlos ante los jueces de forma comprensible, o participa en la detención de alguno de esos usuarios, cuyos ordenadores, redes sociales o cuentas de mail había analizado durante días. Luego, por la noche, regresa a su pequeño apartamento en un barrio humilde de la ciudad, y continúa rastreando la red. Vive por y para su profesión, y creo que en eso se basó inicialmente nuestra empatía. Compartíamos la misma pasión, aunque en trabajos diferentes.

Sin embargo, como devoto de un oficio tan exigente como el suyo, a Chus no se le dan bien las relaciones sociales. Como a mí. Cuando nos conocimos, todavía se

lamía las heridas de una relación sentimental que no supo comprender sus ausencias, sus largas horas concentrado ante la pantalla. Sus viajes en plena madrugada para detener a tal o cual criminal. En la red o en el mundo real. Y por todo eso tardamos varias semanas en encontrar el momento en que pudiese dedicarme su tiempo.

Creo que una vez más la Providencia decidió echarme una mano, porque estoy seguro de que Chus nunca habría encontrado tiempo para atender a un periodista mediocre e ignorante, por mucho que le insistiese nuestro común amigo Berto, de no ser porque su madre —a la que adora— le había hablado de él en infinidad de ocasiones. Casualmente resultó ser una lectora de todos mis libros, y creo que eso fue determinante para que su hijo se decidiese a ayudarme.

La primera de las ocasiones en que visité la casa de Chus sentí cierto consuelo. Por fin me había topado con alguien más paranoico que yo.

A estas alturas ya era de sobra consciente de que cuanto más sabes sobre la (in)seguridad informática, más paranoico te vuelves en la red. Antivirus, cortafuegos, cifrados, VPN… Pero el joven guardia civil iba más allá. Su pequeño apartamento era un auténtico búnker. La puerta, blindada, daba acceso a un pequeño pasillo que desembocaba en un salón, tras dejar a mano derecha la cocina. Del salón salía otro pequeño pasillo que dejaba a la izquierda su dormitorio y a la derecha un cuarto de baño, para concluir en la habitación más importante de la casa: su cuarto de ordenadores, cuya puerta, como la de la calle, estaba protegida por una robusta cerradura que cerraba cada vez que salía de casa. En ese trayecto entre la puerta blindada de la calle y susantasanctórum, colocadas en el interior de la pequeña vivienda, conté hasta cinco cámaras de videovigilancia. Supongo que habría más. Yo solo tengo tres. A eso habría que unir las alarmas en las ventanas, los pestillos en las persianas, el pequeño arsenal… No creo exagerar al referirme a su casa como un búnker inexpugnable. Un lugar al que resulta imposible acceder sin permiso. Ni físicamente, ni por supuesto a través de la red.

Y con Chus, y en este entorno, descubrí el fascinante mundo de las «herramientas de hacking» y la Deep Web.

—En mis tiempos tenías que aprender de cero —me contó—. Escribir tus códigos. Comprender cómo funcionaban los binarios. Ahora existen herramientas para casi todo. Programas que puedes descargarte en tu PC y que se ocuparán de romper la contraseña de un email, utilizando automáticamente todas las combinaciones posibles de un diccionario. Lo que llamamos fuerza bruta. Herramientas para interceptar la wifi de los vecinos, para activar sus webcam en remoto, para crear campañas de *phishing* a tu medida. Y todo a tiro de Google… Nosotros hemos detenido a chavales que no tenían ni idea de informática, pero que habían conseguido hacer montones de trastadas utilizando herramientas que habían aprendido a manejar a través de tutoriales de YouTube… Da miedo pensarlo.

Tenía razón. Da miedo pensar que un poder tan enorme esté al alcance de cualquiera. Pero da más miedo imaginar la magnitud de ese poder.

TOR: el pasaporte a una ciudad sin ley

Las herramientas son programas informáticos diseñados para explotar tal o cual vulnerabilidad en un sistema. Algunas son auténticos arsenales, como la famosa Kali Linux, que en realidad es toda una caja de herramientas a disposición del usuario que sepa manejarlas. La primera vez que la vi fue en el ordenador de Chus. En su sanctasanctórum. Por supuesto, utilizando ordenadores virtuales que había creado de antemano para hacerme las demostraciones. Chus es un hacker, un hacker de sombrero blanco, pero ante todo es un policía. Un buen policía. Y ni él habría aceptado, ni a mí se me habría ocurrido proponerle nada ilícito… Como crackear el correo de MarkoSS88 para averiguar su verdadera identidad.

Después de la Kali Linux, conocí otras muchas, incluso de fabricación española, como Foca, Anubis, etcétera. Y descubrí los embriagadores efectos del torrente de adrenalina que desbordan las neuronas del hacker, cuando accede al interior de un sistema ajeno: una universidad norteamericana, un servicio de Información, una poderosa multinacional, explorando sus puertos, sus impresoras, sus bases de datos, buscando una puerta de acceso al sistema, y encontrándola. Tan excitante como un *striptease,* pero más peligroso.

También me asomé por primera vez a la Deep Web. Y aprendí a explorar la red oscura a través del proyecto TOR (The Onion Router), una red no indexada en los buscadores, como Google, que teóricamente permite el anonimato en la navegación, y te da acceso a una *darknet* o internet oscura, en la que durante años han convivido hacktivistas, revolucionarios, pedófilos y delincuentes. TOR es una herramienta poderosa. Pero también un arma.

Dicen los expertos que el internet que utilizamos los usuarios de a pie —ese al que accedemos a través de buscadores como Google, Yahoo, etcétera— es solo el 4% del internet real. Es decir, que más del 96% de lo que hay en la red no aparece en esos buscadores. Pero ojo, esta afirmación, aun siendo real, tiene trampa. Hay muchos contenidos en la red que no aparecen indexados en los buscadores. Por ejemplo, y como me explicaba César Lorenzana, los perfiles de Tuenti, a diferencia de los de otras redes sociales, no están indexados en Google, por lo tanto formarían parte de la Deep Web, al igual que contenidos internos de empresas, universidades, medios de comunicación, y demás. Incluso páginas ya desaparecidas, que no puedes recuperar a través de los buscadores. Sin embargo, existen servicios, como www.archive.org, que te permiten acceder a esas páginas ya borradas de la red sin necesidad de abandonar tu navegador normal. En otras palabras, es posible acceder a contenidos «ocultos» a los buscadores, si sabes cómo hacerlo. Y eso también es Deep Web.

Aun así, en los últimos años los medios de comunicación han generado toda una leyenda negra en torno a la Deep Web, Hidden Web, o web profunda.

En el segundo capítulo de la segunda temporada de la serie *House of Cards,* el personaje de Lucas Goodwin mantiene la siguiente conversación con un hacker:

—¿Deep Web? He oído algo sobre eso…

—Sí, el 96% de internet no es accesible a través de buscadores estándar. Se puede encontrar de todo por ahí: porno infantil, blanqueo de Bitcoins, compra de narcóticos…

—¿Y cómo se accede?

—Es bastante fácil, pero te advierto: ojito con dónde haces *clic*. Hay cosas de locos que lo flipas… Lo primero que necesitas es TOR…

TOR es una red de comunicaciones en la que el enrutamiento de los mensajes intercambiados entre los usuarios es cifrado, y no revela la dirección IP de dichos usuarios. TOR utiliza un software libre que funciona a través de una serie de *routers* donados por individuos y fundaciones para proteger el anonimato de los internautas y por tanto su libertad de actuación en la red.

El origen de TOR está en el proyecto Onion Routing, del Laboratorio de Investigación Naval de Estados Unidos, un proyecto de enrutado «en capas de cebolla», que permitiría proteger las comunicaciones militares cifrando su contenido y ocultando la identidad de emisor y receptor. Pero a finales de 2004 la organización por la defensa de las libertades digitales en internet, Electronic Frontier Foundation, tomó el relevo de la Armada norteamericana patrocinando el desarrollo de TOR, y un año después, nació The TOR Project, una organización independiente, sin ánimo de lucro, que puso esta herramienta al alcance de todos los usuarios.

En 2011 TOR recibió el galardón Free Software Foundation, que premia los proyectos informáticos más beneficiosos para la sociedad, «por haber permitido que aproximadamente 36 millones de personas en todo el mundo, usando software libre, hayan experimentado libertad de acceso y de expresión en internet manteniendo su privacidad y anonimato». De hecho, TOR tuvo un protagonismo fundamental en las llamadas Primaveras Árabes y en los movimientos disidentes de Irán o Egipto. Pero, como es lógico, el mismo anonimato que permite a un disidente denunciar los excesos de un régimen dictatorial, como el de Hosni Mubarak, o a un periodista de investigación infiltrarse en grupos criminales, también cubre el rastro de los ciberdelincuentes en la red.

TOR es el pasaporte que te permite viajar a una ciudad sin ley. Una ciudad en la que reina la anarquía y en la que todo está permitido. Sin reglas, sin normas, sin autoridades que pongan límite a tus actos. Una ciudad en la que puedes caminar por la calle indocumentado, y ocultando tu rostro tras un pasamontañas y tus huellas digitales con guantes de látex. ¿Imaginas un lugar así? Pues eso es la llamada web profunda…

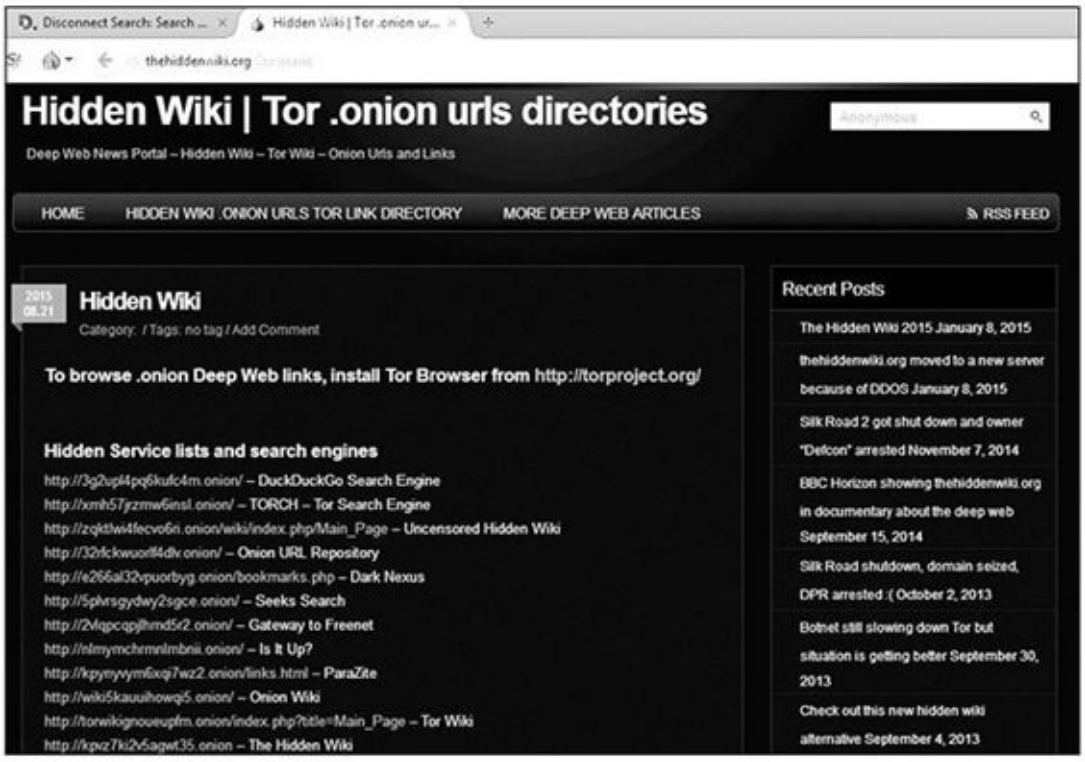
Cada vez que se produce una desgracia en cualquier ciudad del mundo, existen personas que se echan a la calle con medicinas, mantas o agua, para ayudar a las víctimas. Pero también bandidos, salteadores y criminales que aprovechan la confusión para el saqueo y la rapiña. Ni siquiera hay que ponerse en el caso de una tragedia. Incluso un simple corte de fluido eléctrico que apague las farolas de tu

barrio, e inutilice los sistemas de alarma de los comercios, puede hacer que la honradez de los vecinos dure exactamente ciento veinte minutos, antes de comenzar los asaltos. Internet no tenía por qué ser diferente.

Con la ayuda de Chus me descargué el TORBrowser, uno de los sencillos programas que te permiten el acceso a la red TOR. A partir de ahí entras en la ciudad sin ley. La web oculta.

A diferencia de la navegación convencional que hacemos normalmente todos los usuarios, ya he dicho que aquí no valen los buscadores como Google, Bing o Yahoo. Por lo tanto, si no conoces previamente la dirección de la página que quieres visitar, no podrás llegar a ella. Esas direcciones suelen ser una combinación de letras y números aleatorios, que en lugar de utilizar la terminación .com, .es, .org y demás, terminan como .onion («cebolla» en inglés). A falta de Google, pues, lo que sí existen son listados de webs .onion que se renuevan constantemente, ya que las direcciones de las páginas son muy dinámicas, y cambian su URL de un día a otro.

Una buena forma de comenzar a navegar por la Deep Web, una vez instalado el programa TOR, es la Hidden Wiki. Pero no se trata de una Wikipedia, sino de un listado de enlaces que te permite acceder a diferentes páginas de la Deep Web durante el tiempo en que esa URL está operativa.

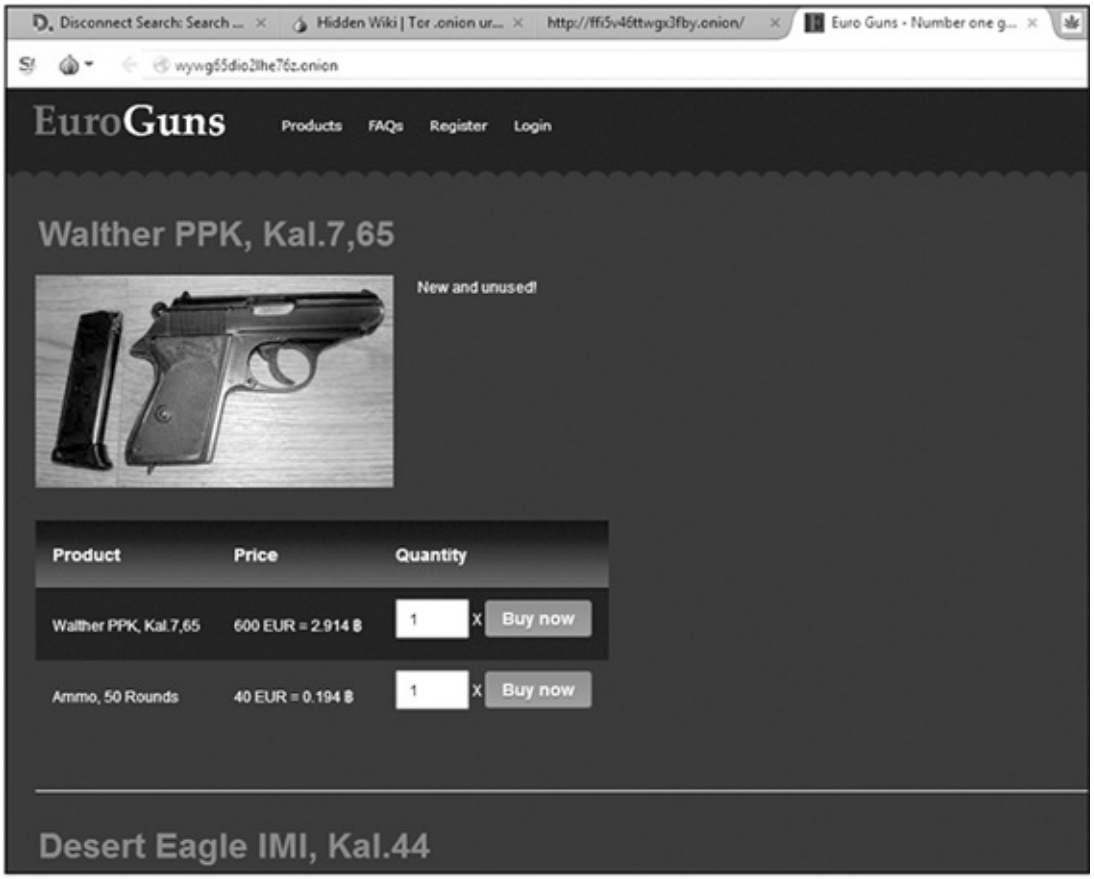


También es posible obtener direcciones de la Deep Web buscando directamente en Google lugares con la terminación .onion, utilizando palabras clave como «TOR links», «List .onion sites», etcétera. Aun así, teniendo en cuenta la velocidad a la que cambian las URL en la Deep Web, es probable que la mayoría de las direcciones que obtengas ya no estén operativas.

La tercera opción es buscar foros .onion. Puntos de encuentro de los cibernautas de la Deep Web donde se intercambian enlaces y direcciones sobre todo tipo de temas… A partir de ahí, todo está permitido.

Hasta para un simple usuario torpe y novato como yo resultó sencillo encontrar páginas donde se ofrecían pasaportes, DNI y todo tipo de documentación falsa, de prácticamente todas las nacionalidades del mundo.

Pistolas, revólveres, fusiles, ametralladoras, granadas y todo tipo de armas, así como la munición para alimentarlas.



O cocaína, hachís, éxtasis, opio, ketamina, marihuana y cualquier otro tipo de sustancia prohibida, que continúan a disposición de los internautas, mucho después del cierre de Silk Road.

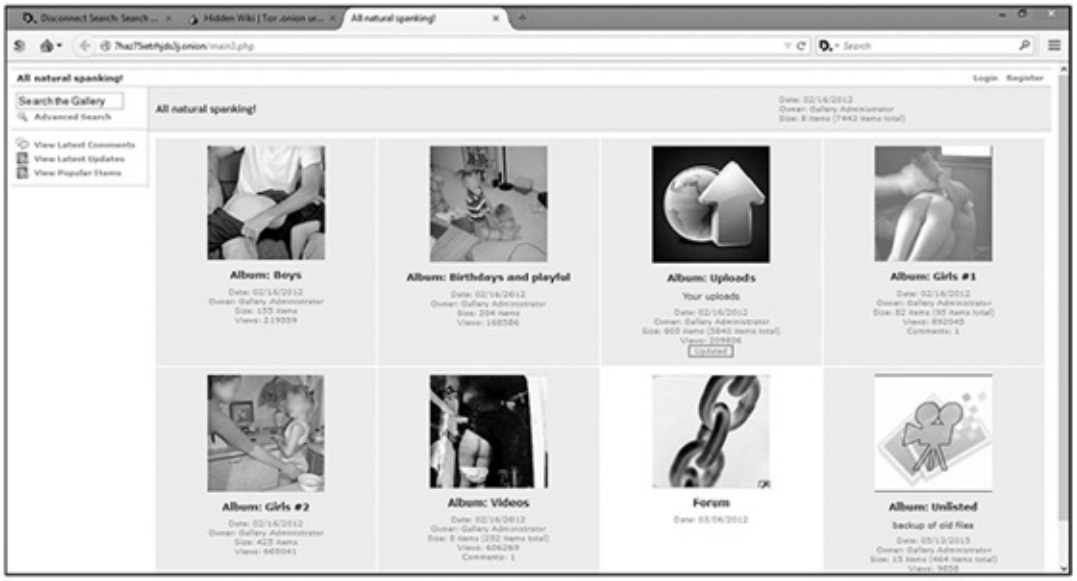
En la Deep Web puedes encontrar cualquier cosa. Si te abruman los millones de resultados que puede ofrecerte la búsqueda de cualquier concepto en Google, que indexa solo el 4% de lo que hay en internet, imagina lo que puedes encontrarte en el 96% restante… Servicios de blanqueo de capitales, anuncios de sicarios y mercenarios, supuestos vídeos *snuff*, falsificación de moneda y/o tarjetas de crédito, ciberdelincuentes ofertando sus servicios…

Es cierto que también existen blogs, programas de radio, servicios de correo y mensajería, *hosting* para el alojamiento de tu propia página en la web profunda, activismo político y social, conspiraciones, anonimizadores… Y sin duda una parte importante de la Deep Web está compuesta por usuarios que buscan proteger su identidad porque desconfían de las autoridades. Pero es evidente que incluso aunque sus intenciones sean lícitas, eso tienen en común con los cibercriminales: quieren ocultarse.

Por eso en la Deep Web me encontré cosas que, publicadas en páginas abiertas, serían objeto de inmediata persecución policial. Como los foros del mercado negro donde los ciberdelincuentes que han zombificado miles de ordenadores ofrecen sus *botnets* para que el comprador las use como mejor le convenga: aumentar seguidores en Twitter, organizar un ataque de denegación de servicio a la empresa de la competencia, posicionar en los buscadores sus propios productos, etcétera.

O foros donde intercambiar y/o vender tus fotos íntimas. Esas fotos que te hiciste para tu novio, amante o pareja, y solo para él. O que conservabas en la memoria de tu teléfono móvil, o en el disco duro de tu ordenador, convencida de que ahí estaban seguras. En la Deep Web existen infinidad de foros de intercambio donde exnovios o parejas actuales intercambian las fotos de sus «amadas» sin su consentimiento. Saben que de hacerlo en una página abierta podrían ser descubiertos o denunciados, pero en TOR cuentan con un anonimato que revela su naturaleza ruin y miserable. La próxima vez que te hagas una foto íntima para enviársela a tu pareja, piensa que dentro de un tiempo quizá deje de serlo… y eso no hará que esas fotos o vídeos desaparezcan. Si has depositado tu confianza en quien no la merecía, quizá miles de personas en todo el mundo, cuya sola presencia te provocaría náuseas, estén ya disfrutando con ellas…

Pero lo peor de todo el viaje a TOR fue descubrir la nutrida, variada y prolífica presencia de la pedofilia en todas sus manifestaciones imaginables. Eso que muchos llaman «pornografía infantil», pero que el comandante César Lorenzana prefiere denominar más correctamente «abusos sexuales a menores».



Es probable que si buscas en ese tipo de páginas, te encuentres a tus propios hijos, sobrinos, nietos… No porque nadie de la familia haya abusado de ellos sexualmente —aunque no sería el primer caso—, sino porque en algunas de esas páginas se compilan esas fotos inocentes de tus hijas en la playa que subiste a Facebook, esos vídeos de tu nieta bailando que tenías en tu disco duro cuando te lo crackearon (tú que dices que no tienes nada que pueda interesar a los ciberdelincuentes), o esas imágenes de tus sobrinos desnuditos sobre la colcha, en las que solo un enfermo mental puede ver un contenido sexual… pero es que esos enfermos mentales existen.

Ese es solo el primer nivel. A partir de ahí comienza una pronunciada pendiente hacia un pozo oscuro sin fondo, donde puedes encontrar todo tipo de atrocidades cometidas con niños de cero a dieciocho años. Todo lo sucio y obsceno que puedas

imaginar, y bastante más.

Yo no lo creía. Lo juro. Estaba seguro de que exageraban. Cada vez que leía una noticia sobre la desarticulación de una red de «pornografía infantil», o que habían incautado imágenes de abusos a niños y niñas de uno, dos, cuatro, seis años… pensaba que exageraban. No podía imaginar cómo es posible tener una relación sexual, completa o no, con una criatura de esa edad. Pero es posible. Lo he visto. Está ahí, en la Deep Web, al alcance de cualquiera. Y ahora no consigo quitarme esas imágenes de la cabeza… Hay cosas que te hacen replantearte tu rechazo a la pena de muerte.

Policías en la red profunda

A pesar de todas las gestiones de Israel Córdoba y David Pérez, finalmente no conseguí la autorización para entrar en la Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía. Todos pensamos que sería más sencillo, pero es que yo tampoco lo puse fácil. Me había empeñado en que no quería pasar por el registro ni por el arco detector de metales, y no porque desconfíe de la profesionalidad y diligencia de los funcionarios de nuestra Policía, sino porque tengo una fe absoluta en lo que puede conseguirse con una buena motivación. Y dejar tu DNI y tus datos en la base informática de una comisaría es dejar una pista que alguien podría seguir en el futuro. Si yo, que soy un simple periodista *freelance*, he podido obtener registros similares en mis investigaciones, cualquiera podría hacerlo.

Recostado en el sillín de la moto, aparcada en la calle Julián González Segador, a pocos metros de la entrada principal del Complejo Policial de Canillas, tuve tiempo, mucho tiempo, para leer y releer la historia de la BIT en la página web oficial del Cuerpo Nacional de Policía: www.policia.es.

Equivalente al Grupo de Delitos Tecnológicos de la Guardia Civil, «la Unidad de Investigación Tecnológica —dicen en su web— es la Unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia. Pornografía infantil, estafas y fraudes por internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería… Nuestra misión consiste en obtener las pruebas, perseguir a los delincuentes y poner a unas y otros a disposición judicial. Nuestras herramientas son la formación continua de los investigadores, la colaboración de las más punteras instituciones públicas y privadas, la participación activa en los foros internacionales de cooperación policial y la colaboración ciudadana».[149]

Después de dos horas esperando en la puerta de la comisaría, mientras Israel intentaba convencer a los responsables de la BIT, me llamó para darme el veredicto:

—Lo siento, Toni, no hay manera. Dicen que tienen órdenes de arriba de que no se puede entrar con cámaras en la Brigada, y menos sin identificarte…

Así que no entré.

Imagino que los anteriores responsables de la BIT debieron de considerar mi negativa a identificarme en los controles como un capricho. Es lícito. Pero dada mi particular situación, y siendo el único responsable de mi seguridad, soy yo quien decide qué medidas de precaución tomo cada día, y en este caso prefería perder esa entrevista antes de dejar un cabo suelto, que después me quitaría el sueño. Sobre todo cuando se trata del CNP. A pesar de que tengo grandes y queridos amigos en este Cuerpo, como han demostrado con la investigación de MarkoSS88, también me he hecho algunos enemigos. Como el jefe de Tribus Urbanas que me delató a los skin, ciertos policías propietarios de burdeles que descubrí durante *El año que trafiqué con mujeres*, o los funcionarios corruptos de *Operación Princesa*. No, definitivamente,

era mejor perder aquella entrevista que pasarme las noches angustiado, por si alguno de aquellos corruptos podía acceder a mis datos en la comisaría.

Sin embargo, un año después de aquellas gestiones en Canillas, el viento se puso de cara. Y ocurrió de la forma más inesperada. David Pérez ya me había advertido de que había movimiento en la Brigada de Investigación Tecnológica. Esperaban la llegada de un nuevo jefe. Lo que no podía imaginar era que ese nuevo jefe, jefa en este caso, era una vieja conocida.

La noticia me llegó directamente a través de ella, vía sms. Y pongo a David Madrid, Pepe, Rubén, Rafa, Álex y los demás por testigos de que ocurrió exactamente así. Porque aquel sms me llegó en plena comida-tertulia con todos ellos, mientras discutíamos nuestro próximo paso en la investigación sobre MarkoSS88.

«Buenas tardes, Antonio, soy la inspectora Silvia Barrera… Me dio tu teléfono el policía David Pérez, soy su jefa. Creo que aunque no personalmente, nos conocemos ya de Twitter. Me comentó que te diera un toque…»

La inspectora Silvia Barrera es la jefa de Grupo de Tratamiento de Evidencias Digitales de la Unidad de Investigación Tecnológica de Cuerpo Nacional de Policía. Profesora colaboradora en el Grado de Criminología en la Universidad Complutense de Madrid, mantiene además su propia web sobre ciberinvestigación: www.sbarrera.es, y también un blog en Tecnoxplora: Internet, Ciudad con Ley.[150] Y me atrevería a decir que junto con la también inspectora Esther Aren (@chicageo68), el rostro amable del CNP en internet y en las CON de seguridad informática. Aren en la prevención, y Barrera en la investigación y represión del delito.

Mucho antes de recibir la grata sorpresa de aquel sms, yo ya había podido asistir a alguna conferencia de Silvia Barrera y, nueva sorpresa también, apenas dos minutos después de comenzar a seguir su cuenta en Twitter, ella comenzó a seguirme a mí… Supongo que la foto de mi perfil en esa red social, de la época como motero *free-biker*, despertó sus sospechas como policía. No se me ocurre otra razón. Sin embargo, pasaría algún tiempo hasta que pudiésemos encontrarnos en persona.

Integrante de diversos grupos de trabajo de la Comisión Europea, Silvia es la representante española del Cuerpo Nacional de Policía en el Ciclo Político Estratégico en materia de Ciberataques e Inteligencia en la Red de la Comisión Europea a través de Europol. Y constantemente viaja para participar en reuniones de Interpol, Europol, Counceil of Europe, G-8, etcétera, sobre el cibercrimen y la forma de combatirlo. Precisamente por eso, por su activa participación en las reuniones internacionales, tiene una visión muy global sobre la lucha policial contra el delito en la red.

El día antes de nuestro primer encuentro me envió un sms desde Bruselas, en plena reunión de Europol. Al día siguiente estaría en Madrid, y yo también. Acordamos vernos, pero antes tuvo la gentileza de enviarme su tesina de final de carrera en Criminología: «La lucha policial ante el horror de la pornografía infantil». Son apenas 120 páginas, pero suponen un auténtico descenso a los infiernos más

oscuros y siniestros de la red.

Al leerla por fin entendí por qué la inspectora Barrera utiliza el nick de «internetpark» en la red. Un seudónimo, dice ella, «que refleja mi pesimista visión del internet de las cosas… Una pesimista visión de la realidad, quizá provocada por mi día a día…».[151]

Para entonces ya había leído y escuchado muchas entrevistas a Silvia Barrera, y conocía ese tono pesimista que subyacía en casi todas ellas, en contraste con su enorme sonrisa. Pero al leerme su tesis entendía mejor de dónde podía provenir ese pesimismo. Para su tesina de fin de carrera, la inspectora Barrera había escogido un tema duro. Quizá el más duro de todos. Y como policía de redes que ya era, había tenido acceso a una información privilegiada sobre el infierno que se oculta en los recovecos más profundos y siniestros de la red: el abuso sexual a menores… La Deep Web es su feudo por naturaleza.

En su libro, la inspectora Barrera repasa, una a una, las principales operaciones de la Brigada de Investigación Tecnológica del CNP en relación a la «pornografía infantil» desde su creación, en 2002. Sin embargo, unos años antes, a principios de 1996, «el director general de Protección Jurídica del Menor del Ministerio de Asuntos Sociales reconocía ante los medios de comunicación la existencia en nuestro país de mafias dedicadas al tráfico de menores. Además de niños y niñas españoles, en la península se compraban y vendían fundamentalmente menores portugueses, dominicanos, marroquíes y procedentes de países del Este de Europa». Yo tuve la oportunidad además de comprar cinco niñas mexicanas…

Barrera aplica la definición más purista de «crimen organizado», es decir, tres o más personas que se reúnen para delinquir, para sugerir que se aplique a este tipo de delitos ese tipo penal, con todos los agravantes que puedan incluirse. Porque la pedofilia es la peor lacra, y un fenómeno universal que no entiende de razas, credos ni lenguas.

> La policía británica recibió del FBI una lista con 7.272 nombres de ciudadanos ingleses que aparecía en la base de datos de LandSlide; la primera gran operación a nivel internacional contra la pornografía infantil iniciada en el año1999desde el Servicio de Inspección Postal de los Estados Unidos, quienes investigaron un portal de contenidos para adultos en el que aparecía un enlacepublicitario ofreciendo pornografía infantil mediante pago con tarjeta de crédito. El portal era titularidad de la empresa americana LandSlide Production Inc.

Es solo un ejemplo. Hay más.

> El 72% de las víctimas son niño/as entre 0 y 10 años de edad. El 44% imágenes que representan violaciones y torturas sexuales sobre menores. El 48% de páginas web, comerciales o no, están alojadas en servidores de América del Norte y el 44% en Europa y Asia. Durante el año 2009 fueron cerrados 1.316 sitios web por contener material relacionado con abusos sexuales a menores.

Y la inspectora Barrera no se está refiriendo a «terroristas» árabes que quieren casarse con menores, como en las noticias falsas de los islamófobos. Estos son

occidentales «cristianos» que solo quieren follárselos.

En su tesis, Barrera analiza la evolución de los abusos sexuales a menores en internet, desde su primera fase en páginas web abiertas cuyos responsables eran fácilmente identificables, hasta la actual Deep Web. En estos años los pedófilos han aprendido mucho. Dice Barrera:

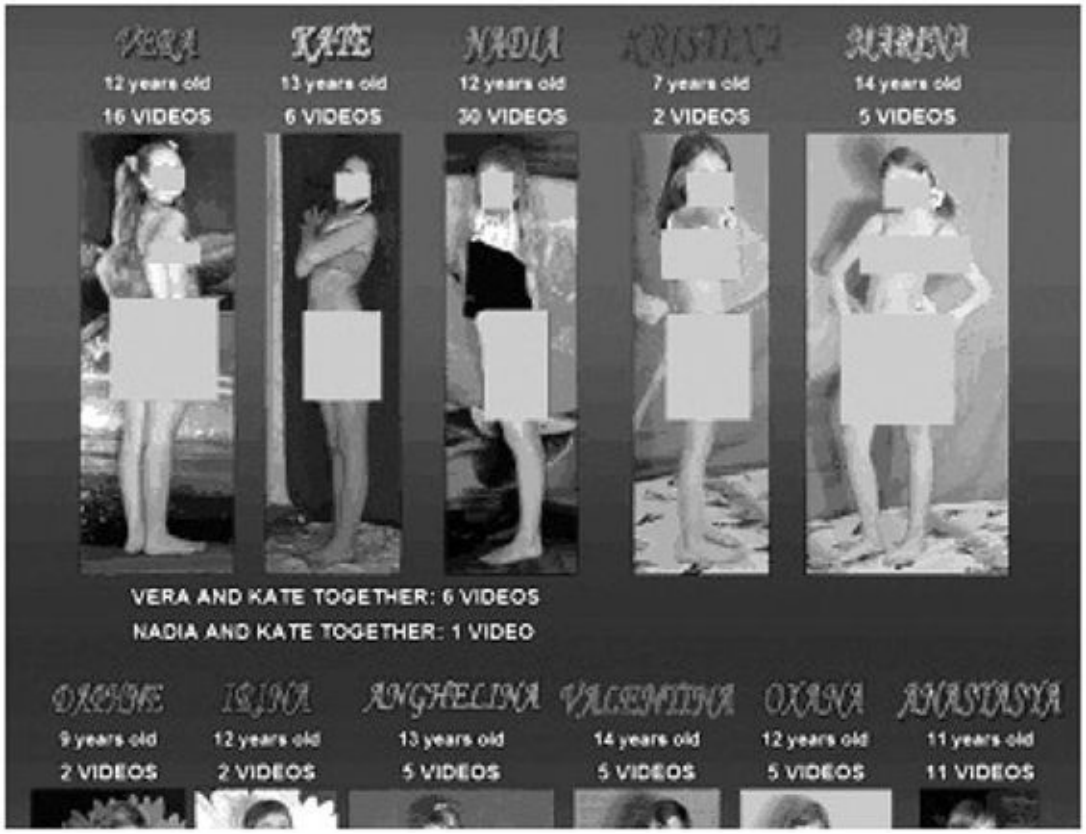
> Durante 1998 la policía inglesa en la Operación Catedral desmanteló The Wonderland Club, una asociación virtual pedófila altamente organizada que contaba con un presidente, un secretario, un comité de gestión, procedimientos establecidos para reclutar nuevos miembros y cinco niveles de seguridad destinados a impedir toda forma de acceso a sus actividades.(…)Esta red tenía presencia en al menos doce países. Para conseguir ingresar en ella, el posible candidato tenía que demostrar la posesión de al menos 10.000 imágenes de pornografía infantil. Los miembros podían tener acceso a centenares de miles de fotografías y a participar en encuentros virtuales. La policía inglesa policía detuvo a 100 miembros de este club y descubrió la existencia de más de un millón de imágenes pornográficas de niños y niñas. Solamente se han identificado hasta la fecha a una veintena de las 1.260 víctimas encontradas en los archivos fotográficos. Se capturaron más de 750.000 imágenes pornográficas de niños, así como 1.800 horas de vídeos digitales que mostraban abusos sexuales a menores. (…) Los integrantes del club empleaban un complejo sistema de contraseñas y tecnologías de codificación. Algunas de los ordenadores incautados posteriormente por la policía contenían material codificado que nunca pudo ser visto por las autoridades o presentado en los tribunales ante la imposibilidad de descifrar el código de seguridad. Un detenido prefirió suicidarse a someterse a juicio, sin saber que, al final, la policía no logró romper el código de su ordenador ni ver una sola imagen ilegal.

Pero la pedofilia en internet no es un fenómeno que se limite a los países más «desarrollados», como Alemania, Reino Unido o Francia. En España contamos con una nutrida y activa comunidad pedófila, y como prueba Barrera expone las principales operaciones de la BIT del CNP contra esa tara de la red.

> OPERACIÓN RUBER.A finales del 2004. Consiguió desmantelar una organización de pederastas en sus tres escalones: prostitución/corrupción de menores, producción/venta de pornografía infantil y la constitución de una comunidad pedófila.
>
> OPERACIÓN ARTUS. Marzo de 2002. A través de las actuaciones coordinadas con Interpol y Europoly en colaboración con Policías de Canadá, Alemania, Suiza, ReinoUnido, Holanda, Suecia o Japón, desarticuló una red que operaba a nivel mundial intercambiando pornografía infantil a través de internet.
>
> OPERACIÓN UVSINTERPOL. 2005. La BIT informa a través de la Oficina Nacional de Interpol a 41 países acerca de 400 conexiones de usuarios que poseían y compartían archivos de vídeo. Estas grabaciones contenían abusos y agresiones sexuales a dos niñas de 6 y 8 años a las que el autor de estos hechos llegó incluso a azotar con el cinturón al negarse a mantener relaciones sexuales con él.

Hay muchas más: Operación Malkone, Baleno-Iceberg, Trigger, Geminis, Kleimborg,Hydrahack, Enea, Troya, Orion, Canal Grande, Lobos…

Solo son nombres. Etiquetas con las que la Policía define una investigación sobre una red de pedofilia concreta. Pero es que tras cada uno de esos nombres se ocultan cientos de «honrados ciudadanos» europeos, occidentales, judeocristianos, blancos, que se excitan sexualmente con los abusos sexuales a menores. Solo en la Operación Carrusel: «Se practicaron 210 registros domiciliarios con el resultado de 120 detenidos y 96 imputados». Casi siempre hombres. Heterosexuales u homosexuales, pero hombres. Así que diez años después de la publicación de *El año que trafiqué con mujeres* me reafirmo en el asco y la vergüenza que siento por mi género. Aunque simpatizantes de ETA, como Sebastián Yanguas, me condenen a muerte por ello.



Silvia aboga, durante toda su tesis, por la utilización del «agente encubierto» como una herramienta especialmente eficiente para identificar y detener a pedófilos.

> La utilización de la figura jurídica del agente encubierto vendría a constituir una herramienta a disposición de la persecución del delito que permitiría la investigación desde dentro de la red criminal, circunstancia que en los delitos de pornografía infantil se revela como fundamental y determinante para la obtención de resultados. (…) No quiero que le coja por sorpresa al lector el siguiente dato: al contrario que en nuestro país, la legislación federal estadounidense contempla desde hace doce años una estricta regulación de las comunicaciones *online* y, cómo no, también del agente encubierto. En aquel país no existe un vacío legal como en el nuestro, no solo por la importancia que allí tienen las telecomunicaciones sino porque el 80% de los delitos están relacionados con internet.

Para ello menciona diferentes casos de redes de pedofilia en los Estados Unidos que fueron desmanteladas gracias al heroico, y utilizo intencionadamente esa palabra, *heroico* trabajo de agentes encubiertos:

> Un agente de la policía estadounidense infiltrado realizó un análisis forense del sitio web localizado en la URL: «http://70.85.21.233/members», el cual mostraba en su página inicial, aproximadamente, 132 imágenes consideradas pornografía infantil. Este «Sitio para Miembros» tenía un contenido total aproximado de 7 GB, consistentes en un forum para usuarios, alrededor de 9.795 imágenes, 329 archivos de vídeo y 41 archivos comprimidos tipo «zip». (El agente encubierto estadounidense, una vez realizó los pagos mediante tarjeta de crédito, recibió en el correo electrónico un mensaje cuya traducción del contenido sería: «Dulces inocentes pequeñas niñas serán pronto mujeres. Ellas aprenden ahora cómo moverse, provocar y seducir a los hombres. Mira a pequeños ángeles enseñando su belleza natural y única feminidad. Pequeñas niñas de 7 a 12 años son modelos de la gran Colección de Fotos y vídeos de Lolitas. Gran archivo de prepúberes eróticas, contenido nuevo y exclusivo. Visita la galería gratuita y descarga alguna imágenes a tu colección privada».)

Lógicamente, yo estoy cien por cien de acuerdo con la inspectora Silvia Barrera.

Sin duda este tipo de delitos son un ejemplo oportuno de cómo el trabajo encubierto es la mejor baza para identificar y detener a los delincuentes. Aunque hace falta tener unas tripas de amianto para desarrollarlo.

La inspectora Barrera, además, analiza minuciosamente los aspectos legales y penales de la pedofilia, y también el *modus operandi* de estas, sin duda, redes de crimen organizado. Así como los protocolos de seguridad y las justificaciones que argumentan para normalizar su comportamiento inmoral, perverso y criminal. E ilustra su análisis con casos tan emblemáticos como El Castillo Azul, una comunidad hispanoparlante de pedófilos *online* con más de 14.000 miembros. Sí, lo he escrito bien: 14.000 miembros…

> Este foro web es un lugar destinado a los boylovers y sus amigos para darse y recibir apoyo mutuo, y también para involucrarse en discusiones amigables: asuntos relacionados con la vida de un boylover y muchas otras cosas (…) Pronto te darás cuenta de que ya no estás solo…

Ese párrafo recoge la página de entrada a una web llena de eufemismos. Como *boylovers*. Así se denominan a sí mismos los pedófilos para dulcificar, disfrazándola de amor, lo que solo es deseo perverso. Candid, underage, kiddy, preteen12, pedo, lolita, russian, childlover, vicky, ddoggprn, child2yo (de «years old»), girl3yo… los pedófilos tienen su propia fraseología en la red, para reconocerse entre ellos.

Silvia Barrera menciona también en su tesis un tema verdaderamente preocupante para todos los padres del mundo: los sistemas de captación de menores de los pedófilos.

Ya he advertido, y lo continuaré haciendo, sobre los riesgos de las redes sociales, pero existe otro lugar donde pedófilos y pederastas buscan niños a los que pervertir. Los juegos *online*.

Recuerdo con especial emoción que durante una edición de las jornadas X1Red+Segura, en la que por cierto participó también Silvia Barrera, Blanca Tulleuda tomó el uso de la palabra tras una charla brillante de su hija. Blanca recordó cómo había descubierto que los pedófilos habían acosado en la red a su niña. Una noche se dejó abierto el ordenador en una página de un juego *online* que, como la mayoría, facilita un servicio de chat en directo a los jugadores. Al echar un vistazo a la pantalla, Blanca reconoció el nick de su hija y también los de varios de sus amigas… pero había más invitados en la sala. Jugadores que utilizaban nicks aparentemente infantiles: Juan12, Pedro13, etcétera. Sin embargo, las cosas que pedían…, el tono de la conversación… No tardó ni un segundo en darse cuenta de que eran pedófilos intentando conseguir que las niñas activasen su webcam o les mandasen fotos «picantes». Tardó más en contárnoslo a los asistentes a las jornadas, porque cada dos palabras se le quebraba la voz y se le llenaban los ojos de lágrimas.

Un juego tan popular como Second Life, explica Barrera, se ha convertido en uno de los canales de pedofilia más extensos de la red (véase también *ABC*, 17 de mayo de 2007).

Según informaciones públicas obtenidas de la prensa digital alemana e inglesa, la Policía alemana comenzó a investigar después de que un periodista, miembro del sitio, denunció que le ofrecieron participar en reuniones en las que se exhibía sexo con niños a cambio de dinero. Algunos jugadores le propusieron incluso intercambiar imágenes reales de pornografía infantil. Aunque los menores tienen prohibido el acceso a Second Life, los adultos sí pueden crearse personajes infantiles, lo que ha suscitado gran polémica. La televisión alemana denunció también que un avatar de un adulto y otro de un niño mantuvieron una relación sexual virtual. Y que un usuario que se hacía pasar por una adolescente de trece años ofrecía fotografías reales de pornografía infantil a otros usuarios.

Según la Policía inglesa, hay un espacio de juegos en Second Life, llamado Wonderland —probablemente al lector este nombre le recuerde algo— donde niños ofrecen sexo a cambio de «dólares Linden», billetes utilizados en el juego que luego pueden ser convertidos en dólares reales. La cadena británica informó también de que hay áreas en Second Life donde los jugadores son estimulados a violar y torturar a otros personajes virtuales.

Además, en su profunda investigación la inspectora Barrera analiza otros aspectos colaterales de la industria de la pedofilia en la red, como las empresas que se benefician económicamente de los pagos a los proveedores y webmaster de las webs, o como el uso que hacen los pedófilos de los anonimizadores, *remailers* y redes como TOR, FREE-NET o I2P, para ocultar su rastro en internet. Yo prefiero no comentar nada al respecto, para no dar ideas.

Como tampoco voy a decir nada sobre las explicaciones que los psicólogos pretenden encontrar a una tara emocional como la pedofilia. Creo que no tengo la fortaleza de los policías…

La inspectora Barrera intenta desarrollar el argumento de su tesis con objetividad policial. Haciendo una exposición fría y empírica de los hechos. Obviando cualquier implicación emocional. Pero, joder, es imposible. Al menos para mí. A pesar de su redacción aséptica e impecable, conforme leo no puedo sacarme de la cabeza la imagen de Mario Torres, y de las niñas mexicanas de diez, doce o catorce años que me vendía, a 25.000 dólares cada una, en el restaurante de la plaza de Cubos, en pleno centro de Madrid. Niñas «nuevitas» por las que «puedes cobrar lo que quieras». Mario conocía el negocio, y sabía que además de prostituyéndolas, esas niñas podrían generar miles de fotos y vídeos de contenido pedófilo, que adecuadamente gestionados, podrían amortizar la «inversión» en cuestión de semanas.

Porque el verdadero problema de la pedofilia en internet es que constantemente necesitan nuevos estímulos. Y «esta capacidad para producir excitación sexual —concluye Barrera— disminuye con la exposición continuada, lo que [el psicólogo Maxwell Taylor] llama tolerancia. De modo que solo así surge el síndrome del coleccionista; esta demanda constante es la que alimenta y sostiene la continua producción de material». Es decir, nuevas imágenes de abusos, o nuevos niños de los que abusar.

Para detectar el «material» nuevo, que aporte pistas sobre los productores, alguien, en alguna comisaría, tiene que haberse visto todo el material conocido, y tiene que clasificarlo, ordenarlo, buscando patrones, para después identificar las aportaciones de nuevos productores.

No me lo quito de la cabeza. ¿De qué pasta está hecho el funcionario que tiene que examinar esas fotos y vídeos? ¿Cómo soportar esa exhibición de la maldad humana en su mayor expresión sin volverse loco? ¿Cómo pueden llegar al domicilio del productor, con frecuencia un padre que abusa de sus propios hijos o hijas, y ponerle los grilletes sin sacar el arma y vaciarle el cargador en la cabeza?

¿Soy yo el bicho raro? Mientras negociaba con Mario Torres la compra de las niñas mexicanas se me pasó por la mente la idea de tomarme la justicia por mi mano. De pronto me sorprendí a mí mismo calculando cuánto tardaría en coger el vaso que estaba ante mí, romperlo con el canto de la mesa y rebanarle el pescuezo… ¿Tendrán los policías que luchan contra la pedofilia pensamientos parecidos?

—No te voy a negar que a veces te cuesta contenerte cuando les pones los grilletes —me respondió Silvia Barrera cuando se lo pregunté directamente.

Nos encontramos en una cervecería situada en el cruce de la calle de Alcalá con Jorge Juan. Apenas a diez metros del Teatro Nuevo Alcalá.

La última vez que la había visto, en una de sus conferencias, vestía el uniforme del Cuerpo Nacional de Policía y llevaba el pelo recogido en una coleta. Ahora, con el pelo suelto y vestida de sport, me costó un poco reconocerla. Se pidió una cerveza

sin alcohol, como yo, y contestó con infinita paciencia a todas mis preguntas.

—¿Cómo viniste a parar a investigación tecnológica?

—Yo estaba muy bien en Policía Judicial en Coslada, en la época del escándalo de Ginés, el jefe de la Policía Local.[152] Y el entonces comisario de Coslada, ahora jefe de la UDEF, que me conocía y sabía que yo trabajaba bien en la investigación, me preguntó cómo andaba de informática y de inglés. Yo le dije: «Jefe, con usted al fin del mundo», y me propuso venirme a delitos informáticos.

—¿Y es muy distinto? Quiero decir, si notas la diferencia entre la investigación policial convencional, en la calle, y la investigación tecnológica.

—Para empezar es muy importante saber escribir bien… Me explico. La investigación tecnológica tiene su propia idiosincrasia. Tienes que saber muy bien lo que quieres buscar y adecuarlo al delito… porque a veces ni siquiera tenemos un delito específico para eso. Saber hablar con los jueces para convencerlos de ciertas cosas, explicándoselo todo muy bien. Porque con delitos de abuso sexual a menores no hay duda; los jueces te dan enseguida el mandamiento judicial, la gente colabora, todo el mundo lo tiene claro. Pero cuando hablas de fraudes, ciberataques y demás, tienes que saber explicarlo muy bien para que entiendan qué es lo que necesitas. Igualmente, cuando acudes a la red social o al proveedor de servicios, debes saber muy bien con quién tienes que hablar, qué tienes que pedir. Luego la investigación en sí es muy compleja. Y esto no se aprende ni en la universidad de Ingeniería informática, ni en la de Derecho, ni en Criminología… Solo se aprende aquí. En el día a día.

Silvia dirige el Grupo de Tratamiento de Evidencias Digitales. No solo la unidad de internet, sino drogas, blanqueo de capitales, homicidios, desapariciones, etcétera. Traducido a operativa policial, es el análisis y volcado de la información de los dispositivos que se intervienen en las investigaciones.

—Pues imagino que no daréis abasto, porque ya todo pasa por la red.

—Todo. Ahora, en un delito como el blanqueo ¿dónde está la prueba? Pues en un ordenador, o en un *pendrive*. Con las drogas, igual: las pruebas están en el contenido de los correos, las conversaciones de WhatsApp o las llamadas telefónicas. En homicidios lo mismo: lo primero que se busca en el sospechoso son sus redes sociales, registros telefónicos y sus correos electrónicos. Todo tiene un componente tecnológico.

Antes de aterrizar en la dirección de Tratamiento de Evidencias Digitales, la inspectora Barrera estaba destinada en investigación de redes. Hace muchos años que Twitter se convierte, con frecuencia, en la escena del crimen.

—Tú vienes de redes, y sabes que ahora la comunidad está muy revuelta con la reforma de la ley que entra en vigor el 1 de julio… ¿Cómo os afecta a vosotros?

—Policialmente en nada. Bueno, salvo algunos delitos, como la difusión de vídeos íntimos, por ejemplo el vídeo de Olvido Hormigos, ¿te acuerdas? —yo asiento con la cabeza—, grabaciones que se hacen en la pareja de forma consentida, pero

luego se difunden de forma no consentida. Antes no se consideraba delito, eran infracciones, pero ahora sí estará tipificado como delito. O el delito de acoso, que ahora se contempla de forma específica. El acecho reiterado en las redes sociales. Y luego, en la reforma de la Ley de Enjuiciamiento Criminal, sí hay cosas que nos afectan, como la figura del agente encubierto.

—Tú en tu tesis lo defiendes mucho.

—Hombre, es que para mí, en temas de menores, es necesaria. La pedofilia en internet es una pirámide. Arriba está el productor, y por debajo la gente que la consume y la demanda. Si hay veinte o treinta productores, que consiguen que haya millones de usuarios consumiendo esa pornografía, vamos a por los productores. Pero esa gente toma muchas medidas de precaución. Son comunidades muy cerradas. Hay que llegar a ellos y ganarse su confianza. Como en la vida real. Tienes que demostrar que eres uno de los suyos, y la única manera, en su caso, es intercambiando material. Y ahí está el problema. Se autoriza el intercambio al agente encubierto, pero nadie habla del tipo de imágenes que se van a enviar. ¿Y de dónde sacamos esas imágenes? ¿Utilizamos imágenes que hayan sido intervenidas en una operación anterior y que probablemente ya conozcan? No podemos usar imágenes de jóvenes aunque aparenten menor edad de la que tienen porque lo que quiere esta gente son imágenes de extrema dureza, cuanto más jóvenes mejor. Te hablo incluso de niños de meses…

Silvia acababa de poner el dedo en la llaga. En sus conclusiones subraya que «el agente encubierto es urgentemente necesario»; sin embargo, y como explica a la perfección en su tesis, la única manera de infiltrarse en las comunidades de pedofilia más influyentes, pasa por enviar «material» (es decir fotos y/o vídeos de abusos sexuales a niños) que ellos no conozcan. Y si utilizar ese tipo de documentos en una investigación policial se nos antoja inmoral y difícilmente justificable, obtenerlo supone un problema casi irresoluble.

Otro de los grandes problemas a los que se enfrentan los policías que investigan los delitos tecnológicos son los proveedores. Y esto es muy interesante, porque lo que para la comunidad hacker es una escandalosa pleitesía de los gigantes de internet —como Google, Yahoo, Microsoft o Facebook, entre otros— para con las agencias de Inteligencia norteamericanas, a ojos de Silvia Barrera es una colaboración envidiable. Ni siquiera yo me había parado a analizar desde esta perspectiva las revelaciones de Edward Snowden…

—Esta es mi lucha, conseguir la colaboración de los proveedores —me explicó la inspectora—. Cuando tú investigas un delito, sigues los datos, y los datos pasan por los proveedores. Pasan por Twitter, por Facebook, por Gmail. No es como cuando investigas la escena de un crimen en el mundo real, que tienes ahí, en ese lugar, la sangre, las huellas, el cadáver… Aquí la prueba está en la red. Si yo quiero investigar a un usuario que ha colgado un vídeo donde dice que te van a matar, por ejemplo, ese vídeo está en YouTube y YouTube está en Estados Unidos. Pero en España no existe una legislación que obligue a YouTube a darte esa información. Y si no quieren darte

esa información, no te la dan, te pongas como te pongas. De hecho, no lo hacen. Se pasan por el forro las peticiones policiales.

—¿Me lo dices en serio? —repliqué realmente sorprendido.

—Claro. Casi siempre es así. ¿Te acuerdas, por ejemplo del caso de la presentadora Lara Siscar? —Yo asentí, conocía perfectamente el acoso que vivió en Twitter la presentadora de TVE durante meses—.[153] Pues lo podíamos haber resuelto en un mes, pero tardamos ocho. Porque Twitter se negó a colaborar. Les daba igual que un juez hubiese visto indicios de delito. Twitter se niega a dar las IP de los acosadores. Dicen que los datos están en los Estados Unidos, y que el juez debe enviar una comisión rogatoria para que un juez americano ordene a Twitter facilitar esa información. Un proceso largo, carísimo e innecesario. Y una forma de intentar disuadir a la justicia. Y mientras, pasan los meses, y los acosadores siguen atormentando a la víctima…

Cuando me despedí de la inspectora Barrera, volví a tener esa sensación de vacío. De amargura. De impotencia. Internet es un espacio inmenso. Colosal. Gigantesco. Como el inescrutable océano al que se enfrentó Colón. Como el desconocido desierto del Sahara que exploró mi inspirador Ali Bey. Como el inconmensurable espacio cósmico al que ahora comienzan a asomarse nuestros astronautas. Y como ese universo en expansión, la red también crece y crece cada día.

Si nuestras fuerzas de seguridad se ven limitadas para investigar los delitos que se producen en ese inmenso lugar que es internet, porque los grandes señores de la red restringen su capacidad de investigación tecnológica, ¿qué les queda? Pues no tienen más remedio que convertirse en hackers. Utilizar el pensamiento lateral. Buscar otras opciones…

Operación Cool Daddy: cazar a un monstruo en ocho días

A David Pérez, uno de los policías de la Brigada de Investigación Tecnológica del CNP a las órdenes de Silvia Barrera, no le gusta recordarlo. Todavía se le atraganta. Fue uno de los casos que vivió con mayor intensidad, y un ejemplo perfecto de lo qué es realmente la pedofilia en internet. Yo me negaba a creerlo. Hasta que vi las evidencias. Me parecía inasumible. El argumento de los guionistas de Hollywood para una peli de suspense, pero inimaginable en el mundo real. Pero existen. Personajes como H. J. no pertenecen a la ficción.

En abril de 2011 la Policía alemana localizó en las redes de pederastas de la Deep Web un vídeo que no aparecía en las bases de datos. Era «material» nuevo. El vídeo lo había subido a la red alguien que se identificaba como Chriss, y explicaba que los abusos los había cometido él, con sus hijos y con los hijos de su expareja. Los niños tenían entre diez y cuatro años. En el texto que acompaña el vídeo, facilita una dirección de email que solo permanecerá operativo del 28 de febrero de 2011 al 30 de abril.

La Policía alemana —que inicialmente se hizo cargo del caso ya que los actores hablaban alemán— encuentra en las imágenes indicios de que los abusos se podían estar produciendo en España, y remite el vídeo a la BIT del CNP. Era el 13 de abril de 2011. Y comienza la cuenta atrás. Saben que los proveedores de internet, como me explicaba la inspectora Silvia Barrera, no van a colaborar o tardarán meses. Y cada día que pasaba, se prolongaría el infierno de aquellos cuatro niños. Así que los agentes de la BIT echaron mano de todo su ingenio para hackear al pedófilo, utilizando las técnicas policiales convencionales. Y muchas, muchas, muchas horas.

—Cuando nos llegó el vídeo —me explica David— lo analizamos con lupa. Por un lado teníamos abusos que se producían en lo que parecía un camarote de un barco, y por otro abusos que se realizaban en lo que parecía un chalet o una casa grande. En total aparecían cuatro niños, dos niños y dos niñas, muy pequeñitos. Entre cuatro y diez años… Los pedófilos con frecuencia son bisexuales. El placer del control prima sobre el sexo de la víctima.

En las imágenes rodadas en el barco, los niños tienen la piel bronceada, por lo que los policías deducen que se han grabado en verano. Pero en las tomadas en el chalet, los niños tienen la piel más clara y se cubren con mantas. Lo que sugiere que fueron tomadas en invierno. Esto significaría que no se trata de abusos puntuales sino prolongados en el tiempo…

El abusador oculta la cara, así que los policías analizan otras partes de su cuerpo, como las manos, manchadas de grasa. Parecen manos de trabajador manual. Es una pista. Otra, el tatuaje de un lagarto que tiene en el hombro derecho. El camarote donde se consuman parte de las violaciones y sus peculiares cortinas también son una

pista. Como la fecha, «26/12/2010», impresa en uno de los fotogramas; una sábana que parece de mascota; un objeto rectangular con la palabra *chef;* los calcetines que lleva el abusador… Los agentes elaboran una primera hipótesis: el pederasta puede ser alguien encargado del mantenimiento de barcos.

—En una de las imágenes vimos una gorra con una expresión en mallorquín: «ca'n», así que enfocamos la investigación en Mallorca. Se acercaba la Semana Santa, es decir, las vacaciones escolares, y nos daba mucho miedo que el abusador pudiese aprovecharlas para continuar perpetrando las violaciones, así el 14 de abril Luis y yo —se refiere a su superior entonces en la BIT, Luis García Pascual— volamos a Mallorca y empezamos a hacer el trabajo policial convencional, sobre el terreno, mientras nuestros compañeros seguían haciendo el trabajo informático desde Madrid.

En Mallorca, Luis y David reciben la colaboración de la Policía Judicial mallorquina para, divididos en tres equipos, atacar tres frentes. Uno de los grupos busca por los puertos. Otro visita las oficinas de venta de yates para tratar de identificar el barco que aparece en los vídeos. El tercero, con las capturas de vídeo en los que se ve perfectamente la cara de los menores, peinará los colegios de Mallorca con alumnos alemanes, intentando identificar a las víctimas.

En uno la secretaria cree reconocer a las dos niñas… Una sigue en el colegio… La identifican… Falsa alarma. No es ella. Continúan buscando.

—Llegó el viernes —continúa David— y no habíamos conseguido nada. Y se acercaban las vacaciones, así que estábamos muy angustiados. Te ibas a la cama en el hotel con el runrún en la cabeza todo el tiempo. Qué podemos hacer… qué podemos investigar… Y me levantaba por la mañana, todavía con los ojos pegados, y enseguida llamaba a Luis: Luis, Luis, se me ha ocurrido esto… Estábamos todo el día pensando en lo mismo.

David y Luis regresaron al colegio alemán. Había cambiado de propietarios, así que intentarían localizar a la antigua directora por si ella pudiese reconocer a la otra niña.

16 de abril. Los alemanes colaboraron. Como decía Silvia, con delitos como la pedofilia siempre lo hacen. Y Luis y mi amigo tuvieron suerte. La antigua directora del colegio estaba en la isla. Así que fueron a verla. Y hubo suerte. La directora todavía conservaba algunas cajas con las fichas escolares, así pudieron identificar a las niñas y a su presunto agresor: su padre. H. J.

—Con el nombre del padre nos salieron muchas empresas, pero todas tenían domicilios falsos o antiguos. Perdimos varios días vigilando esas empresas, identificando a la gente que entraba o salía, pero nada, todo eran callejones sin salida.

Con el nombre del presunto pederasta pueden recomponer la historia. Dos de los niños eran hijos de su anterior pareja, ya trasladada a Alemania. Pero el padrastro abusó de ellos antes. Los otros son sus propios hijos… y todavía viven en Mallorca.

Descubren además que H. J. figura como propietario de un barco: el *Beryll,*

matriculado en Hamburgo. Creían que ya lo tenían, pero no es el mismo barco que aparece en los vídeos. No importa. Los agentes continúan investigando.

17 de abril. En Madrid descubren una pista en el BOE. Unas ayudas a otro colegio con alumnos alemanes les ofrece una nueva pista.

18 de abril. Faltan dos días para las vacaciones. Luis y David saben que el pedófilo las aprovechará para consumar más violaciones. Así que se disfrazan de operarios de la construcción y entran en el colegio como si estuviesen haciendo reparaciones para intentar identificar a los niños sin llamar la atención de los padres ni de los educadores. Y entonces ocurre algo mágico.

—Fue la casualidad. Recuerdo que era la hora del recreo. Y en un momento dado, noto que me tiran de la camisa. Me giré… y era ella… la niña pequeña que aparece en los vídeos… Me dijo: «Vosotros sois los que venís a arreglar el colegio»… —Al llegar a este punto, a David se le quiebra la voz. Para unos segundos para tomar aire —. Me… me impresionó mucho. Porque todo lo que llevas hasta ese momento de la investigación lo sueltas cuando ves allí a la personita indefensa que es… La verdad es que impacta… Lo podrás contar mil veces pero te juro que nadie sabe lo que se pasa en ese momento, te juro que no he vuelto a ser el mismo… De hecho, al año me fui de menores y me metí en lo mío, la parte técnica.

Joder si impacta… Yo no puedo imaginar lo que tuvo que sentir mi amigo David al encontrarse cara a cara con la pequeña a quien había visto sometida a abusos y vejaciones por su propio padre.

A partir de ahí todo fue rápido. Siguieron a la madre, que vive muy lejos del colegio, y vigilaron la casa durante horas, pero H. J. no estaba allí.

Descorazonados, regresaron al hotel, pero de nuevo la Providencia decidió echarles un cable. Ya de noche les telefoneó la directora del colegio. La madre de las pequeñas acababa de llamarla. Mañana no podrá ir a recoger a sus hijas: irá H. J. …

No es casualidad. Ese día terminaban las clases. El hijo de puta acudía a buscar a las niñas porque quería tener tiempo para satisfacer sus deseos. Se había ofrecido amablemente para hacerse cargo de ellas durante toda la Semana Santa. La intuición policial era correcta.

Veinte policías de incógnito rodeaban esa mañana el colegio. Lo detuvieron en cuanto se bajó del coche.

—Luis me llamó y me dijo: «¡Es él, es el padre!». Y lo hicimos todo muy rápido. No queríamos que lo viesen los niños. Quince segundos y el tipo ya estaba esposado y metido dentro del coche. Casi nadie se enteró…

En el registro de su casa incautaron todos los soportes digitales: ordenadores, tarjetas de memoria, discos duros… Allí estaba todo. En el momento de grabarse el vídeo que inició esta investigación, la niña pequeña tenía solo cuatro añitos. Pero el hijo de puta abusaba de ella desde que tenía uno. Todo mi escepticismo se fue a tomar por culo ante el peso de estas evidencias. La pedofilia es una realidad. Brutal. Enorme. Cercana. Y mucho más frecuente de lo que podríamos imaginar.

H. J. aceptó todos los cargos, y una condena a diecisiete años de cárcel. Pactó con la Fiscalía. De lo contrario, podrían haberle caído cincuenta. Ojalá en prisión alguien le pueda hacer comprender, de forma elocuente, lo que sintieron sus hijos cuando los violaba.

Pero lo que no entró en prisión fueron esos vídeos. Continúan circulando por la red con otros millones de imágenes de abusos sexuales a menores. César Lorenzana tiene razón. Eso no es pornografía. Es otra cosa.

Y cada vez que un pedófilo se masturba con esas imágenes, es como si los cuatro hijos e hijastros de H. J., J., M., L. y D., volviesen a ser violados.[154]

Supongo que David pudo descansar, por primera vez en esa frenética semana, la noche de la detención. O quizá no. Quizá aquellas imágenes le persigan siempre, incrustadas a fuego en su retina. Como a mí. Sin embargo, David no duraría mucho más en la BIT. La burocracia institucional y la jerarquía no suelen gestionar con demasiada lucidez el talento de sus funcionarios… Antes de que terminase 2015, David abandonaría la Policía para continuar su trabajo en la empresa privada. David fue hacker antes que funcionario. Y sin duda lo seguirá siendo hasta que se muera. Nuestros cuerpos policiales deberán esforzarse más para conservar sus talentos…

Son precisamente los hackers, los investigadores informáticos, los que ahora han venido en ayuda de la Policía para luchar contra la pedofilia en la red. Un ejemplo oportuno es el programa Negobot, desarrollado por informáticos de la Universidad de Deusto. Como su nombre indica, Negobot es un *bot*, es decir, un programa que interactúa con los usuarios como si fuese una persona real.

El test de Turing, diseñado por el genio que descifró la máquina Enigma, está considerado la prueba de fuego de la inteligencia artificial. ¿Puede una máquina pensar? Para responder a esa pregunta todos los años, desde 1954, se celebra un experimento. Un grupo de científicos de la Royal Society dialogan con un interlocutor y tienen que averiguar si hablan con un ordenador o con una persona real. En 2014, por primera vez en la historia, un *chatbot* (un programa diseñado para charlar *online*), bautizado como Eugene Goostman, consiguió convencer al 33% de los jueces de que era un niño ucraniano real de trece años.[155]

Siguiendo esa línea de trabajo los investigadores de Deusto diseñaron un *bot* que simula ser una niña de catorce años, programado para detectar comportamientos sospechosos en los chat y lo han soltado en la red. Buena caza…

ABRIL DE 2015
SILVIA HIERRO NO EXISTE

«En la política, hay que conseguir el apoyo de las mujeres; el apoyo de los hombres viene solo, después.»

Adolf Hitler, recogida por su secretaria Christa Schroeder

Localizar la identidad real de MarkoSS88 se había convertido hacía mucho en un reto personal. Y quienes me conocen saben que no me gusta perder ni al parchís. Pero si Markos era lo suficientemente hábil como para borrar su rastro digital, quizás su exnovia no lo fuese tanto.

Así que decidí intentarlo por ahí. Y una vez más, tuve ayuda. Manu estuvo allí el 5 de marzo de 2014. En el campus de la Universidad Rey Juan Carlos en Vicálvaro. Sentado junto a Ángel, compañero suyo y buen amigo mío. Donde todo esto comenzó. Y cuando se enteró de lo que estábamos descubriendo, se implicó en cuerpo y alma en la investigación. Todavía hoy no sé cómo agradecerle las horas, días y semanas que robó a su tiempo libre para ayudarme a desentrañar el enigma de MarkoSS88.

Manu fue quien me dio la noticia. Nos citamos en la última planta de El Corte Inglés de la plaza de Callao, en Madrid. Allí arriba situaron una cafetería que por las noches habilita una terraza, en plan *chillout,* con unas vistas privilegiadas de la Gran Vía y de todo Madrid.

—No lo entiendo, Toni —me dijo mientras me mostraba el informe con sus pesquisas—. Silvia Hierro no existe.

Yo tampoco lo entendía. Aquello era absurdo. Silvia Hierro tenía una dilatada vida digital documentada en Facebook, Twitter y Ask como mínimo. Manu es un profesional excepcionalmente cualificado. Ha participado en la investigación de los acontecimientos más trascendentes de la historia de España, pero los responsables de la cafetería de El Corte Inglés de Callao tenían que haberse pasado con la cafeína en su Coca-Cola, porque aquella afirmación era absurda. Silvia existía, vaya que si existía, había docenas de fotos suyas en internet posando con MarkoSS88.

—No puede ser, Manu, estás equivocado… Mírala —le dije mientras le mostraba una foto del perfil de Silvia Hierro en Twitter en la que posaba radiante al lado de su ya exnovio MarkoSS88—. ¿Me estás diciendo que esta persona no existe?

—No, Toni, te estoy diciendo que no existe ninguna Silvia Hierro de

diecinueve años, que estudie Medicina en ninguna facultad de ninguna universidad de Madrid. Es más, te digo que no existe ninguna Silvia Hierro de diecinueve años en toda España.

Una vez más, en esta investigación, mi rostro debió de adoptar la apariencia de una boca de metro. Con la boca abierta, y los ojos también. Como si tuviese que recibir la máquina de la línea 4, con todos sus vagones y pasajeros.

—Pero… no entiendo…

—Lo que te estoy diciendo. Primero comprobamos las universidades. Y al

no encontrar nada, fuimos abriendo el perímetro de la búsqueda. Primero en Madrid, y luego en el resto de España. Míralo tú mismo…

Allí estaba la evidencia incuestionable. Según INEbase y las bases de datos demográficas y de población del Instituto Nacional de Estadística, el registro del padrón municipal de Madrid solo tenía registradas a tres Silvia Hierro. Una nacida en 1992, la otra en 1968 y la tercera en 1965. En toda España, el padrón solo tenía constancia de quince. Y todas habían nacido antes de 1951 o después de 1985. Ninguna coincidía con el perfil de la novia de MarkoSS88.

—Te lo repito, no existe ninguna mujer que se llame Silvia Hierro y que tenga esa edad. ¿Se puede saber dónde te estás metiendo?

—No lo sé, Manu, no lo sé… Pero gracias por la gestión…

Me quedé unos minutos absorto, contemplando desde lo alto la Gran Vía madrileña. Desde aquella novena planta, las personas se veían pequeñitas. Las observé mientras caminaban por la calle más emblemática de la capital. A la derecha, el edificio color crema donde Mercedes Dantés, el enigmático personaje interpretado por Megan Montaner, planifica su venganza en la serie *Sin Identidad* de Antena 3, protegida tras una vida totalmente ficticia. Enfrente, el Teatro Callao.

Justo allí, sobre aquel mismo asfalto, muchos años atrás caminé con mis camaradas de Hammerskin, tras asistir a la proyección de un documental sobre la División Azul en el Teatro Callao. Me recordé a mí mismo, con la cabeza rapada, las Dr Martens y la cazadora bomber llena de pins y parches de UltraSSur, Blood & Honour o Hammerskin, caminando por aquella misma calle al salir de la proyección. Recordé la sensación de poder que experimenté cuando todas aquellas personas que cada día atestan la calle más céntrica de Madrid agachaban la cabeza, miraban hacia otro lado o se cambiaban de acera a nuestro paso. Recordé aquella embriagadora convicción de que las calles eran nuestras. Eso mismo tenía que haber experimentado MarkoSS88 en alguna ocasión. Pero si su novia no existía… ¿quién coño era entonces la chica que aparecía en aquellas fotos?

Capítulo 17
RootedCON y las vulnerabilidades de la banca

«Porque nada hay oculto, si no es para que sea manifestado; ni nada ha estado en secreto, sino para que salga a la luz. Si alguno tiene oídos para oír, que oiga.»

San Marcos 4:22

RootedCON

Israel Córdoba fue muy amable al invitarme. La Rooted probablemente es la conferencia más importante sobre hacking de todas las que se celebran en España. No solo por la calidad de sus participantes y por las vulnerabilidades que se dan a conocer en cada una de sus ediciones. También por el número increíble de participantes. En la Rooted de 2015, más de 1.300 interesados en la seguridad informática nos reunimos bajo un mismo techo. El del Centro de Congresos Príncipe Felipe, ubicado en el hotel Auditórium, de Madrid.

—Yo voy a participar en una mesa redonda que creo que te va a resultar especialmente reveladora. Se titula «¿Tiene que dar alguien el carnet de hacker?».

Por supuesto acepté. No me la perdería por nada del mundo. Sin embargo, Israel no asistiría a todas las conferencias. La dilatada agenda profesional de Aiuken, y que es un veterano de la vieja escuela al que poco nuevo podían enseñar la mayoría de los participantes, hizo que acordásemos vernos en la sala de conferencias cuando él acudiese para el panel en el que participaba. Yo sí quería asistir a todo, aunque todavía no sospechaba la sorpresa que me deparaba el destino, y que haría realmente incómoda mi presencia en el auditórium más de uno o dos días.

Cuando Israel me dio la dirección, no lo podía creer.

—Joder, no puede ser…

—¿Qué pasa? —me preguntó Israel con lógico desconcierto.

—No, nada, nada —mentí para desviar la conversación—, que está a tomar por saco. Pensé que estaría en el centro de Madrid.

El hotel Auditórium está situado en el número 400 de la avenida de Aragón, muy cerca del Aeropuerto de Barajas. Exactamente al otro lado de la carretera, justo enfrente, está la calle Ezequiel Peñalver, en cuyo número 10, un antiguo burdel, se erige el Club House del capítulo Madrid de los Ángeles del Infierno que yo tan bien conocía.

En otras palabras, tres años después iba a regresar al mismo lugar que había visitado durante la investigación de *Operación Princesa*, para pasarme tres días rodeado de hackers, a solo unos metros del local de los Hell’s Angels de Madrid. Sí, definitivamente iba a poner a prueba mi sangre fría.

Los Ángeles del Infierno, que obviamente no habían leído *Operación Princesa*, habían reaccionado muy mal a la publicación de mi novela. En Estados Unidos habían sufrido varias infiltraciones entre sus filas a cargo de agentes del FBI o la ATF, y no llevaban bien lo de los *insider*, pero en España jamás les había ocurrido. Y que un periodista se hubiese atrevido a colarse en su mundo, con una cámara de vídeo, les había enfurecido más allá de lo razonable.

No importa que mi descripción sobre el mundo de los MC 1% hubiese sido escandalosamente objetiva. Ni que realmente hubiese llegado a sentir un afecto sincero por alguno de sus componentes. De todos los Motorcycle Club que conocí

durante esa investigación, los primeros en reaccionar agresivamente fueron los Hell's Angels. Y eso a pesar de que otros MC, como Pawness, pudiesen tener más razones para enfadarse. Al fin y al cabo, durante esa infiltración llegué a encontrarme con viejos camaradas como Fabián, uno de los Hammerskin contra los que declaré en el juicio, y que años después volvería a toparme, ahora como presidente del capítulo de Tarrasa de Pawness MC. O Juan Molina, el mediático cura que participó en la edición 12+1 del *reality* Gran Hermano, que tampoco se sintió muy cómodo con las informaciones que publiqué sobre su motoclub. Pero al menos Molina se puso en contacto conmigo para pedirme que suavizase el tono de mis artículos, y tuvimos una relación muy cordial.[156]

Yo no soy ningún valiente. Y confieso que cuando conducía hacia el hotel Auditórium, el 5 de marzo de 2015, no estaba tranquilo. No solo porque justo ese día se cumplía un año del incidente de MarkoSS88 en la Rey Juan Carlos, sino porque además no podía quitarme de la cabeza que la última vez que había recorrido esa avenida había sido para visitar el Club House de los Ángeles del Infierno, y era consciente de que podía cruzarme con ellos en cualquier momento.

Pero la Providencia no estaba contenta con eso, y decidió apretar un poco las tuercas para calibrar mi capacidad de tensión. Porque lo que ocurrió en cuanto llegué a la RootedCON resultaría absolutamente increíble, de no estar grabado.

Se suponía que iba de incógnito. Nadie, absolutamente nadie a excepción de Israel Córdoba, sabía que yo pensaba asistir a la Rooted. Y me había molestado mucho en que así fuese, tras descubrir que mis viejos hermanos de asfalto de los 81 estaban al otro lado de la avenida.

Aparqué la moto al lado de la puerta principal. El aparcamiento del hotel estaba absolutamente atestado y, de haber ido en coche, probablemente tendría que haber buscado un hueco a varias manzanas del hotel. Cientos de jóvenes y no tan jóvenes hackers habían llegado desde todos los rincones del planeta, para participar en la nueva Rooted. «Será fácil pasar desapercibido», pensé antes de encadenar el casco a la moto y entrar en el hotel siguiendo a un grupo de jóvenes que parecían salidos de un episodio de *Big Bang Theory.*

Cruzamos el vestíbulo principal del hotel, hacia la derecha, y en el primer pasillo, hacia la izquierda. Cientos de participantes se agolpaban ya en las entradas del Centro de Congresos Príncipe Felipe, para ir acomodándose poco a poco en el enorme anfiteatro donde se impartirían las conferencias.

En cuanto pude entrar en la colosal sala de conferencias, busqué un sitio discreto en la última fila. Cerca de la puerta. Por si había que salir corriendo.

Un par de jóvenes que parecían recién llegados de Silicon Valley charlaban animadamente, y pensé que era un lugar tan bueno como otro cualquiera para establecer mi base de operaciones. Quizá, pensé, pueda entablar conversación con ellos y aprender algo, tienen pinta de hackers…

Prometo solemnemente que lo que ocurrió a continuación sucedió tal y como

relato. En cuanto me senté a su lado puse la oreja, imaginando que aquellos chicos estarían discutiendo sobre algún tipo de *malware*, sobre un ataque de Zero Day o sobre la última operación hacktivista de Anónymous… Ni de coña. Nada más lejos. Estaban hablando de mí.

—Te digo que Antonio Salas no existe. Eso es un invento de la editorial. Son varios autores que firman con el mismo nombre para vender más libros, pero son un grupo, te lo digo yo. Un tío solo no puede hacer eso.

—Y yo te digo que no. Yo me he leído alguno de sus libros y te cuenta cómo va haciendo cada cosa. Paso a paso. Y es un tío solo…

No, no podía ser. Era imposible. Aquello no podía estar pasando… No era la primera vez que me encontraba en una situación similar. Lo único bueno del anonimato es que puede darse la circunstancia de que asistas a conversaciones sobre ti, sin que tus interlocutores sospechen que estás presente. Y esa es la única forma de averiguar lo que opinan de verdad.

De hecho, la mayoría de mis amigos más cercanos, y buena parte de mi familia, no sabe que yo soy Antonio Salas. Y en alguna ocasión, sobre todo cuando aparece un nuevo libro o reportaje en televisión y se crea un cierto revuelo mediático, se ha dado la circunstancia de que mis propios amigos o familia debata sobre si el tal Salas es o no es real, sin imaginar que me tienen sentado a la misma mesa. Pero en la Rooted, con el Club House de los 81 tan cerca, no me sentía con ánimo para seguir ese juego.

Discretamente me levanté del asiento y recorrí el pasillo superior del salón de actos, hasta el otro extremo de la sala. Busqué un asiento pegado a las escaleras, al lado de la pared, y me acomodé allí, sin perder de vista a los empollones que seguían discutiendo tan animados sobre si yo existo o soy un producto editorial. Por un instante pensé que era una broma de Israel Córdoba. Quizá eran dos de los trabajadores de Aiuken y les había pedido que me vacilasen un rato… Pero no, no tenía sentido. Israel había sido exquisitamente discreto hasta ese momento. Jamás se le había escapado ni una palabra sobre quién era yo o lo que estaba haciendo. Y además, había sido yo quien había escogido aquel asiento en la sala…

Estaba abstraído con esos pensamientos, cuando de pronto volvió a ocurrir. No me lo podía creer.

—Pues yo sé de buena tinta que Antonio Salas se tuvo que hacer una operación de cirugía estética para que no lo reconociesen. Como el poli ese que se infiltró en ETA. El Lobo…

—Anda ya, tía, qué dices. Seguro que este se lo inventa todo sin moverse de su ordenador. ¿No has visto lo que dice aquí…?

Empecé a sentirme realmente incómodo. Era imposible, pero justo en la fila inferior a la mía, un chico y una chica también estaban discutiendo sobre mí. ¿Qué probabilidades podía haber de que ocurriese algo así por azar?

Me notaba paranoico. Comencé a mirar a todos lados en busca de una amenaza.

Quizá, de alguna forma misteriosa, los Ángeles del Infierno se habían enterado de que iba asistir a la Rooted y habían desplegado a todos sus *prospects* para intentar volverme loco antes de partirme la cabeza… Pero eso tampoco tenía sentido. Si de verdad hubiesen sospechado que estaba allí, me habrían emboscado antes de entrar.

La pareja situada en la fila inferior continuaba charlando, y de pronto el chico señaló algo en la revista que tenía en las manos… Era una foto mía. Me eché hacia delante para intentar averiguar qué publicación era, y no fue difícil. Reconocí inmediatamente el ejemplar de la revista *ONE* del mes de febrero anterior.[157] Y entonces me di cuenta de que a la derecha de aquella pareja había otro grupo ojeando la misma revista. Y más abajo también. Y al girar la vista hacia la entrada, me di cuenta de que casi todos los participantes en la Rooted que continuaban entrando en el auditorio, llevaban un ejemplar con el mismo número 12 de la revista *ONE*. Un número dedicado a los «espías» y profesiones afines, en el que me habían dedicado ocho páginas.

Me levanté de mi asiento y salí de la sala en dirección contraria al público que llegaba. Quería averiguar de dónde lo sacaban todos los asistentes. Y no fue difícil. Sobre varias mesas situadas junto a una de las columnas, había cientos y cientos de ejemplares del número del mes anterior de la revista *ONE,* que la editorial había obsequiado a la organización de la Rooted para que cada asistente pudiese tener la suya.

«Tiene narices que justo hoy, y aquí, regalen una revista en la que me dedican tantas páginas…», me dije. Esa era la razón por la que algunos participantes estaban comentando mi trabajo. No existía ninguna broma de Israel Córdoba ni de nadie, ni ninguna conspiración de los Ángeles del Infierno. Como casi siempre, la solución al problema era la más sencilla.

Saqué la cámara y volví a grabar el recorrido de la entrada, hasta aquella montaña de revistas, y luego hasta el interior del auditorio donde muchos de los participantes todavía debatían algunos artículos, incluyendo la entrevista al periodista enmascarado que tenían a unos centímetros. «Si no lo grabo —concluí—, no se lo creerá nadie».

En todo caso, el mal trago con el que comenzó la Rooted no tardaría en diluirse. Allí, entre aquellas paredes, se habían concentrado algunos de los mejores cerebros del hacking internacional. Y yo estaba allí para aprender de ellos. Lo demás ya no importaba.

Vulnerabilidades

En el mundo de la seguridad informática, la palabra *vulnerabilidad* hace referencia a una debilidad o agujero de seguridad en un sistema, que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. Y, por desgracia, todos los sistemas tienen alguna.

Para un usuario de internet, sin la menor formación técnica como es mi caso, esas vulnerabilidades suenan como los nombres de grupos de rock, o los títulos de películas de ciencia ficción: Clickjacking, Cross Site Request Forgery, SQL Injection, Cross-Site scripting, Desbordamiento de búfer… Cuando no sabes qué cojones es el búfer, resulta difícil entender su desbordamiento.

A diferencia de eventos más divulgativos como la CyberCamp, la Rooted y otras CON parecidas (Mundo Hacker, Navaja Negra, No cON Name, etcétera) son más técnicas. Aquí es donde se conocen las nuevas vulnerabilidades descubiertas por hackers españoles. Y en ocasiones el alto contenido técnico de las conferencias dificulta mucho su seguimiento para un simple usuario.

De hecho, ese fenómeno se produce en cualquier conversación entre hackers en la que podía introducirme. Recuerdo que tras su participación en el panel, Israel Córdoba me invitó a acompañarle. Varios de los participantes de la Rooted habían acordado comer juntos en un restaurante situado al otro lado de la carretera, más cerca aún del Club House de los Ángeles del Infierno, con algunos de los asistentes al evento. «Ven con nosotros, Toni, te encantará ver cómo hablan y cómo se relacionan los hackers lejos de la pantalla del ordenador.» Y como siempre, Israel tenía razón.

Aunque me pasé la comida en tensión, atento al sonido de los motores que llegaban al restaurante por si reconocía las Harley de mis antiguos hermanos de asfalto, la reunión resultaba un lujo del que pocas veces puede disfrutar un periodista. Allí estaban algunos de los principales profesionales del sector, pero también un grupito de jóvenes hackers. Jóvenes pero brillantes, que pronto se enzarzaron en apasionados debates sobre cuestiones técnicas que escapaban a mi comprensión. No importa que les expliques que no estás a su nivel. Por mucho que intenten evitarlo, en cada frase emplean infinidad de tecnicismos, anglicismos y jerga hacker que terminan por convertir su idioma en una lengua diferente, solo accesible a los iniciados.

No podía ser de otra manera. Ocurre en todas las disciplinas. Podemos charlar con un poeta sobre la belleza y la grandiosidad del cielo estrellado en una noche de verano, pero si queremos debatir con un astrónomo sobre los secretos del universo, la composición de los agujeros negros, la relatividad del espacio-tiempo, o la estructura de la emisiónderadio de un sistema formado por un púlsary una estrella masiva, es imposible hacerlo sin tener nociones de astronomía, y sin utilizar el lenguaje apropiado.

Ambos, astrónomos y hackers, son científicos, y las más de las veces

vocacionales. Hablan idiomas muy similares: algoritmos, derivadas, integrales y otros «dialectos» matemáticos. Y si algo descubrí en conferencias como la Rooted, o al participar en reuniones privadas como aquella comida, es que, aunque no pudiese comprender los matices técnicos, aquellos jóvenes hackers y sus predecesores tenían algo en común. Algo que flotaba en el ambiente, y que cualquier persona con un mínimo de sensibilidad podía percibir: pasión.

Como en todo oficio vocacional, el hacking implica unos conocimientos técnicos profundos, una inteligencia superior a la media y el uso del pensamiento lateral de forma especialmente creativa. Pero no basta con eso. Hay que echar horas, y horas, y horas… Recuerdo jornadas en casa de David Pérez, donde la mañana dejaba paso al mediodía, y después a la tarde, sin levantarnos de los ordenadores más que para coger otra bebida energética y otra bolsa de patatas, mientras la música tecno nos acompañaba en nuestro viaje por la red… Después, bien entrada la tarde, David se disculpaba: «¡Hostia, tío, que ni siquiera hemos comido!». Se equivocaba. Yo me había empachado de conocimientos.

Recuerdo el rostro de Chus, inclinado sobre la pantalla, a punto de romper un sistema, susurrándole a su máquina… «Vamos, bonita, vamos, tú puedes…», con la ternura y cariño con el que se susurra a una amante. Hasta que el sistema se rompe abriéndole paso hasta lo más profundo de sus entrañas: «Ábrete, Sésamo…».

Recuerdo cenas con hackers de currículos brillantes y precoces, regadas en generosa cerveza hasta las seis de la madrugada, intercambiando anécdotas que antes me parecerían inverosímiles: «Y cuando descubrí aquella vulnerabilidad me tiré tres días y tres noches sin levantarme de la silla. Me había hecho una cacerola de garbanzos que tenía al lado del ordenador y es lo que comía, cenaba y desayunaba… Al final meaba también en la cacerola para no perder tiempo caminando hasta el baño…».

Hoy sé que esa anécdota es real, que mi amigo no exageraba. Los hackers son exploradores. Cosmonautas en un universo microscópico cuyos enigmas escapan a la comprensión del resto de los mortales, a pesar de que dicho universo condiciona totalmente nuestras vidas. Y como exploradores en ese nuevo mundo, ellos son quienes nos marcan el camino.

Si hoy podemos descargarnos cientos de aplicaciones en nuestro teléfono móvil, para medir nuestro ritmo cardiaco, para conocer el clima en Guinea Ecuatorial o para cualquier otra cosa, es en buena medida gracias a GeoHot.

Con solo diecisiete añitos George Hotz (GeoHot) consiguió descubrir una vulnerabilidad en iPhone que le permitió «liberar» por primera vez un teléfono que había sido concebido por Apple para uso exclusivo de sus productos. El *jailbreak* de GeoHot hizo historia, y posibilitó que hoy nuestros teléfonos móviles sean un poco más libres. El suyo, el primer iPhone que hackeó, lo cambió por un flamante deportivo Nissan 350z. Aunque mantuvo su promesa de que no cobraría un dólar por su descubrimiento, nada le impedía aceptar la oferta de la compañía telefónica

Certicell, interesada en conservar aquella pieza única en la historia del hacking. Certicell consiguió su fetiche, y GeoHot, un coche espectacular.

Más tarde volvió a hacerlo. La consola PlayStation 3 de Sony era la única que no había conseguido ser hackeada… hasta que GeoHot se puso a ello. Pero en esta ocasión la empresa no reaccionó con tanta deportividad como Apple, sino que le puso una denuncia. Craso error. La comunidad hacker consideraba al joven George un héroe y reaccionó con un ataque masivo a Sony, creándole tales brechas de seguridad, que tardaron meses en solucionarlas. Incluso mucho después de que hubiesen retirado la demanda, continuaban parcheando las heridas de sus sistemas.

Cuando recibió la demanda, GeoHot compuso un rap a Sony, que grabó en su propia casa y que ganó un Pwnie Award a la mejor canción en la edición 2011 de la Black Hat, una de las conferencias más prestigiosas del mundo hacker en los Estados Unidos. Ese vídeo casero, colgado en YouTube, dice más sobre la esencia del espíritu hacker, que todo lo que yo pueda explicar…[158]

GeoHot invirtió 500 horas, y mucha bebida energética, en liberar el iPhone. Y probablemente los hackers que han conseguido localizar vulnerabilidades similares, haciendo nuestra vida digital un poco más cómoda o segura, han hecho lo mismo.

Google, Facebook, Yahoo, Twitter, Apple, Amazon, Microsoft, eBay… los gigantes de la informática y las telecomunicaciones se gastan auténticas fortunas en seguridad. Contratan a los mejores, me consta, y como es lógico intentan que sus productos comerciales sean los pioneros del sector. Sin embargo, siempre aparece un nuevo hacker que identifica una nueva vulnerabilidad.

Habitualmente solo, en la intimidad de su cuarto, rodeado de libros de informática y compuestos electrónicos, y con una lata de bebida isotónica o una taza de café siempre a mano, se pasará días y noches enteros explorando el código fuente, aplicando herramientas, utilizando diferentes lenguajes de programación y distintos navegadores, aplicando el principio de ensayo-error una, y otra, y otra vez… Y en ocasiones, explorando más allá del software, desmontará el dispositivo para añadir nuevos componentes de hardware para potenciar o limitar una capacidad de la máquina. Así fue como GeoHot rompió la seguridad del iPhone. Y así es como muchos hacker consiguen encontrar esa debilidad del sistema, esa puerta trasera… Comprendiendo a la máquina, entendiendo su forma de expresarse y comportarse para, engañándola con delicados susurros al oído, alterar su funcionamiento.

Son genios. Por lo general poco reconocidos fuera de la comunidad hacker, pero merecedores de que la Academia de Ciencias de Suecia establezca el Nobel de Hacking. Cuando en 1895, un año antes de su muerte, el químico, ingeniero, inventor y fabricante de armas sueco Alfred Bernhard Nobel instauró el premio que lleva su nombre, el hacking informático era algo inimaginable. Pero la dedicación, creatividad, conocimiento, ingenio y vocación por la investigación que implica el hallazgo de una nueva vulnerabilidad bien se merecen un Nobel específico. Sobre todo porque ese hallazgo implicará una mejora en la seguridad y calidad de nuestra

vida digital. Y la vida digital cada día está más implantada en nuestra sociedad.

En realidad, esas grandes empresas son las primeras en explotar nuestras vulnerabilidades como usuarios. Y sobre todo nuestro desconocimiento.

¿Cómo es posible que cuando visito librerías *online*, buscando libros sobre terrorismo, periodismo de investigación o informática, aparezcan en mi pantalla anuncios con esos libros cuando abro el navegador? ¿Por qué recibo un mensaje de Facebook diciéndome que tengo muchos contactos en mi correo que no tengo agregados como amigos en la red social? ¿Cómo ha averiguado mi email Linkedin, empeñada en que tal o cual amigo me invita a unirme a su red?

Los proveedores de internet hace años que invaden nuestra intimidad impunemente, a través de las *cookies* del navegador, a través de las agendas de contactos de nuestros colegas, o de las nuestras propias al autorizar tal o cual aplicación. Saben lo que buscamos, cuándo lo buscamos y dónde. Conocen a nuestros amigos, familia, amantes. Tienen acceso a toda nuestra vida digital. A nuestras compras. A nuestros viajes. Y nosotros, como usuarios, solo podemos adoptar el papel de sujetos pasivos, confiando en que ese inmenso poder que les otorga tal cantidad de información se utilizará de forma lícita. Los hacker no se conforman con eso, y les devuelven una ración de su propia medicina.

Si Edward Snowden tiene razón, y todopoderosas agencias de Inteligencia como la NSA tienen un control casi total de las comunicaciones electrónicas, ¿quién estaría más interesado en que los hacker no descubran y denuncien esas deficiencias en la seguridad de nuestras comunicaciones?

En la Rooted se presentaron algunas de esas vulnerabilidades, que a ojos de un profano como yo resultaban estremecedoras.

Recuerdo como especialmente inquietante la conferencia de Hugo Teso, sobre el hacking a la seguridad de aviones comerciales… por razones obvias. Hugo nació en Barcelona, pero como nadie es profeta en su tierra, se fue a predicar a Berlín. Piloto privado, y hacker autodidacta, ahora es consultor en seguridad de la empresa alemana N.runs, y tras una investigación de tres años sobre la seguridad de los aviones descubrió varias vulnerabilidades que, en malas manos, resultarían extremadamente peligrosas. Teso explicó a una audiencia tan fascinada como yo cómo se podía hackear un avión utilizando simplemente un teléfono móvil… Aterrador.

Fascinante me pareció también la forma que José Selvi descubrió para burlar la seguridad de Google, alterando las fechas del calendario con un ataque *man in the middle*. Fantástico. «Si te llevas el equipo al futuro, y vuelves, no pide actualizaciones… HTTPS cambia a HTTP alterando la hora del equipo por NTP… La fecha no es un elemento crítico, está poco protegido…» Y adiós, candadito…

Selvi, cuyas conferencias ya había disfrutado antes y volvería a disfrutar poco después —en la CON de Mundo Hacker en abril siguiente por ejemplo—, nos había obsequiado con un ejemplo del pensamiento lateral que caracteriza a los hacker a la hora de enfrentarse a un sistema. Explorarlo hasta buscar el eslabón más débil, en

este caso el calendario que actualiza las protecciones. Su conferencia se tituló «El tiempo en MIS manos». No se me ocurre un enunciado mejor.

También me maravilló la aportación de Eduardo Cruz, que nos demostró que el hacking no se circunscribe al software del ordenador… de igual forma es posible hackear el hardware. Su charla, titulada «Ingeniería inversa de circuitos integrados», nos ilustró sobre cómo la parte física de la informática ofrece asimismo diferentes vulnerabilidades explotables por manos expertas. Otros participantes en la Rooted, como Sebastián Guerrero, ya habían mencionado de igual modo en sus charlas esa parte física del hacking, en su caso atacando el escáner de huellas digitales de Apple Pay.

En realidad, todas las conferencias y paneles fueron brillantes. Los organizadores saben escoger a los mejores. David Barroso, Carmen Torrado, Miguel Tarasco, Pablo Casais, Adrián Villa, Raúl Siles, Eduardo Arrios, Ricardo J. Rodríguez, Sebastián Guerrero, Christian López, Andrzej Dereszowski, Yaiza Rubio, Félix Brezo, Antonio Guzmán, Abel Valero, José Pico o el gran Chema Alonso, entre otros. Es imposible reseñar, como se merecen, las aportaciones que hicieron todos y cada uno de ellos. Las mismas que hacen cada año en esta y otras CON parecidas, donde los hackers presentan en sociedad el fruto de meses o años de trabajo silencioso y solitario, ante sus ordenadores.

Al final del evento, sales con la sensación de que podemos sentirnos orgullosos de los hackers españoles. Aunque menos valorados, sus cerebros están tan bien dotados como los de la comunidad hacker norteamericana, china o rusa. Solo que cuentan con muchos menos recursos para hacer su trabajo.

Todo ellos son capaces de localizar vulnerabilidades ocultas que muy pocos verían. Eso mismo fue capaz de hacer otro de ellos, un informático monegasco, y su caso terminaría ocupando la primera plana de los periódicos del mundo entero.

Falciani, o cómo hackear la banca suiza

Me enteré de que Hervé Falciani estaba en España gracias a Aurora, una de las responsables de prensa del bufete del juez Baltasar Garzón. Llevaba medio año «acosándola», tanto a ella como a su compañera, para que me consiguiesen una reunión con Garzón. Sabía que él era uno de los abogados de Julian Assange y fue una de las vías de acceso que intenté para llegar al fundador de Wikileaks.

Garzón nunca llegó a recibirme. Incompatibilidades de agenda, supongo. Sin embargo, me costa que sus colaboradoras lo intentaron por todos los medios. Y sensibilizadas con mi trabajo, me ayudaron en todo lo posible. Por eso, cuando Aurora se enteró de que Falciani venía a España, me dio el chivatazo. Desde aquí se lo vuelvo a agradecer de corazón.

Hervé Falciani, como Assange o Snowden, eran tres de mis objetivos. De hecho, ya había iniciado los trámites para regresar a Italia, cuando la Providencia me quiso facilitar un poco las cosas.

España es uno de los pocos países europeos por los que Falciani puede moverse sin ser detenido y extraditado a Suiza. Los otros dos son Francia e Italia. Assange lo tiene peor. Solo puede moverse por el interior de la embajada de Ecuador en Londres.

Nacido en Montecarlo (Mónaco) en 1972, Falciani es un ingeniero informático que en 2009 salta a las portadas de toda la prensa internacional al ser identificado como el autor de la mayor filtración de evasores fiscales de la historia de la banca suiza. La llamada «Lista Falciani» incluía algunos de los nombres más poderosos del planeta, señalándolos como evasores fiscales multimillonarios: 1.300 griegos, 1.800 japoneses, 1.800 españoles, 6.000 estadounidenses, 10.000 italianos, 11.000 británicos, 12.000 franceses, etcétera. En total 130.000 presuntos evasores fiscales millonarios, de 183 países distintos.

Entre los usuarios de las cuentas en la banca suiza filtradas por Falciani había políticos, jefes de Estado, banqueros, empresarios… pero también narcotraficantes y terroristas. Todos protegidos por el inexpugnable secreto bancario. Hasta que Falciani lo hackeó. Literalmente.

Hervé Falciani estudio informática en el Sophia Antípolis, un parque tecnológico situado en los Alpes. Y en 2001 se incorporó a la filial suiza del poderoso The Hong Kong and Shanghai Banking Corporation (HSBC), uno de los bancos que custodian las fortunas de los hombres más poderosos del planeta. Su trabajo consistía en reorganizar la base de datos de la entidad para reforzar su seguridad informática…

Entre 2001 y 2008, Falciani, solo o en compañía de otros, se hizo con un volumen de información confidencial sobre los clientes del HSBC que, tras un proceso a la par rocambolesco y ambiguo, terminó en poder de las autoridades cuando fue detenido, en 2008. Desde entonces es un personaje tan mediático como controvertido. Para unos, un héroe, al nivel de Julian Assange o Edward Snowden, que sacrificó su bienestar para revelar una información escandalosa. Para otros un «Judas» de manual,

[159] que intentó lucrarse con la información que consiguió sustraer de un sistema informático. A mí me contó una versión diferente a ambas…

El mensaje de Aurora me alertó de que el 25 de mayo de 2015, Falciani estaría en Madrid. Por fortuna, yo también.

Los días 22 y 23 había asistido a la edición 2015 de X1Red+Segura, en la que por cierto se esperaba como agua de mayo la ponencia de Josep Albors, director de comunicación y del laboratorio de ESET España, al respecto de la pandemia de *ransomware* de Correos.[160] Pero si destacase algo de esta edición sería la última mesa redonda. Tras un panel sobre las Fuerzas y Cuerpos de Seguridad del Estado y la seguridad informática, y una fascinante mesa redonda *online* con la participación de hackers desde Bolivia, Chile, Ecuador, etcétera, llegó el turno de las CON. Allí, en un mismo escenario, y moderados por la periodista de RTVE Mavi Doñate, estaban los directores de las principales conferencias de hacking del país: AlbahacaCon, ClickaSeguro, ConectaCon, GSICKMinds, Hackron, Honey Sec, Qurtuba, Navaja Negra, No cON Name, MorterueloCon, RootedCON, Sec Admin y Sh3llcon.

No pude evitar levantarme de mi asiento, cruzar la sala, y acercarme hasta la segunda fila —donde el comandante De la Cruz, ya sin uniforme tras intervenir en la primera mesa redonda, seguía con mucha atención esta de los hackers— para inmortalizar el momento. Aquella imagen del jefe del Grupo de Delitos Telemáticos de la Guardia Civil, escuchando a los hackers me pareció todo un símbolo de que las cosas estaban cambiando. Enemigos irreconciliables durante décadas, hackers y policías habían llegado a un punto de colaboración y entendimiento del que todos los usuarios salimos beneficiados.

El caso es que tras las jornadas de Angelucho y los suyos, me había quedado un par de días por Madrid, así que no me costó nada presentarme en la dirección que me había facilitado Aurora.

Falciani había viajado a España para conceder una rueda de prensa con motivo de la traducción al español del libro *La cassaforte degli evasori,* editado por Chiarelettere en febrero de ese año, que Hervé firma en coautoría con el periodista Angelo Mincuzzi, redactor jefe del diario *Il Sole 24 Ore*.

La editorial española La Esfera de los Libros había comprado los derechos, y la presentación de *La caja fuerte de los evasores* corrió a cargo de Ymelda Navajo, obviamente satisfecha por el poder de convocatoria de Falciani. El Salón Nueva Estafeta del Ateneo de Madrid estaba absolutamente repleto de cámaras de televisión, grabadoras y cámaras fotográficas.

Me planté allí sin acreditación e improvisando sobre la marcha, y tuve suerte. Si en lugar de La Esfera de los Libros, hubiese sido cualquier otra editorial la responsable de la traducción, probablemente mi plan no habría salido bien, pero en cuanto reconocí a Mercedes en medio de la legión de periodistas que rodeaba a Falciani supe que iba a conseguirlo. Mercedes, actualmente responsable de prensa de La Esfera de los Libros, es una vieja amiga. Era la jefa de prensa de la editorial

Temas de Hoy cuando se publicó *Diario de un skin*, y lo siguió siendo más o menos hasta la época de *El Palestino.* Desde un punto de vista editorial, ella fue la que más sufrió las particulares circunstancias de mi trabajo, porque debía promocionar un libro cuyo autor no podía presentar, ni participar en ferias literarias, firmas de ejemplares, y casi ni conceder entrevistas físicas. Lo cierto es que por mi culpa sufrió muchos quebraderos de cabeza.

Cuando comenzó el acto, sentí un poco de envidia de Falciani, hasta él podía subirse a aquella mesa y hablar libremente sobre su obra. Yo no.

Me acerqué a Mercedes sigilosamente en cuanto mis compañeros de la prensa la dejaron libre. Creo que de verdad se alegró de verme.

—¡Toni! ¿Qué haces aquí? Qué sorpresa… —Dos besos, un abrazo y saludo de rigor.

—Merche, necesito que me hagas un favor… ¿Hasta cuándo se queda Falciani en España?

—No se queda. Llegó esta mañana y esta tarde coge un avión de vuelta.

—Vale. Imagino que tendrás un montón de medios esperando para entrevistarlo.

—Uff, están todos locos con él. ¿Quieres que te reserve a ti un rato?

—Sí, pero necesito estar a solas con él, sin más medios. Y que sea la última entrevista que conceda hoy. Justo antes de marcharse al aeropuerto. ¿Podría ser?

—Claro. Dalo por hecho. Déjame ver…

Mercedes consultó su agenda y me dio una hora y un lugar. Así que conseguí un ejemplar de *La caja fuerte de los evasores*, y busqué una cafetería acogedora, muy cerca del Congreso de los Diputados, ubicado a pocos metros del Ateneo donde Falciani seguía presentando su libro a la prensa.

Me puse cómodo y empecé a leer. Tenía menos de cinco horas para terminar el libro y sacar notas para la entrevista. Todos mis compañeros habían recibido el ejemplar el mismo día, y por lo tanto no habían tenido tiempo de leerlo, así que era probable que yo fuese el primer periodista español que entrevistaba a Hervé tras haber leído su libro, y sé por experiencia cuánto se agradece que el entrevistador se haya molestado en leer la obra sobre la que te está preguntando. Así se evitan muchas preguntas estúpidas.

Durante casi trescientas páginas Mincuzzi recompone la biografía de Falciani, desde su nacimiento, hasta la actualidad. Pero la historia que se relata en la obra difiere en algunos puntos de la que yo había compilado tirando de hemeroteca.

A solas con Falciani

Hervé estaba cansado. Se le notaba. Había llegado a Madrid poco antes y tras la rueda de prensa se había pasado las siguientes horas respondiendo, estoy seguro, una y otra y otra vez a las mismas preguntas. Los periodistas no solemos ser muy originales en las entrevistas a un personaje como Falciani. Así que yo intentaría llevar el interrogatorio por otros derroteros. Él lo agradecería y yo tendría más posibilidades de conseguir su ayuda para alcanzar otro objetivo. Mi verdadero objetivo.

Casi todos mis compañeros querían nombres. Como si no los conociésemos. Como si valiese de algo. Y durante la rueda de prensa varios reporteros le preguntaron directamente por alguno en concreto. Falciani siempre esquivaba esas preguntas insistiendo en que lo importante era conocer los mecanismos, y no a tal o cual evasor. Además, en su libro cita a varios clientes del HSBC con nombres y apellidos, como Emilio Botín; la madre del exprimer ministro Yorgos Papandréu; Stephen Green, exministro de Comercio del Reino Unido; o Jerome Cahuzac, exministro francés.[161]

¿Qué más da? En 2013 el Consorcio Internacional de Periodistas de Investigación (ICIJ) publicó los nombres de miles de propietarios de sociedades en paraísos fiscales de todo el mundo en el llamado Caso Offshore Leak. ¿Y? Otro titular llamativo sobre un nuevo escándalo de corrupción apilado en la hemeroteca. Y hasta el siguiente. En España, casos como los ERE de Andalucía o Bárcenas deberían haber hecho dimitir a toda la cúpula del PP y el PSOE cogidos de la mano. Pero no pasa nada. Asumimos que la financiación ilegal de nuestros partidos políticos es una práctica habitual, y no pasa nada. Así que, salvo por alimentar el morbo del momento y llenar un par de titulares condenados al olvido con el siguiente escándalo, que Falciani pronunciase uno o dos nombres más no iba a tener ninguna repercusión real. Imagino que esa es la razón por la que prefiere hablar de otros temas.

—Casi naciste en un banco —le pregunto para romper el hielo—. Al salir del colegio te ibas a la sucursal donde trabajaba tu padre y jugabas en sus pasillos. O sea, que la banca y los secretos bancarios de los poderosos han sido tu jardín de infancia…

—Montecarlo es muy pequeño. Todos estamos mezclados. La banca, los ricos, los famosos, cuando eres niño todo te parece natural. Todo lo que pasa en Montecarlo se queda en Montecarlo. Yo crecí con el secreto bancario. Pero al mismo tiempo me generó el interés por el conocimiento de ese secreto.

—Pero la diferencia del banco donde trabajó tu padre y el HSBC es que en aquella época el dinero se movía en efectivo. Hablas de grandes cantidades de dinero en *cash* que llegaba desde Francia, Italia…

—Sí, claro. Cada vez que se producía una crisis importante en algún país, en Montecarlo se recibían grandes cantidades de billetes. Como lo que está pasando

ahora en Grecia, que mucho dinero ha salido del país. Porque los poderosos temen perder su dinero. Como cuando en Italia la mafia lo sacaba del país, es natural.

—Vale, creces en un banco, después trabajas de grumete en un yate, y tras terminar tus estudios de informática, tu primer trabajo aplicando la informática a una banca ¿es en un casino?

—A uno de los jefes del casino lo conocía porque los dos practicábamos remo. Montecarlo es un pequeño pueblo, nos conocíamos todos, y por eso cuando terminé de estudiar pude empezar a trabajar en el casino de Montecarlo, y de ahí pasé a la banca.

En la versión que presenta en su libro, Falciani sugiere que siempre fue un infiltrado —«Pero es mejor decir *insider*», me dijo—. Lo habría reclutado un grupo de personas vinculadas a diferentes servicios de Información, para infiltrarse en la banca suiza, y para reclutar a otros colaboradores que tuviesen acceso a los archivos informáticos a los que él no podía llegar.

—Creo que tu etapa en el casino es importante porque ahí nace «La Red», ¿no? Ahí es donde conoces a los expolicías o exagentes de otras agencias, que llevaban la seguridad del casino y que luego serán los impulsores de tu misión en Suiza, según cuentas en el libro.

—Sí, porque antes de trabajar en la banca del casino, yo empecé trabajando en la seguridad. Eso significa que durante las guardias, noches enteras, podías hablar horas y horas con tus compañeros. Jubilados de la policía, el servicio de aduanas, la gendarmería, el ejército… Eran prejubilados de esos servicios de información, con cincuenta o cincuenta y cinco años, que me confiaban todo lo que habían vivido. Investigaciones que habían realizado con otros países, como Suiza. Me explicaron cosas que yo no sabía, ni imaginaba. Y esas cosas me las guardé durante años. Gracias a ese mundo que descubrí con ellos, he tenido esta oportunidad de que ellos me ayudasen.

—La oportunidad la tuviste tú, o la tuvieron ellos. Porque según cuentas, cuando ya te trasladas a Ginebra para llevar el sistema informático del HSBC, te das cuenta de que hay aspectos oscuros del sistema bancario que nos afectan a todos. Pero, según dices, la operación para extraer esa información no se limita a ti. No eres un Manning[162] o un Snowden que trabaja solo, sino que hay toda una red detrás…

—La Red va más allá del banco. Yo no tenía acceso a los sistemas. Yo solo era el encargado de analizarlos. Así que era necesario algún empleado del banco con acceso. Pero la Red va más allá. Había muchos investigadores, jubilados o no. Incluso gente que vi solo una vez, un minuto, y que me orientaban hacia dónde tenía que ir y qué tenía que buscar.

Falciani sugiere que la Red la constituían más de cien colaboradores.

—Tienes que entender que muchas veces se habla de personas que cambian. Especialmente la parte de Ginebra, que se hizo con gente que cambiaba cada mes.

En su libro Falciani no detalla demasiado como hackeó la banca suiza:

El mecanismo se basaba en un software parecido al BitTorrent, un protocolo peer-to-peer (P2P) para el intercambio de archivos en internet. La información que introducían nuestros contactos del interior del banco se fragmentaba en miles de documentos y se repartían entre otros tantos ordenadores. Los propietarios de esas máquinas no sabían que entre sus discos duros se conservaban los datos del HSBC. [163]

—Creo que estuvisteis ocho meses ocultando miles de documentos en la nube a través de la Deep Web. Pero ¿cómo lo hicisteis? Nunca has detallado esto.

—Usamos muchos sistemas. Por ejemplo, la esteganografía, ocultando la información en películas o fotos para subirla a la nube. Al mismo tiempo que se subía, yo podía descargarla para auditar que la información era correcta y completa.

La historia de Falciani se inicia en Beirut, cuando bajo la falsa identidad de Ruben Al-Chidiack se reúne con la directora del banco Audi para ofrecerle la información extraída del HSBC. Aquella reunión desataría los acontecimientos que terminarían con su detención en Francia y el conocimiento público de la existencia de una «Lista Falciani».

—Me llama la atención tu visita al Líbano. Conozco Beirut y puedo imaginar lo que sentiste. Según tu versión ese viaje con tu compañera era para ponerle una trampa, sacando a la luz que teníais en vuestro poder los documentos y motivar la actuación de los servicios secretos…

—Puede ser difícil de entender, pero es fácil si conoces cómo funciona la banca. Solo hace falta una alerta para que empiece una investigación de las autoridades suizas. Todos los bancos suizos tienen la obligación de disparar las alertas en caso de riesgo de violación del secreto bancario. Necesitábamos un lugar donde yo pudiese activar esa alerta. En el libro no se explica mucho, pero por supuesto existían alternativas al Líbano; antes estudiamos la posibilidad de hacerlo en Montecarlo. Pero cuando llegó al banco esta compañera, nos sirvió en bandeja la posibilidad del Líbano. Y esta estrategia que usamos, esta trampa, también se puede utilizar hoy. Se puede hacer saltar una alerta bancaria porque sabemos que los emails, las llamadas telefónicas, todo se puede vigilar. Hoy lo sabemos gracias a Snowden.

Para las autoridades suizas, Falciani robó información confidencial del banco donde trabajaba y trató de lucrarse vendiéndola al mejor postor. Según la versión de Falciani, el viaje a Líbano formaba parte de una estrategia para motivar su detención, la incautación de su ordenador y su ofrecimiento a colaborar con las autoridades francesas (las primeras en acceder a la «Lista Falciani») para destapar toda la mierda acumulada en las cámaras de seguridad de la banca suiza.

Centrar el debate en dirimir si Falciani robó la información para sacar un rédito económico o si sacrificó su vida anterior para revelar al mundo la corrupción de la banca puede ser un debate entretenido. Pero más allá de si Hervé es un héroe o un villano, lo cierto es que la información es real. Y eso es lo más importante.

Los argumentos de quienes intentan desacreditar la «Lista Falciani» argumentando que su autor intentó ganar dinero me recuerdan vagamente los pataleos de los skin o los bolivarianos, asegurando que yo trabajo para diferentes servicios

secretos. ¿Y? Ahí están mis grabaciones. Rebátelas si puedes… Y ahí están los documentos de Falciani.

Uno de los aspectos de su historia que a mí me resultaban más interesantes enlaza con el tercer gran filtrador del siglo XXI: Edward Snowden.

—Ahora que mencionas a Snowden… ¿Coincidiste con él? En 2007 estuvo trabajando para la CIA en Ginebra en algo relacionado con banca. Y tú mencionas reuniones con personas que hablaban un inglés americano perfecto, implicados en la Red…

—Cuando nosotros trabajábamos con la nube, la gente de la Red tenía miedo a que otros equipos del mismo servicio secreto pudiesen estar trabajando para proteger los intereses del banco. Los intereses geopolíticos de lo que está pasando en Ginebra van mucho más allá de un banco. Por eso la presencia de Snowden en Ginebra. Yo estoy convencido de que su trabajo allí fue útil. Y me ayudó a hacer el mío.

Uno de los momentos más intensos de su biografía se produce cuando sus amigos los «espías» de la Red simulan su secuestro ante la sospecha de que podían estar siguiéndole. Intentaban dotarle de una coartada en caso de que sospechasen de él. Si alguien veía la escena, describiría a unos hombres de aspecto árabe que había metido a Hervé en un coche a punta de pistola, para obligarle a colaborar con ellos… Era su forma de ocultar la verdadera Red.

—Después de tu primera detención, cuando te incautan el ordenador con parte de los documentos, viviste episodios muy dramáticos. Incluso un falso secuestro.

—Cuando llegó la persona del Líbano nos pusimos muy nerviosos. Sabíamos que me estaban vigilando porque no sabían exactamente lo que habíamos obtenido. Y aquel día yo acababa de salir de un encuentro con gente del banco. Y volviendo a casa, por la noche, me cogen por detrás y me meten en una furgoneta, me tiran al suelo… y por unos segundos, hasta que me explicaron lo que estaba pasando, pensé: se acabó. Pensé de verdad que eran los suizos.

En 2009, Falciani comienza a colaborar con las autoridades italianas. Y a pesar del esfuerzo de los agentes de la Guardia de Finanza, «en Italia, el primer ministro era Silvio Berlusconi, y el ministro de Economía era Giulio Tremonti. El aspecto problemático de la situación era que las leyes italianas, a diferencia de las españolas, no permitían el uso judicial de información obtenida por canales no oficiales».[164]

—Empiezas a colaborar con las autoridades francesas, italianas, y por fin llegas a España.

—Sí, y con otros países, que todavía no se han revelado.

La «Lista Falciani», como era previsible, se convirtió en un arma. Y Hervé menciona casos sangrantes de cómo su información se instrumentalizó políticamente: «Los únicos estados a los que las autoridades francesas les negaron rotundamente el material fueron aquellos donde el nivel de corrupción era notoriamente elevado, como Rusia, China e India. Más tarde el Gobierno de Nueva Delhi llegó a un acuerdo con Sarkozy: era la época en que el presidente francés quería que India comprara un

lote de aviones de combate Dassault Rafale, y así, a cambio del pedido, Sarkozy le entregó la lista al Gobierno indio».[165]

—Mencionas varias personas que se han aprovechado de tu información… Bueno, quizás sería más exacto decir *vuestra* información.

—Vuestra. Sí, Sarkozy, por ejemplo. Cuando él se sentó a negociar con el ministro de Economía griego, ya sabía que él y su familia aparecían en nuestra lista. Y al conocer el secreto de esta persona estás en situación de superioridad. Hace poco detuvieron al ministro por esos delitos…

El 30 de junio de 2012 Falciani es detenido en Barcelona, en cuanto pone un pie en suelo español, tras bajarse del ferry que le había traído desde Sète, en el sur de Francia. Según su relato, su detención formaba parte de un plan preestablecido para poder facilitar legalmente a las autoridades del país la documentación sobre los evasores españoles. Dadas las dimensiones del caso, el juez de Barcelona no se declara competente y Falciani es derivado a la Audiencia Nacional en Madrid.

Se pasó casi dos meses en el módulo 1 de la prisión de Valdemoro. Compartiendo instalaciones con «un terrorista de ETA que hablaba muy bien francés (…), mafiosos que ya no tenían las huellas digitales y un asesino a sueldo rumano con pasaporte venezolano».[166]

—En tu celda, en la prisión de Valdemoro, coincides con un neonazi cocainómano, con un narcotraficante… pero con ningún banquero.

—Bueno, coincidí con el responsable de las finanzas de Casper,[167] pero con un banquero de verdad, no.

Sin embargo, en su libro Falciani reflexiona sobre algunos importantes banqueros españoles, a los que no vio en prisión:

> … entre los nombres de la lista de clientes del HSBC de Ginebra —como ya hemos mencionado— estaba el presidente del Banco de Santander, Emilio Botín. El banquero se puso de acuerdo con el ministro de Hacienda Cristóbal Montoro, para pagar tan solo el 10% de los impuestos que había evadido, a pesar de que Montoro había declarado públicamente que el HSBC era el caso de evasión fiscal más grave de la historia de España. Botín era un multimillonario, y dirigía el banco más grande de Europa y Latinoamérica. Pagó tan solo 286 millones de euros por una evasión de 2.800 millones, y no fue objeto de ningún proceso penal.[168]

—Y cuando sales de la prisión, comienzas a colaborar con la Policía y el CNI español en algunos casos que han sido muy mediáticos en España, como la mafia china de Gao Ping o la trama Gürtel.

—Los casos que mencionamos en el libro solo son para que la gente entienda los enlaces. Las relaciones que existen entre las cosas que se están viviendo en la calle y lo que ven en las noticias. Y si hemos mencionado casos concretos, es para demostrar que desde los chinos a los políticos, todos utilizan los bancos. El caso de Gao Ping fue muy interesante para demostrar que con muy poco se puede sacar el dinero.

Uno de los grandes problemas que han tenido los investigadores, me consta, es la complejidad de la información extraída por Falciani. Tengo buena amistad con uno de

los mandos de la Guardia Civil que ha tenido ocasión de trabajar con ella, y una vez me comentó que se sentían desbordados por el torrente de datos, fragmentados e incompletos, y lo imprescindible que era Falciani para el procesamiento coherente de aquella montaña de datos.

Pero el mismo Falciani especifica en su libro que la información llegaba fragmentada de origen. «Si hasta hace pocos años un magistrado podía pedir la incautación de un servidor en Suiza con la relativa seguridad de que allí encontraría toda la información que buscaba, hoy ya no es así. La información ya no está en Suiza, sino diseminada por todo el mundo…»[169]

—De hecho, explicas cómo los bancos fragmentan la información, para que una parte esté en un servidor de India, otra en Japón, otra en Suiza…

—Es que lo importante es comprender el sistema, y conocer las leyes. Te ayuda a entender por qué los políticos te engañan. Por ejemplo, ahora los nombres y apellidos se quedan solo en Suiza, pero las transacciones se pueden hacer fuera. Así que cuando llega una orden, se les puede entregar el nombre del cliente, pero las transacciones van por otros países. La fragmentación es fundamental para mantener el secreto. Tanto los bancos como los servicios secretos tienen esta habilidad para fragmentar la información. Si no sabes cómo juntarla, no tienes nada.

Recordé una de las frases que le había leído: «Es fácil comprender por qué los políticos no hacen nada para combatir la evasión fiscal, el poder desmedido de los bancos y la corrupción: al proteger a los bancos se protegen a sí mismos». No se podía decir más claro.

—En España hemos vivido un fenómeno curioso, que no sé si se ha dado en otros países. En los últimos veinte o treinta años, las cajas de ahorro y bancos poco a poco se han ido fusionando y desapareciendo, hasta quedar al final bajo el control de muy pocas familias. No sé si esto es bueno…

—Es muy malo. Hoy muy poca gente puede manejar el imperio bancario. Y pueden manejar una estrategia que solo ellos conocen. En los tiempos de mi padre, todos los empleados del banco podían conocer todo lo que estaba pasando. Hoy, gracias a la tecnología, un empleado conoce solo su área, y siempre hace lo mismo. Y no sabe qué transacciones está manejando.

—Cuando usas la expresión «guerra bancaria», ¿a qué te refieres?

—Claro que hay una guerra. Son enemigos. Que utilizan los puntos débiles que tenemos en la política económica. Pero no hablo solo de bancos, también de empresas, como Google, que sabe muy bien cómo no pagar impuestos. Esto significa que tenemos agujeros en nuestra política fiscal. No puedes pedir a un lobo que deje de comerse las cabras. Lo que necesitas es proteger las cabras. Las cabras son los impuestos, y empresas como Google son lobos.

Decidí concluir la entrevista porque Falciani tenía que tomar un avión, e imaginé que estaría ya hastiado de periodistas. Pero antes de despedirnos le pedí que nos tomásemos una foto juntos, y entonces se produjo la anécdota del episodio.

Falciani aceptó. Mercedes, que me conoce, y era la única persona presente en la entrevista, fue la primera en advertirle:

—Ahora te vas a asustar.

—En serio, no te asustes ahora —repliqué yo.

Falciani, seguro de sí mismo, empezó a decir algo. «No, al contrario es un pla…», pero se quedó petrificado y con una cara digna de verse, en cuanto me puse los guantes y el pasamontañas que me había regalado el agente del Grupo VII de Información de Tres Cantos durante el juicio a Hammerskin. Imagino que por un instante revivió el trauma de su falso secuestro, y quizá temió que un sicario contratado por la banca suiza por fin lo hubiese localizado. Solo y sin escapatoria posible.

No es broma. Durante años Falciani vivió esperando un atentado inminente. Durmiendo cada noche en un lugar distinto. Acompañado siempre por escoltas policiales. En España, cuando comenzó a colaborar con la Fiscalía, tenía que salir a hacer ejercicio de noche, rodeado por cuatro agentes de policía, ante el temor de que alguien atentase contra su vida. Ver a un tipo poniéndose los guantes y el pasamontañas no debió hacerle puñetera gracia.

Mercedes le explicó que yo era un periodista español especializado en el periodismo encubierto, y que había publicado varios libros. Y entonces se hizo la magia.

En 2011, la editorial italiana Newton Compton había comprado los derechos de *El Palestino,* traducido en Italia bajo el título de *L'infiltrato: una storia vera.* Sorprendentemente, Newton Compton, que editó mi libro en tapa dura, omitió todas las fotografías y documentos incluidos en la edición española, a diferencia de las ediciones portuguesa o polaca del mismo libro. Aun así *L'infiltrato* armó un cierto revuelo en Italia, y por esa razón Falciani abrió mucho los ojos cuando Mereces le dijo mi nombre.

—¡Tú eres Antonio Salas!

Falciani por fin relajó su expresión corporal, y de hecho en la fotografía posa muy sonriente abrazándome.

Era el 25 de mayo de 2015. Ese día, exactamente, se cumplían cinco años de la publicación de *El Palestino.* Lo consideré una buena señal.

Falciani me obsequió con una dedicatoria muy cariñosa en su libro, y me prometió que haría una gestión con su abogado francés, que es el mismo que defiende en Francia los intereses de Edward Snowden, para tratar de buscarme una vía de acceso al autor de la mayor filtración informática de la historia.

MAYO DE 2015
LA PISTA PENAL

«Seguramente la primera etapa de la cultura humana se basó menos en el empleo del animal doméstico que en los servicios prestados por hombres de raza inferior.»

Adolf Hitler, *Mein Kampf,* cap. 11

Imagino que mis amigos comenzaron a implicarse en la investigación del caso MarkoSS88 preocupados por mi ansiedad y el peligro que podía acecharme, pero tengo que suponer que en algún momento, y dado lo extremadamente difícil que resultaba avanzar, continuaron por amor propio, o por curiosidad personal, o por rabia, no lo sé.

Una y otra vez volvimos sobre nuestros pasos, releyendo hasta el exceso las entradas de su blog, los mensajes en las redes, los emails que me mandaba…

—Espera, espera, aquí tenemos algo —dijo un día Álex—. Nos hemos centrado en sus identidades, pero no hemos comprobado su historia. Volvamos al principio. Markos dice que en 2012 mató a un chico sudamericano, ¿no?

Yo asentí con la cabeza.

—¿Conoces a alguien en Homicidios?

—Sí. Hace años hice un reportaje y estuve con ellos. Todavía llevaba el grupo el inspector Rapino. Debo de tener su tarjeta por algún lado.

—Estupendo. Ocúpate tú. Luego tenemos su fecha de entrada y salida de prisión… Eso también es rastreable. Necesitamos a alguien en Instituciones Penitenciarias.

Álex estaba en lo cierto. En las entradas de su blog todavía se encontraban los posts que Markos había subido como despedida de sus «cachorros» y el mensaje, diecinueve días después de su ingreso en prisión por el homicidio del joven latin king, pidiendo la solidaridad de la comunidad neonazi. La fecha era histórica, aquel ingreso en prisión había originado la recogida de firmas en apoyo a Markos subida a Change, y los *hashtags* en Twitter #MarkosLibertad y #TodossomosMarkos. Y unos meses más tarde el post en que regresaba a la red, un día después de salir de la cárcel. Eran buenas pistas, ahora había que comprobarlas.

Rastreé las hemerotecas durante días. Los periodistas de mi generación sabemos lo que significa encerrarse en el trastero donde los periódicos

conservan los tomos de la edición en papel de todos sus diarios. Conocemos el olor a humedad, el tacto de las cubiertas de cuero y de las hojas de papel añejo en la punta de los dedos, pasando página a página durante horas.

Y conocemos también las máquinas de microfilmes, donde años después los medios más potentes compilaron todas sus ediciones, para facilitarnos a los investigadores nuestro trabajo. Aparatos grandes y toscos, que imitaban el aspecto de un viejo ordenador, y que iban desplazando los diarios microfilmados, al ritmo que marcaba una rueda del panel de control.

Pero ahora no es necesario. Los grandes diarios —como *El País, La Vanguardia,* el *ABC,* etcétera— han liberado sus hemerotecas *online* en un gesto que los honra. Cualquier investigador puede acceder gratuitamente a ellas desde internet, y consultar todos los números publicados, incluyendo sus ediciones locales. Los otros, los de pago, ofrecen el mismo servicio por un módico precio.

Y nada. Yo no fui capaz de encontrar ni una sola noticia de prensa sobre el homicidio de un latin king, en Madrid, en 2012, a manos de un skinhead neonazi. Así que puse todas mis esperanzas en que mis amigos hubiesen tenido más suerte con Instituciones Penitenciarias.

Pero no tenía ni idea, lo confieso. En ningún momento pude imaginar que la lista de candidatos fuese tan enorme. Manu y sus compañeros acudieron a Instituciones Penitenciarias y consiguieron el listado de todos los reclusos que habían ingresado en prisión en la fecha señalada por Markos, y todos los que salieron de la cárcel cuando él volvió a la red. Eran más de 600 candidatos… y los comprobaron uno a uno. Una labor ingente.

No existía ningún Markos, ni ningún otro skin, ni miembro de ninguna banda, que hubiese entrado y salido de prisión en esas fechas por un asesinato. MarkoSS88 jamás había estado en prisión.

En el grupo de Homicidios tampoco tenían constancia de la muerte de ningún latin king en 2012 a manos de un skinhead llamado Markos ni de ninguna otra manera.

Insistimos. En el grupo había agentes nuevos, así que acudimos a los veteranos que, como Rapino, ya habían dejado el grupo. Nada. Nadie recordaba ningún caso que se pareciese remotamente a lo que Markos relataba en la entrevista y en sus redes sociales.

Volvimos a insistir, rogándoles que echasen un vistazo a los expedientes de 2012, tal vez se les había pasado… Tampoco. En el archivo del grupo de Homicidios no había constancia de ningún caso semejante.

—Además —concluyó con muy buen criterio uno de los policías del grupo de Homicidios—, ¿en serio creéis que un caso así se habría pasado por alto?

El policía tenía razón. En el fondo era obvio. Estaba ante nuestros ojos

desde el principio. En España existe una sensibilidad especial para con los crímenes de odio. Los asesinatos y homicidios de Susana Ruiz, Lucrecia Pérez, Aitor Zabaleta, Manuel Ríos, Miguel Grau o más recientemente Jimmy, no solo son portada de todos los diarios cuando se producen, sino que vuelven a ser recordados, una y otra y otra vez, en cada aniversario, en cada nuevo caso de crimen fascista, o cuando las organizaciones como el Movimiento Contra la Intolerancia o CEIDIV intentan remover las conciencias contra el odio racista. Era del todo imposible que Markos hubiese matado a un latin king y que absolutamente nadie se hubiese enterado…

MarkoSS88 quizá se había creído su propio discurso, y nos consideraba a todos una raza inferior; tal vez creía, como decía el Führer, que solo éramos útiles para servir a sus propósitos. Como animales irracionales dotados de una inteligencia primaria. Pero había cometido un error. El castillo de MarkoSS88 comenzaba a desmoronarse.

Capítulo 18
Hacktivismo

«Es mi forma de ser. Disfruto creando sistemas a gran escala y ayudando a gente vulnerable. Y disfruto machacando a hijos de puta.»

Julian Assange

El hombre que lanza piedras a la luna

Fue un suplicio, lo reconozco. Pero desde nuestro primer contacto Lord Epsylon dejó claro que solo se comunicaría conmigo a través de emails cifrados con PGP. Supongo que para un hacker es un paseo, pero para un simple usuario resulta terriblemente engorroso aprender a manejarse con el aburrido, lento y desesperante programa de cifrado. La seguridad requiere un esfuerzo.

Primero tuve que instalarlo. Después crear una clave pública y una privada. Habilitar el programa de descifrado con una nueva contraseña. Y a partir de entonces, para un simple «cómo estás», tenía que abrir un programa de edición de textos, escribir el mensaje, pasarlo por el programa de cifrado, autorizarlo con mi contraseña, solicitar la clave pública del receptor, cifrar el mensaje, copiar en un nuevo documento de texto el inmenso galimatías de dígitos en que se convierte el simple «cómo estás», adjuntarlo al email y enviarlo.

Y cada vez que recibía un mensaje cifrado, repetir todo el proceso pero a la inversa. Sin embargo, no había otra manera. Epsylon simplemente no contestaba mis correos cuando le enviaba un mensaje no cifrado.

Exactamente lo mismo que le ocurrió a Glenn Greenwald con Edward Snowden. Y como Snowden solo aceptaba correos cifrados con PGP, Greenwald no tuvo más remedio que aprender a utilizar el cifrado. Y yo seguí su ejemplo. E igual que Greenwald, yo no me conformaba con recibir información vía email. Quería un encuentro personal.

Por fin, después de semanas de intercambio de correos cifrados, Lord Epsylon aceptó recibirme en su último refugio secreto. Me envió un lugar, un día y una hora.

El viaje fue largo y pesado. Con el temor de que aquello pudiese ser una trampa. Tras la publicación del post sobre mi experiencia con los talleres de artes marciales para «cazar policías», escrito para MarkoSS88, había recibido mucho odio por parte de jóvenes de extrema izquierda, que no habían entendido nada. Estoy seguro de que se habían limitado a ver el vídeo grabado con cámara oculta en la casa okupa de Barcelona, sin siquiera leer el texto y la denuncia que hacía de cómo los había manipulado un servicio secreto. Pero en todos los colectivos hay descerebrados. ¿Y si sabían que yo era el autor de las imágenes y me habían preparado una emboscada? No le había dicho a nadie adónde iba. Y acudía solo… Inevitable que algún mal pensamiento te pase por la cabeza durante tantas horas de carretera, pero estaba seguro de que Lucas, mi aval ante Lord Epsylon, no me habría colocado en una situación de peligro intencionadamente. Aunque, ¿y si él no sabía que me estaban esperando para darme un correctivo ejemplar por la infiltración en el movimiento antisistema…? ¿Y si lo habían utilizado para ponerme un cebo…?

Así transcurrieron las horas, y los kilómetros. La soledad de la moto implica darle muchas vueltas a los pensamientos. Pero la única manera de averiguar si aquel viaje era una encerrona o merecía la pena era darle gas.

Mi vieja Harley Davidson, que ya era añeja cuando la compré de segunda mano para la investigación de *Operación Princesa,* continúa resistiendo los kilómetros, aunque esta vez sufrió con el recorrido. A la pobre, que ya está llena de achaques, se le van cayendo las piezas por el camino. Esta vez perdí un intermitente trasero en algún punto de la ruta. Lo que siempre implica problemas con las autoridades locales.

Unas sirenas encendidas en el retrovisor. Una orden de detenerse en el arcén. Otra multa. Retraso en el viaje.

Llegué una hora tarde al punto de encuentro. El pueblo donde me había citado Epsylon era un auténtico laberinto. Me perdí. Callejeaba apretando el acelerador de la moto, sinceramente inquieto por si el hacker se había cansado de esperarme y se había marchado, haciendo inútil el largo viaje. No tenía forma de contactar con él, Epsylon no tiene teléfono, así que empecé a sentirme realmente preocupado. Habían sido muchos kilómetros y una multa. No me haría ni puta gracia que el viaje hubiese sido en vano. Y de repente, él salió a mi encuentro.

Lo reconocí enseguida. Llevaba el pelo más largo. Y barba. Estaba muy distinto a la fotografía que había encontrado en Google en la que posa, mucho más joven, afeitado y con el pelo corto, al lado de Richard Stallman, pero era él. Sin duda.

Caminaba descalzo, con unas chanclas en la mano, y sonreía.

—Te vi llegar. Y me imaginé que estarías perdido.

El pueblo donde me había citado Epsylon no estaba elegido al azar, sino por sus cualidades geoestratégicas. Desde la Edad de Bronce, fenicios, cartagineses, griegos, árabes, etcétera, todos pasaron por aquella montaña, y en ella, estratégicamente situado, el lugar donde me había citado Epsylon. Allí arriba, en lo alto, existe un punto, donde casualmente está situada la comisaría de Policía, desde el que se controlan los dos únicos accesos al pueblo. Su paranoia era incluso superior a la mía.

Yo estaba agotado por el viaje, pero tras un apretón de manos sincero, conseguí convencerle para tomarnos unas cervezas (las mías sin alcohol), antes de continuar el viaje hacia su «batcueva». Así se refirió a ella, y no iba a tardar mucho en descubrir que no ironizaba…

Durante aquellas primeras horas de charla supe que el esfuerzo había merecido la pena. Lord Epsylon es un creyente. Consecuente hasta límites insospechados con la filosofía original del movimiento hacker.

Epsylon no es un activista de fin de semana, ni un teórico. Tampoco se parecía a muchos «antisistema» de todo a cien que conocí durante la infiltración en la extrema izquierda, jóvenes de la burguesía barcelonesa que acudían al centro social okupa a beber, fumar hachís y escuchar música, mientras lanzaban incendiarias arengas contra la Europa capitalista, antes de volver a sus lujosos apartamentos de Sant Gervasi, Bonanova o Les Corts para dormir entre sábanas de seda. No, Epsylon es un activista 24/7. 365 días al año. Y para ello ha renunciado a muchas cosas… casi todas materiales.

Ante la ausencia de teléfono en su vida, su madre, tan sufridora como la mía con

esto de las nuevas tecnologías, ha tenido que aprender también a manejar el cifrado PGP para poder mantener un canal de contacto con su hijo, cuando se embarca en alguna de las cruzadas que lo han llevado a vivir en locales ocupados de Holanda o Alemania, en un hacklab de Francia, o en misiones hacktivistas en Colombia o Azerbaiyán…

—¿Te parece que nos vayamos a mi casa? Allí podremos charlar con más libertad.

A Lord Epsylon, como a mí, le inspira cierta desconfianza cualquier tipo sentado en la mesa de al lado que te mira dos veces, la camarera que te sirve las cervezas, el encargado del kiosco de la plaza que te observa aburrido desde el mostrador…

—Claro —le respondí—. Donde te sientas más cómodo.

—Vale. Pero antes tenemos que parar a hacer la compra. No estaba seguro de que vinieses y tengo la nevera vacía.

Antes de llegar a su refugio hicimos una parada para comprar productos básicos. Pescado, leche, bebidas… La noche iba a ser larga. La compra de Lord Epsylon fue otra lección de coherencia. Los alimentos, las bebidas, todolo que entraba en su cesta eran productos naturales. Leche de soja, pan de horno, pescado azul y lubina, ricos en fósforo, vitamina D y vitamina B3, de un vivero conocido… Puedes compartir o no las ideas de Epsylon, pero es innegable que él es consecuente con ellas hasta las últimas consecuencias. Incluyendo su alimentación.

Con la compra hecha, seguí su coche durante varios kilómetros, hasta su escondite. Él circulaba delante, pisándole fuerte. En algunos tramos me costó seguirle, cuando dejó el asfalto para meterse por caminos de tierra y la inmensa polvareda que levantaba su coche se me metía en los ojos a través del casco. Me resultaba difícil evitar que las ruedas de la moto derrapasen con la gravilla, haciéndome salir del camino. Una Harley no está pensada para ese tipo de rutas.

Tardamos un buen rato en llegar a su escondite, e intuyo que no fue por casualidad. A pesar de que evité mirar todos los carteles indicadores, supongo que Epsylon se sentía más seguro mareándome un rato para dificultar que pudiese recordar la ubicación de su refugio. No era necesario. Puedo jurar solemnemente que no tengo ni la menor idea de dónde está la casa de Lord Epsylon. No solo por su entretenido paseo por los campos no asfaltados de la zona, sino porque desde el primer instante me propuse no saberlo. Esa es la mejor forma de no delatar a una fuente.

Por fin, lleno de polvo y a punto de estrellarme en un par de ocasiones, llegamos a una pequeña casa de campo perdida en sabe Dios qué lugar. Cuando se refirió a su refugio utilizando la palabra «Batcueva», no lo hacía con ironía. Es que a la izquierda de la entrada existe una pequeña cueva natural cubierta totalmente por los árboles, que utilizaba como garaje para su coche. Imposible avistarlo desde el aire.

—Ahora tenemos que pasar un pequeño ritual —me dijo en cuanto escondió el coche en la cueva—. No te asustes. ¿Le tienes miedo a los perros?

Está claro que cuando alguien te dice «no te asustes», te asustas. Adoro a los animales. Me entiendo con ellos mejor que con los humanos, pero aquella advertencia no resultaba tranquilizadora.

—Vale, haz lo que yo te diga. Tienes que quedarte aquí, de pie, con las manos en los bolsillos y sin moverte. Voy a abrir la verja y va a salir el perro. Se llama Ufo. Te ladrará y te gruñirá un poco antes de olerte. No lo toques, y no te muevas. En cuanto vea que yo te toco en el hombro se calmará y te dejará entrar. Es mi seguridad perimetral.

Así fue. En cuanto Epsylon abrió la verja de acceso a la propiedad, un imponente perro se abalanzó hacia mí, y permanecí firme como un recluta en día de revista, sin mover un músculo. Durante unos segundos Ufo me rodeó rugiendo y ladrando, olfateándome y tratando de discernir si era una amenaza para su amo. En cuanto Epsylon me tocó y le dijo que era amigo, dejó de ladrar. El ritual había terminado.

—Ya está, podemos entrar. Ufo huele las intenciones de las personas. Nunca falla. Cuando alguna vez ha venido alguien que no era de fiar, me lo ha hecho saber, y nunca se equivoca. Pero parece que le caes bien…

—No sabes cómo me alegro. No me gustaría caerle mal. Tiene pinta de ser un adversario duro.

—Es un lobero. Los perros que se utilizan para defender al ganado de los lobos. No le tienen miedo a nada. Hace tres años una mujer que iba a sacrificar tres cachorros me preguntó si quería uno, pero yo soy un nómada, me paso la vida viajando de un sitio a otro y me parecía una complicación, así que le dije que los pusiese en el suelo y que si alguno venía hacia mí, me lo quedaba. Ufo vino directamente hacia mis pies, y desde entonces somos inseparables.

Subimos la pequeña cuesta que conducía a la propiedad, con Ufo escoltándonos fielmente. Ágil, esbelto, elegante. Parecía un pastor alemán, pero su pelaje era más recio, y de color gris oscuro.

—Intenté adiestrarlo para que no durmiese cuando yo duermo, pero todavía no lo he conseguido. Sin embargo, sí ha aprendido a ladrar de una forma cuando se acercan humanos, y de otra cuando detecta animales o quiere algo.

Epsylon no exageraba. Doy fe. Yo mismo podría constatar la eficacia de su sistema de vigilancia perimetral esa noche y al día siguiente.

Al llegar a la vivienda lo primero que me sorprendió es que estaba abierta. Epsylon no necesita cerraduras. La casa era pequeña. La cocina estaba unida al salón. Un dormitorio y el cuarto de baño completaban las dependencias. Me recordó un poco al apartamento que utilicé durante la infiltración de *Diario de un skin.* Austero. Sin apenas decoración. Solo lo imprescindible. Lo que pudiese entrar en el maletero del coche en caso de tener que salir precipitadamente.

Mientras se enfriaban las bebidas y empezaba a arder la leña en la barbacoa, Epsylon me mostró algunos de sus tesoros. Gadgets electrónicos, fabricados por él mismo, que bien podrían ocupar un expositor en el Museo del Espía. Desde una caja

de música incrustada en una vieja caja metálica de galletas, a un receptor de baja frecuencia VLF Inspirer, pasando por lectores RFID. Todos construidos por él: no solo es un hacker sorprendente y un escritor de código erudito; además es un mecánico avezado y un técnico electrónico autosuficiente. Al ver aquellos gadgets recordé una de las conferencias de Epsylon que pude localizar en la red mientras preparaba aquel viaje.[170] Allí había mencionado el proyecto de la creación de teléfonos móviles de madera, alimentados por generadores a pedales. Entonces me pareció una afirmación delirante, pero viendo lo que podía hacer, empecé a considerar que lo imposible es relativo.

Como los primeros hackers, Lord Epsylon es ante todo un científico. Un investigador de las tecnologías, tanto en software, como en hardware. Su casa es un auténtico centro de I+D tecnológico en el que experimenta, ensaya y fabrica nuevas herramientas de hacking. Y no solo a través del código fuente.

Sin embargo, la mayor de las sorpresas estaba sobre nuestras cabezas. Lo seguí hasta la parte trasera de la casa, desde donde ascendimos, por una escalera de metal, al tejado. Allí había instalado una antena parabólica orientada hacia la constelación de los satélites Iridium.

—Yo no tengo teléfono, ni me conecto por cable —me dijo con una sonrisa de complicidad—. Esta es mi conexión a internet. Yo entro por Iridium. Por eso mis IP pueden aparecer en Alaska, Nueva Guinea o el Polo Sur. Yo entro en la red desde el espacio.[171]

Además de sus habilidades tecnológicas, Epsylon resultó un magnífico anfitrión, y un cocinero excepcional. Poco después nos sentábamos en el jardín, disfrutando de unas magníficas lubinas a la sal, y unos deliciosos «solomillos del mar», que preparó en la barbacoa, mientras charlábamos sobre lo que significa vivir como un hacktivista.

Entonces ocurrió algo sorprendente. Le pedí permiso para grabar nuestra conversación, y sonrió con ironía. «Sí, claro, inténtalo». Coloqué la grabadora sobre la mesa, orientando el micrófono hacia el hacker, que hablaba con un buen tono de voz. Hice una prueba de sonido y por suerte la escuché antes de iniciar la entrevista. Menos mal. De lo contrario me habría encontrado con una desagradable sorpresa cuando intentase transcribirla.

Nos envolvía el canto de las cigarras. Y a pesar de que mi grabadora estaba correctamente colocada sobre la mesa, el sonido de los cicádidos solapaba por completo nuestras voces. Se las comía. Mi anfitrión volvió a sonreír:

—Son mi inhibidor de micrófonos natural.

Fascinante. Nada era casual. Epsylon llevaba demasiados años luchando en la primera línea del hacktivismo y todo en su vida era fruto de una dilatada experiencia. Tendría que acercar más el micrófono, y tomar nota manualmente de todo, si no quería perder detalle. Si algún servicio de Inteligencia, o algún periodista, hubiese intentado grabar clandestinamente las actividades de Lord Epsylon, solo habría

podido escuchar el canto frenético de millones de cigarras.

El encantador de códigos

Lord Epsylon lleva muchos años implicado en el hacktivismo. Ya en 2008 lideró a un grupo de hackers españoles que intentó hacer llegar a Bill Gates una serie de planteamientos sobre el poder de la red, colándolos en una entrevista que había concedido a un canal de televisión de Indonesia. En España, el diario *Público* se hizo eco de aquella iniciativa.[172]

—¿Por qué escogiste ese nombre: Lord Epsylon?

—La Epsylon es un concepto matemático. Es lo más insignificante, el resto, los últimos decimales que desprecias en una operación. Sin embargo, son los que te permiten comprenderla totalmente. Es algo así como el inverso del infinito. Cuando se define la convergencia de Cauchy se hace por una épsilon.

—Tú empezaste en la época del IRC…

—Sí, también andaba por allí. Pero pronto me decanté más por el hacktivismo que por la visión comercial o el cibercrimen. Mientras los *whitehats* aspiraban a entrar de consultores de seguridad en cualquier empresa, y los *blackhats* iban directamente a por la pasta, los *greyhats* tenemos otros intereses. La verdad es que en el fondo los blancos y los negros van a por lo mismo: el dinero. Unos robándotelo, y otros cobrándote por protegerte para que no te roben. Pero el hacktivismo juega en otra liga. Nosotros creemos que a través de nuestras acciones realmente se pueden conseguir cosas más importantes que lo material. —Para Epsylon, la definición de hacktivismo es el uso de la tecnología para lograr cambios sociales.

—¿Como qué? ¿Cuál fue la primera acción en la que participaste?

—La campaña contra la SGAE. Fue brutal, porque fue la primera vez que todos nos unimos por una causa. *Whitehats*, *greyhats*, abogados, Anónymous… Empezamos con pequeñas concentraciones, *mail bombing*, ataques… Me acuerdo de que se tumbó la web de los premios Goya, y que tres activistas de Anónymous se colaron en el escenario en plena ceremonia de los premios con la máscara de Guy Fawkes. Además, se hackeó el algoritmo de Google, y cuando ponías la palabra *ladrones* en el buscador, y le dabas a «voy a tener suerte», se te abría directamente la página de la SGAE. Fue glorioso, porque ganamos. Cuando encerraron a Teddy Bautista y toda la peña, demostramos que nosotros teníamos razón. ¿Pirata yo? ¡Pirata tú!

Realmente, el ataque de Anónymous a la Sociedad General de Autores y Editores y al Ministerio de Cultura, conocida como Operación Payback —al menos en su primera fase—, consiguió acaparar la atención mediática.[173]

En protesta por el canon digital y la ley antidescargas, Anónymous organizó un ataque de denegación de servicio contra las web de la SGAE y Cultura, entre otras. Consiguieron tumbar sus páginas web durante algunas horas, indignados por el cierre de lugares como Megaupload. Supongo que su fundador, Kim Dotcom, que se hizo

multimillonario gracias a la piratería, se lo agradeció desde su mansión de lujo…

Sin embargo, en el blog de referencia hacker Security By Default, Yago Jesús, una de las primeras espadas de hacking español, hizo una lectura más crítica del ataque.[174]

—Y ahí empezó tu carrera como hacktivista. Pero como España se te queda pequeña, empiezas a implicarte en proyectos internacionales. Una especie de trabajo social hacktivista…

—Sí, bueno, cosas como llevar internet a pueblos donde no la tenían, montar redes wifi, enseñarles a cifrar las comunicaciones…

—¿Dónde, por ejemplo?

—Uf, por todo el mundo. Estuve en Azerbaiyán, Holanda, Francia, Alemania. En Cali y en Medellín, en Colombia…

—Creo que en Colombia casi te detienen.

—Te cuento cómo lo viví. En realidad, nos escapamos porque salimos en la parte de atrás de un coche del museo en el que habíamos quedado para unas reuniones, porque había dos agentes del DAS preguntando por nosotros. Allí conocí a un activista canadiense que hizo los mapas de todas las explotaciones irregulares que hacía el Gobierno de Canadá en Colombia, y denunció cómo los distintos presidentes del país lo estaban vendiendo a potencias extranjeras. Le ayudé a cifrar su correo, le creé varias cuentas pantalla y le urgí a trabajar con TOR. Después estuve con el sindicato estudiantil, la principal amenaza del Gobierno, que esos años estaba dando mucha caña en varias ciudades de Colombia. Fui en una moto, muerto de miedo, hasta un lugar en la selva. Allí conocí a… digamos que a gente interesante a la par de influyente. Yo fui a poner redes wifi, a dar un curso de cifrado, prácticas de navegación segura y a visitar los hacklabs de la zona.[175] Y mientras pasaba esto, en la televisión local no paraban de hablar del ataque a varias páginas del Gobierno por parte de un hacker español llamado Anónymous. No podía evitar soltar una sonrisa cada vez que lo veía. Otra vez no han entendido nada…

Pero en 2011 Epsylon regresa a España. El 15 de mayo, tras una manifestación convocada por diferentes colectivos indignados con la corrupción política, cuarenta individuos deciden acampar en la Puerta del Sol de Madrid de forma espontánea. Esa misma madrugada los desaloja la Policía. Se producen diecinueve detenciones.

En respuesta, al día siguiente diez mil personas se vuelven a congregar en Sol. Entre ellos Kaótica. Y llegaron para quedarse. Había nacido el Movimiento 15-M o Movimiento de los Indignados. Los indignados toman la Puerta del Sol, el Kilómetro 0 que marca el centro geográfico de España, y allí permanecerían acampados hasta junio, inspirando acampadas similares en otras partes de España, y movimientos «indignados» en toda Europa, Estados Unidos, América Latina… No solo querían ocupar Sol. Querían ocupar la red.

—Me han dicho que tú fuiste uno de los que colaboraron a la hora de crear la infraestructura wifi del campamento del 15-M.

—Uno más, colaboramos muchos. Yo estaba en el extranjero cuando llegó la noticia de lo que estaba pasando en Sol. Me cogí un avión, el ordenador y me fui para allí. ¿Yo qué sé hacer?, pues eso, temas de redes, wifi… Pues eso. Montamos una antena utilizando un palo de una escoba, y gracias a un piso que habían alquilado unos colegas a unas manzanas de allí, conseguimos montar la cobertura para que la peña pudiese conectarse, tuitear lo que estaba pasando, enviar sus mensajes… Si te miras los informativos de La Sexta, verás que yo soy el primero al que pilla la Policía para desalojar la plaza. No sé si iban a por mí o fue casual, pero que soy el primero al que sacan lo puedes comprobar.

Gracias al trabajo de voluntarios como Epsylon o Kaótica, los acampados en Sol tuvieron la oportunidad de lanzar su mensaje al mundo a través de redes como Twitter donde *hashtags* como #spanishrevolution, #democraciarealya, #nonosvamos, #15M, #notenemosmiedo, etcétera, hicieron llegar su mensaje a todos los rincones del planeta.

—Supongo que para vosotros fue como un reconocimiento a años de defender ese mismo mensaje.

—Sí, pero había mucha gente que venía solo a desahogarse. Lo comenté con un sociólogo y me dijo que era normal. Que la gente empezaba a darse cuenta de las cosas y necesitaba expresarlo, pero yo me acuerdo de estar horas y horas trabajando en montar el soporte informático, sentado en el suelo con el culo plano, y estar escuchando todo el tiempo las mismas quejas. Que sí, que los políticos son unos corruptos, que los bancos nos roban… pero nosotros eso ya lo sabíamos. Hasta que al segundo día una chica dijo: «Al 15-M se viene llorado de casa», y todos aplaudimos. Porque no se trata de quejarse, sino de aportar alternativas. Yo te puedo decir: «No uses Facebook, porque están dándole una base de datos al Gobierno de los Estados Unidos», pero además te doy una alternativa…

—¿Te refieres a la red social que se utilizó en el 15-M?

—Sí, Lorea, que significa «flor» en euskera.[176] La pensé, diseñé y programé, junto con otros activistas, mientras estaba en Holanda, y pretende ser una alternativa a otras redes como Facebook, que especulan con tus datos. Loreautiliza diversas técnicas de cifrado, distribución de la información, federación de contenidos y eliminación del rastreo, que asegura el control al usuario para evitar que la información caiga en manos de terceros. Y esa es la red que se usó en el 15-M. En Holanda estuve un año y pico, sobre todo programando, pero como también estaba vinculado al movimiento de okupación, lo simultaneaba con las actividades típicas del grupo: okupar edificios, evitar desahucios, realojar familias de refugiados, defender territorios, controlar a los fascistas Estuve justo cuando la okupación era legal e iba a pasar a ser ilegal. Era un hecho histórico del movimiento y pensé que debía estar allí. Fue para mí un aprendizaje, de la mano de grandes maestros, que abrió mi mente en muchas direcciones. Recuerdo que teníamos más de doscientos edificios controlados por el movimiento y muchos de ellos con familias en exclusión,

hasta que lo ilegalizaron y entonces se lio parda. Manifestaciones,[177] cortes de cables, ataques a comisarías para sacar a gente de las celdas… Pura acción directa.

Lorea fue una herramienta fundamental para la coordinación *online* del 15-M, pero hubo más. En la página de HackSol se publicó una cronología digital del movimiento de los indignados en la red.[178] Auténtica memoria de ese acontecimiento histórico.

—¿Ves? —le dije—. Yo puedo llegar a entender la eficacia o no de las acciones directas, a pesar de las penas de cárcel que implican cuando os pillan… pero no termino de comprender cosas como los *defacements* o los ataques DoS.

—¿Qué es lo que no comprendes?

—Para qué vale, por ejemplo, cambiar la foto de Zapatero en una web oficial, por una de Mr. Bean. Como chiquillada está bien, pero no veo el activismo de esa acción…

El 4 de enero de 2010 la página web oficial de la Presidencia española de la Unión Europea sufrió un ataque de *defacement*. En la página de inicio a la web, la fotografía del presidente Zapatero fue reemplazada por otra del actor Rowan Atkinson caracterizado como Mr. Bean, que, con los ojos muy abiertos y cara de sorpresa, saludaba con un «Hi there» («Hola a todos», en un inglés coloquial).

—No has entendido nada. El ataque a la web de la Presidencia no fue una chiquillada. Cambiar la foto de Zapatero por la de Atkinson solo tenía como misión llamar la atención de la prensa internacional. Y lo consiguió.[179] Todos los medios del mundo se hicieron eco de la noticia. Y lo más importante, del mensaje hacktivista. El Gobierno le había pagado a Telefónica 11,9 millones de euros por aquella página web, y solo hizo falta aprovechar una vulnerabilidad del código llamada XSS *(cross-site scripting)* para hackearla. Era un timo. Una forma de derrochar el dinero de los españoles. Y el ataque a la web era el modo de demostrar el modelo informático de contratación donde el dinero se pierde en despachos y subcontratas, precarizando al programador. Probablemente el autor de esa web era un informático subcontratado, por una subcontrata de una subcontrata de Telefónica, y no cobró ni el 1% de lo que pagó el Gobierno por la página.

Me quedé pensativo unos instantes. Lord Epsylon había conseguido desarmarme. Hasta ese instante siempre había pensado que los *defacement* de Anónymous o de otros grupos hacktivistas eran simples travesuras sin ningún tipo de reivindicación social o política, pero me equivocaba. Ufo movió las orejas y se relamió, como si quisiese decirme «capullo, deja tus prejuicios capitalistas en casa».

Además, a estas alturas ya había conocido a varios de esos programadores, subcontratados por subcontratas de grandes empresas, que son los que realmente hacen el trabajo, por el que otros cobran sumas millonarias. La programación tiene mucho de arte, y como el arte, es difícil ponerle precio. Lo que significa que resulta muy sencillo utilizarlo como tapadera para todo tipo de fugas de capital. Hasta un profundo ignorante podía darse cuenta de que valorar en casi 12 millones de euros la

web de la Presidencia del Gobierno era un fraude a los contribuyentes. Pero Anónymous nos lo demostró con sentido del humor.

—Tiene sentido. Pero ¿y los ataques DoS? ¿En serio pensáis que por tumbar una página web de una multinacional o un Gobierno durante unas horas conseguís algo?

—No seas simplista. Cuando el servidor de una web oficial recibe de repente y de forma simultánea cientos de miles de peticiones, se colapsa y se cae… pero a lo mejor en ese momento es más vulnerable y alguien aprovecha para entrar en el sistema y buscar cosas. Cosas que luego se darán a conocer. Acuérdate de Stratfor…

El 24 de diciembre de 2011 Anónymous atacó la consultoría de inteligencia norteamericana Strategic Forecasting, Inc. (Stratfor). Durante el ataque, los hacktivistas consiguieron entrar en los servidores de la empresa y hacerse con miles de correos electrónicos, así como más de 200 Gb de datos. Esa misma noche se publicó en Twitter un enlace con la lista de clientes de la consultoría, que incluía a financieras como Goldman Sachs o MF Globa, o el Ejército y la Fuerza Aérea estadounidenses.

Pero lo verdaderamente demoledor del ataque es que los activistas consiguieron los datos de las tarjetas de crédito de los clientes de la compañía. Con ese dinero, y a diferencia de lo que habrían hecho los cibercriminales de sombrero negro, los *greyhats* hicieron donaciones millonarias a organizaciones humanitarias como CARE, Save the Children o Cruz Roja. Hay que reconocer que el mensaje en esta ocasión era todavía más claro: robar el dinero de quienes especulan con la guerra para entregárselo a los más necesitados… Por desgracia, al revisar la hemeroteca he visto que pocos de mis colegas periodistas se dieron cuenta de la trascendencia de aquella acción. La mayoría se limitaron a señalar la «gamberrada» de los «piratas informáticos». Pero el ataque a Stratfor tuvo muchas más consecuencias.

Poco después, la página de Wikileaks que publicó la información obtenida en el ataque a Stratfor recibió a su vez el ataque de The Jester.

The Jester es el enemigo natural de hacktivistas como Wikileaks o Anónymous, a pesar de considerar sus acciones como «hacktivismo patriótico». Identificado como uno o más individuos que habían pertenecido a las tropas norteamericanas destinadas en la ocupación de Irak, desde su aparición en enero de 2010 The Jester ha protagonizado los principales ataques contra la web de Julian Assange o el foro 4chan, donde nació Anónymous. Así como contra la página del presidente Mahmoud Ahmadinejad, webs yihadistas del ISIS, etcétera. The Jester demuestra que también existe el hacktivismo de extrema derecha.

A pesar de que en un principio no se detuvo a nadie por el ataque a Stratfor, dos años después, en noviembre de 2013, el conocido hacktivista Jeremy Hammond fue condenado a diez años de prisión por su papel en dicha acción. Hammond fue uno de los hackers a los que Héctor Xavier Monsegur, alias «Sabu» —cofundador del grupo hacktivista Lulzsec—, delató como parte de su pacto con el FBI.[180]

Y es que generalizar siempre es un error. La comunidad hacker no es un remanso

de paz, y guerras como la que mantiene The Jester contra Wikileaks se dan también entre los hackers que visten diferentes sombreros. El Movimiento contra la Seguridad, AntiSec, es el mejor ejemplo. Se trata de una comunidad de *blackhats* y *greyhats* que han declarado la guerra a los *whitehats* y consultores de seguridad, ejecutando ataques contra las páginas de empresas como SecurityFocus, SecuriTeam, Milw0rm, etcétera, así como contra foros, canales de IRC y listas de correo de seguridad informática como «full-sisclosure», «vuln-dev» o Bugtraq. La última campaña de AntiSec se produjo en septiembre de 2015.[181]

—O sea, que los chicos de la máscara de *V de Vendetta* no son solo unos cachondos traviesos…

—Para nada. Anónymous ha hecho muchas cosas. Desde tumbar la web del Mosad en protesta por los bombardeos a Gaza, hasta sufragar la operación de un niño con leucemia, pasando por identificar a los neonazis alemanes o italianos y sus fuentes de financiación, o montones de operaciones contra el yihadismo o la pedofilia en internet. Eso es el hacktivismo. Una filosofía de vida. No un simple pasatiempo.

—Entiendo, es convertir en algo real lo conseguido en el mundo digital, pero ¿siempre son acciones locales?

—Antes, la comunidad de Anónymous de España y las de otros países hispanohablantes libraban sus propias batallas, sin embargo llegó un día en que se aliaron, y ahora Anónymous España participa en las acciones de América y viceversa. Pero Anónymous no es una organización terrorista. Anónymous te avisa previamente de lo que va a hacer, y explica cada acción, los cómo y porqués en sus manifiestos. Aunque la Policía prefiere criminalizarlos y los periodistas pasan de profundizar en el tema. Por eso existe esa idea tan distorsionada.

Durante mucho tiempo yo también había pensado que Anónymous era una agrupación de cibergamberros simpatizantes de la extrema izquierda, sin mayor recorrido. Sin embargo, en octubre de 2010 Antena 3 emitió el documental «Historia de un infiltrado», basado en mi libro *El Palestino.* Por cuestiones de actualidad, el reportaje se centraba principalmente en los capítulos dedicados a Venezuela, obviando todo lo demás. En cuanto se emitió, el canal venezolano antichavista Globovisión pirateó el reportaje, censurando aún más las partes que no le interesaban, y lo emitió sin autorización, ni de Antena 3 ni mía.[182] A partir de ese instante se produjo un fenómeno curioso. Anónymous Venezuela —que en este caso está vinculada a la oposición antichavista, es decir, a la derecha— comenzó a bombardear las redes sociales con mi reportaje, y llegó incluso a manipular el título original, cambiándolo por «El Palestino: Historia de un infiltrado en Venezuela». Obviamente, los lectores de mi libro conocen de sobra mi opinión sobre la política de Hugo Chávez y la relación de los movimientos bolivarianos con organizaciones terroristas como ETA, FARC, Hizbullah. Pero a los internautas parece resultarles más cómodo ver un documental manipulado, que leerse un libro. Y a mí Anónymous Venezuela no me avisó…

—Es que Anónymous al final es solo un heterónimo —continúa Epsylon—. Al ser tan heterogéneo, admite cualquier ideología. Se dice que actúa como una «mente colmena». Con los años y la experiencia en técnicas asamblearias, han desarrollado unos sistemas de consenso que permite decidir colectivamente qué acciones se ejecutan y cuáles no. Y esto se produce porque desde su comienzo tienen su decálogo ético que seguir y saben qué puede hacerse y qué no. Se proyectan.

La historia del hacker español The Lord of Darkness es un ejemplo excelente de que el mero hecho de plantear una acción a Anónymous no garantiza que se pueda lograr un ataque. En 2012, tratando de impresionar al colectivo Anónymous para colaborar con los hacktivistas, The Lord of Darkness saboteó una web neozelandesa que recaudaba fondos para niños con carencias alimenticias. Anónymous no solo no aceptó al hacker madrileño, de treinta y cinco años, en sus operaciones, sino que se movilizó para revelar su identidad.[183] Él tampoco había entendido lo que es Anónymous.

—Sin embargo, también hay batallas dentro de Anónymous, y enfrentamientos entre unas facciones y otras —prosiguió Epsylon—. Es normal, al ser algo tan abierto y heterogéneo entra de todo. Y esa también es parte de su fuerza, ser una idea compartida y no una organización. No hay líderes, por eso cuando la policía dice que ha desarticulado la cúpula de Anónymous, es una estupidez tan grande como cuando aquel poli colombiano decía que yo era el hacker español Anónymous. No tiene sentido. Es verdad que de Anónymous salieron otros grupos, que se independizaron y crearon su propia línea de hacktivismo activo y teórico, pero ya no eran Anónymous. En parte, también buscaban una etiqueta que los diferenciara. Como por ejemplo TeaMp0isoN o Lulzsec…

Lulzsec supuso un fenómeno dentro del mundo del hacktivismo desde su aparición. Su lema: «¡Riéndose de tu seguridad desde 2011!»no deja lugar a dudas. Lulzsec se burlaba de la seguridad informática de las grandes empresas, y protagonizó audaces ataques que ya han pasado a la historia. En mayo de ese año, por ejemplo, y en represalia por la demanda de Sony contra George Hotz, Lulzsec dirigió el primero de sus ataques contra Sony, llevándose miles de datos de sus usuarios.

Un mes después atacaron la PBS y la FOX, en protesta por su documental sobre Wikileaks. La NASA, la CIA o el Senado norteamericano también fueron objeto de sus intrépidas acciones, que detallaban en tiempo real en su cuenta de Twitter. Pero todo terminó cuando, en marzo de 2012 el FBI desarticuló el grupo. Según la historia oficial, Héctor Xavier Monsegur, alias «Sabu», había olvidado ocultar su IP al entrar en un chat vigilado por los federales, obsesionados por dar caza a Lulzsec tras haber sido humillados una y otra vez por los hackers. Aquella IP les permitió seguir la pista de Sabu hasta detenerlo, en marzo del año siguiente. Sabu llegó a un acuerdo para delatar a sus cinco compañeros de Lulzsec a cambio de una reducción en su condena. Hoy Sabu ya está en la calle, mientras compañeros como Jeremy Hammond continúan en prisión.

—Sin embargo, en España sí se ha tratado a Anónymous como una «amenaza internacional de primer nivel» —planteo mientras acaricio la cabeza de Ufo, sentado a mi lado—. Recuerdo aquella rueda de prensa, en junio de 2011, con el portavoz de la Policía mostrando la máscara de Guy Fawkes a los periodistas.[184] O la revelación de la contabilidad del PP. El Gobierno puso una denuncia oficial ante la Guardia Civil contra Anónymous…[185]

—Es que no han entendido nada —repite Epsylon—. Anónymous no es un grupo, es una idea, una dinámica. Personas de distinta ideología, país, raza, que puntualmente se unen para colaborar en un proyecto, aunque ni siquiera se conozcan entre ellas. Por ejemplo, detener a los administradores de un foro donde pasan miles de internautas y cada uno dice lo que quiere es una estupidez. Es como si te detienen a ti porque yo deje un comentario en tu blog, que tú quizá ni siquiera has visto. Lo de la filtración de la contabilidad del PP es diferente. Es curioso comprobar cómo aún hoy la gente se llena la boca de soflamas contra el Gobierno, hablando de la corrupción y los distintos casos que tiene abiertos el PP, de Bárcenas y lo que aún guarda, de la financiación ilegal durante décadas… Coño, pues ya está publicada. Desde julio de 2013 tienes disponible en la red toda la contabilidad del partido del Gobierno, entre 1990 y 2011.[186] Y si te tomas la molestia, como he hecho yo, de compararla con las declaraciones de Bárcenas ante el juez Ruz, verás que coincide.[187] Pero denunciar a Anónymous por eso es tan estúpido como denunciar una idea, pero con la maldad que esconde hacerlo para criminalizarlo.

Anónymous respondió esa misma semana a las detenciones de su supuesta «cúpula» con un ataque a la página web del Cuerpo Nacional de Policía.[188] Que la web de la Policía se viniese abajo por un ataque de denegación de servicio fue el menor de sus problemas. Anónymous llegó a publicar miles de cuentas y nombres de policías, tras atacar un conocido foro policial en la red. En aquel momento me pareció una irresponsabilidad. Fruto de una visión simplista del mundo en el que todos los policías son unos «siervos de los gobiernos fascistas», muy habitual en la extrema izquierda. Pero unos meses más tarde tendría las pruebas de que una acción hacktivista, incluso de buena fe, puede acarrear consecuencias catastróficas por esa conducta irresponsable que solo ve a corto plazo…

Un ejemplo más reciente se produjo en septiembre de 2015, cuando Anónymous atacó la web del Ayuntamiento de Tordesillas, e implantó en su página de inicio un manifiesto contra la ejecución de *Rompesuelas*, el Toro de la Vega torturado ese año como parte de una «tradición cultural». Sin embargo, aquel *defacement* ocultaba un ataque más profundo…

—¿Y cuando apareció Wikileaks? Imagino que para vosotros fue como ver una luz al final del túnel.

—Imagínate… Assange ya era conocido en la comunidad, porque antes de Wikileaks ya llevaba años en el activismo y en el movimiento Cypherpunk. De hecho, una exnovia suya es amiga mía… Pero Wikileaks fue mucho más. Antes ya se

utilizaban las wikis, pero era distinto. Hackeabas una web con un *defacement*, acuérdate de lo que te dije, para llamar la atención, y dejabas ahí la filtración. Por ejemplo, conseguías la contabilidad del PP, hackeabas la web de Endesa y la dejabas allí, y era la manera que tenías de filtrar cosas. Pero, para mí, Wikileaks supuso un lugar con mucha más proyección para filtrar cosas. Tú piensa que los hackers siempre han estado muy solos. Yo saco algo brutal, como la contabilidad del PP, y a quién se la doy… ¿A *El Mundo*, *El País*, el *Telegram*, el *Spiegel*, el *Herald*? ¡No había nadie! Te la podían jugar todos. O como se vio, ganaban dinero con tu filtración. Acuérdate de la primera filtración de Wikileaks. Fueron a la Asociación de la Prensa para darles los documentos y esa peña se lucró. A mí eso no me gustó nada.

De pronto, Ufo se puso a ladrar con un tono más grave del que había utilizado antes, se levantó de un salto y salió corriendo hacia la verja. «Tranquilo, es el vecino que vuelve a casa, ese es el ladrido de humanos», respondió Epsylon sin levantar la mirada de la taza de café.

—Todos los hackers que he conocido son un poco paranoicos… pero tú te llevas la palma.

—No sé si eso es bueno o malo, pero si tratas de tener la mentalidad hacker, comprobarás que tu nivel de paranoia es directamente proporcional a lo que sepas de las cosas. Y cuanto más sabes de cómo funciona todo, más paranoico te vuelves al comprobar los intereses oscuros que oculta. La gente ahora tapa la cámara de su ordenador, pero el micrófono sigue abierto. Y cuando tú sabes cómo te pueden activar el micro para escuchar lo que se dice en la habitación, te vuelves más paranoico y lo cierras.

Supongo que tienen sus razones para esa paranoia, porque ni siquiera Julian Assange está a salvo del espionaje en la embajada de Ecuador en Londres. En septiembre de 2015, el prestigioso diario británico *The Guardian* se hacía eco de una denuncia realizada por Focus Ecuador: Julian Assange estaba siendo espiado por la propia Inteligencia ecuatoriana… Ahora entendía por qué había tantas trabas para llegar hasta él.[189]

—¿Y no es poco exagerada tanta precaución?

—Para nada. Estamos en peligro. Por ejemplo, ahora el CNI nos incluye como una de las ciberamenazas principales: el *malware*, el cibercrimen, el hacktivismo… Y tú me estás viendo. Los gobiernos del mundo nos llaman piratas, terroristas… aunque cuando tienen un problema acuden a nosotros. No somos criminales. El hacktivismo no es solo lo que se lee en la prensa sobre Anónymous. El hacktivismo es el código abierto, el software libre, es Stallman, es Assange, es Snowden. Es una forma de vivir y una actitud hacia el mundo.

—Vale, todo eso está muy bien. Pero si alguien decide vivir del cine, la música, o de los libros, y en vuestra política de que todo sea libre y abierto fomentáis la piratería, estáis jodiendo a mucha gente que solo quiere vivir de su trabajo.

—Bueno, se está jodiendo el modelo antiguo que están usando. Pero hay otros

modelos. Tus libros y tus películas, tu trabajo, es tan válido y justo como cualquier otro que se desarrolle alrededor. Pero el problema está en los intermediarios y en sus formas. Supongo que no estarás de acuerdo en que yo pague un canon por conectarme a internet, por si me da por bajarme contenido con copyright. Es decir, que me criminalicen, antes de siquiera comenzar a usarlo. Es darle la vuelta al principio de presunción de inocencia. Entiendo al artista, pero no comparto el intermediario. Creo que el artista debe estar en contacto directo, tanto con su arte, como quienes lo disfrutan. Si te juntas con una mafia, lo siento, pero te señalaré como parte de ella hasta que no vea que deseas cambiar esa situación, al menos, desde dentro. Si no es así, mi ideología libertaria de compartir siempre prevalecerá por la de los intereses de unos pocos. Teddy Bautista tenía en su despacho una bola del mundo hecha de ébano de más de 100.000 euros para servir copas. Si este es tu modelo, créeme, algún día dejarás de poder pagarte todo con él. Por cierto, somos los mismos que hemos puesto a tu disposición totalmente gratis el correo electrónico, las plataformas de vídeo y distribución de contenidos de manera neutral. No lo olvides. No somos nosotros quienes te quitan el pan, precisamente.

No me convenció el argumento. Mis libros, como las películas o la música de otros autores, son mi única fuente de ingresos, y la única financiación de mis investigaciones. Aquel viaje se había pagado, como todos los realizados para este libro, con los derechos de autor de mi libro anterior. Y ese, con los del previo. Y así sucesivamente. Si yo o cualquier otro escritor, músico o director de cine quisiese utilizar otro modelo, debería tener derecho a escoger, y no a que me lo impusiese una piratería amparada por una supuesta ideología libertaria. Una piratería con la que otros, como Kim Dotcom, llegan a hacerse millonarios, sin ni siquiera haber arriesgado en la creación. Pero no estaba allí para defender mis derechos como autor, sino para comprender el hacktivismo…

—Okey, lo de Wikileaks me queda claro. Y de pronto aparece Snowden. ¿Qué supuso para el hacktivismo?

—Para mí es un ejemplo del *whitehat* que se pasa al sombrero gris. Es un tío que tiene su vida montada. Que tiene un trabajo, un buen sueldo, además en una agencia gubernamental, y de pronto decide arriesgar todo eso para decir al mundo cómo nos están espiando. Para mí eso es la hostia. Ojalá todos los hackers de empresa, los consultores de seguridad, tuviesen el valor de hacer lo mismo. Como hizo Falciani con la banca suiza. Para mí eso fue lo más importante. En segundo lugar, toda la comunidad seguimos con mucho interés la reacción de los gobiernos y la Policía, porque lo que le pase a Snowden nos podía pasar a cualquiera. Y de hecho, en muchos países se endurecieron las penas por filtración de secretos a raíz de esto. Y en tercer lugar, a mí no me interesó tanto lo que Snowden contaba sobre lo que la NSA hace, que eso ya lo podíamos intuir, sino lo que no puede hacer. Por ejemplo, cuando él revela que la NSA no puede romper el cifrado PGP, eso es importante, porque me enseña a partir de dónde puedo empezar a moverme. A partir de qué nivel de cifrado

puedo escribir mis códigos para que sean indescifrables y por tanto seguros. Pero no podrán ganar nunca, es una guerra que tienen perdida…

—¿Por qué?

—Porque ellos son funcionarios. Trabajan por un sueldo. Y nosotros creemos en lo que hacemos. Por eso nunca podrán ganar…

Por unos instantes se hizo el silencio. Yo miraba fijamente a Epsylon y Ufo nos miraba a los dos. Realmente hablaba en serio. A esas alturas ya tenía claro que aquel escritor de código creía firmemente en lo que decía. Y vivía en coherencia con lo que creía. Pocas veces me había enfrentado a un hacker que tuviese las ideas tan claras, a pesar de que pagase un alto precio por ello. No solo económico. Todos sus esfuerzos por proteger su conexión al mundo a través de la red contrastaban con su soledad en el mundo real. En aquel momento su única familia cercana era Ufo.[190]

—Supongo que el problema es que os ven como un terrible peligro potencial. Sobre todo cuando amenazáis el poder de los gobiernos, los ejércitos o la banca… Por ejemplo, lo de los Bitcoins… Eso puede suponer una revolución, ¿no?

—Satoshi, el creador del Bitcoin, nos dejó un mensaje oculto en el propio código. Nos decía que la manera de acabar con el capitalismo es encontrar la forma de distribuir y crear nuestro propio dinero. Toda una declaración de guerra al capitalismo escrita en el código. Al principio tuvimos muchas dudas de si podía ser una nueva maniobra de J. P. Morgan o Goldman Sachs o alguno de estos, que hayan sacado el Bitcoin para llevarnos a un capitalismo electrónico. Y todavía no lo sé, porque nadie sabe quién es Satoshi, pero desde luego el código es una obra maestra, y los comentarios parecen más de un anarquista que de un programador de una empresa.

Satoshi Nakamoto es el autor o autores del protocolo Bitcoin, la moneda electrónica de más éxito en los últimos tiempos. En 2008 alguien con ese nombre publicó un artículo en la lista de correo sobre criptografía Metzdowd, describiendo un sistema P2P de dinero digital que pudiese burlar el monopolio de la banca internacional. Como otros escritores de código antes que él, Satoshi entregó su creación a la comunidad, antes de desaparecer en la red tan misteriosamente como había aparecido. No se conoce su identidad real. Y a pesar de que en su perfil se identificaba como un varón japonés de treinta y siete años, muchos autores sugieren que su dominio del inglés es demasiado perfecto para ser japonés, y que el código del Bitcoin es demasiado genial para haber sido escrito por una sola persona. Además, Satoshi nunca escribió nada en japonés.[191]

—De vez en cuando se publican noticias sensacionalistas que anuncian «¡Ya sabemos quién es Satoshi!», «¡Satoshi detenido en los Estados Unidos!». Pero siempre es mentira. ¿Cómo van a detener a Satoshi? Un tipo que ha sido capaz de crear una arquitectura distribuida de intercambio de bienes y transferencias, que es lo que viene siendo el Bitcoin, ¿tú crees que va a ser tan tonto de dejarse pillar? Un tipo al que querría matar muchísima gente de la banca. Además, liberó el código, nos lo entregó y ahora han salido miles de monedas clones del Bitcoin. La que yo he creado

está inspirada en él.[192]

—¿Tú has creado tu propia moneda?

—Sí, el Ecoin. Lo tienes todo en la página Myecoin.net. Bitcoin nos enseñó el camino, y ahora hemos ido mejorándolo. El Bitcoin te da la posibilidad de ser tú el creador de dinero. Como hace la Reserva Federal en los Estados Unidos, una empresa privada, con los dólares americanos. En la historia hemos encontrado sistemas similares, como por ejemplo el de una antigua tribu africana, que utilizaba conchas recogidas directamente del mar como dinero o material de intercambio de bienes y servicios. Es decir, cuando necesitaban comprar algo, se iban a la costa, buscaban las conchas, cogían las que necesitaban y compraban lo que querían. En ese momento las conchas entraban en un valor real de transferencia. Se materializaban como valor de confianza. Y esa sociedad funcionaba. Imagínate que vivimos en una sociedad en la que el dinero lo encuentras. Al capitalismo en el que vivimos no le entra en la cabeza algo así. Creen que entonces nadie trabajaría, y no es así. Tú tienes que trabajar para conseguir los bienes que tú intercambias por esas conchas. Pero en vez de ser un banco, o una empresa privada la que te dé el dinero, lo creas tú. Y eso te da mucho poder. Porque si tú quieres vivir mejor, gastarás más tiempo en conseguir más «conchas», pero si estás bien con lo que tienes, no necesitas más.[193]

—Pero no entiendo bien que tiene eso que ver con los Bitcoin. No creo que se encuentren en las costas…

—No, en el modelo Bitcoin tú eres el minero. ¿Qué es la minería en el Bitcoin?, la cadena de bloques. Los bloques son unas piezas algorítmicas únicas, como la moneda. Si coges un dólar, verás que tiene impreso un número de serie que lo hace único. Con el Bitcoin, a través de unos cálculos matemáticos que hace el procesador de tu máquina, calcula todos los números de Bitcoin que ya existen, y genera un número nuevo, único. Y ya tienes tu Bitcoin. Entre toda la comunidad se han creado todos los Bitcoin que circulan por la red. ¿Qué pasa ahora?, pues que hay tantos millones de Bitcoins que no te compensa el gasto de tiempo y energía que necesita tu ordenador para minar números nuevos. Y es una carrera que tenemos perdida, porque ahora ya se han puesto especuladores de gobiernos, de grandes empresas, con cadenas de equipos supersofisticados para generar Bitcoins, y nosotros no podemos competir. Al principio las conchas estaban ahí y cualquiera podía cogerlas, pero ahora las conchas pesan cada vez más, y solo los gobiernos que tienen tecnología, excavadoras, etcétera, pueden cogerlas.

—Y por eso han aparecido las nuevas monedas…

—Exacto. Ahora, lo que necesitamos es que estas monedas digitales se utilicen. Que los comercios los acepten, que la gente confié en ellas. Por ejemplo, hoy un Bitcoin vale 297 euros, más que el euro o el dólar. El valor depende de lo que la gente confíe en la moneda. Por eso debemos entender que este tipo de criptoeconomías no son un fin en sí mismo, sino un medio para presentar una alternativa socioeconómica, al capitalismo voraz de la banca y financiero, basado únicamente en la especulación y

la usura.

Desgraciadamente, y como toda forma de dinero, el Bitcoin ya ha entrado en el circuito criminal. En mis incursiones en la Deep Web me di cuenta de que era la moneda preferida por los ciberdelincuentes para que el contratante abonase sus servicios. También existen páginas para el «blanqueo» de Bitcoins.

—Satoshi era un escritor de código, como tú.[194] ¿Qué os diferencia de un hacker normal?

—Bueno, también puedes incluir a los hackers como escritores de código. Si te refieres a un *pentester* o a un consultor de seguridad, generalmente ellos usan las herramientas que hacemos nosotros. Cuando escribes un código, tienes que pensar en todas las opciones que puede tener el usuario cada vez que pincha en un botón. Tienes que anticiparte a todo.

—Sin embargo, a veces se os olvida algo, ¿no? Eso son las vulnerabilidades…

—Exacto. Así es. Por eso es tan importante el código abierto. Porque así todo el mundo puede leer tu código, comprenderlo y perfeccionarlo. Tim Berners-Lee, él fue el programador de la World Wide Web, la WWW de internet. Linus Torvalds inventó el kernel (núcleo) de Linux y Richard Stallman desarrolló el GNU, sistema operativo. Podían haberlo patentado y hacerse multimillonarios, pero nos lo regalaron gratis. Y su código dice mucho de ellos.

—¿A qué te refieres?

—A que cuando lees un código, puedes deducir cómo es el programador que lo escribió. Ahí puedes ver la abstracción y el nivel intelectual de la persona, por cómo resuelve los problemas. Si es una persona impaciente, ambiciosa, previsora… igual ha dejado un bloque para integrar otro código en el futuro. No sé. O al revés, si es un chapuzas que resuelve con un bucle o con cualquier chorrada parecida que consume mucho procesador cuando podría haberse hecho de otra manera. Puedes ver muchas cosas.

Ufo no perdía comba de la conversación. Sin apartar la vista de Epsylon nos escuchaba como si realmente pudiese comprendernos. Incluso como si pudiese comprender mejor que yo mismo las explicaciones técnicas del hacktivista.

—Pues no lo entiendo, Epsy. Un tío con tus conocimientos podría estar forrado. Me consta que las empresas de seguridad informática se pelean por contratar a tipos con tu perfil, y sin embargo tú te niegas a entrar en el sistema. ¿De verdad se puede vivir así? ¿Cómo te ganas tú la vida?

—Yo también he estado y sigo estando en el sistema, de un modo u otro. A veces he estado mucho más alejado, en comunas, y otras veces más cercano, en grandes ciudades. Además, he trabajado puntualmente para empresas. De todas maneras, lo que tenemos que entender es que el dinero no es la única forma de cobrar por tu esfuerzo. Y no te hablo ya del criptodinero. Lo que quiero decir es que si yo consigo que alguien me dé una caja de tomates, o pasta, o leche, por hacerle una página web, también vale para seguir viviendo sin ser utilizado como valor productivo por algo o

alguien que va en contra de mis principios individuales. Por eso uno de nuestros proyectos es Codejobs.org; un portal, tipo Infojob, pero para que los programadores puedan poner cuáles son sus necesidades para vivir, y encontrar un trabajo en el que le puedan pagar en base a ellas. Como una especie de Crowdfunder, pero en lugar de con dinero, con lo que necesites para vivir.

»Otra forma es ganar premios. Yo por ejemplo una manera que he tenido de subsistir, al mismo tiempo que hacía trabajo científico, es a través de empresas o fundaciones o universidades, que ofrecen un premio, 2.000 o 3.000 euros, por solucionar un problema técnico, o por desarrollar tal programa, o por crear un plugin. Siempre de software libre, por supuesto. Y las hay. En España no, pero fuera sí.[195] Si juntas eso, con otra forma de vivir, de ver la vida y de consumir, puedes hacerlo. Puedes vivir de puta madre y ser consecuente con tus principios, como trato de hacer yo. Y lo tengo claro, si yo puedo, lo puede hacer cualquiera. No hay nada especial. Es constancia. Entiendo que no tienes la seguridad de un sueldo. Que a veces va bien y otras no tan bien, yo las he pasado putas más de una vez. Pero te sientes mucho más realizado como persona. En vez de aportar tu código a una empresa que lo va a cerrar y lo va a usar para lucrarse, estás aportando algo al resto del planeta. Estás contribuyendo a la parte científica, que es lo que nos gusta y en definitiva, lo que nos mueve.

—¿Y los hackers que trabajan para una empresa de seguridad informática?

—Yo respeto a todos, *whitehats, blackhats…* pero me parece que en el fondo, salvando las distancias morales, viven de lo mismo. Los sombreros negros, de robarte el dinero, y los sombreros blancos, de venderte protecciones contra ellos. Pero ¿si no hubiese ciberdelincuentes, de qué iban a vivir los consultores de seguridad? ¿Conoces al mítico GriYo? Era un escritor de *malware*…

—Sí, claro —ahí pude apuntarme un tanto ante Lord Epsylon—, el que escribió el virus contra ETA.

—Exacto. GriYo es un genio del *malware,* y al final terminó fichado por una gran empresa. Y él decía que para unos era un hijo de puta por crear esos virus, pero para otros era un genio.

Lord Epsylon es muy expresivo. Mientras gesticulaba, me fijé en sus tatuajes. No estaban hechos en la parte exterior de los brazos, como los lleva el 90% de la gente, sino en la cara interior. Seis símbolos. Tres en cada brazo. Y cuando me interesé por ellos, nueva sorpresa

—Los llevo hacia dentro porque son para mí, no para que los vea la gente. Son para recordarme quién soy y de dónde vengo.

—Pero ¿qué significan?

—Todos son símbolos relacionados con las matemáticas. El primero es el Glider, el símbolo de la cultura hacker. Este es la letra épsilon, por razones obvias. Este tiene que ver con los copos de nieve, que nunca son iguales pese a utilizar figuras simétricas, y es, en parte, el símbolo del Ecoin, la criptomoneda que he hecho. Esto

es la «media vida», presente en la estructura atómica y aún inexplicable por la ciencia. Esta espiral representa el cromosoma, el número áureo, las constelaciones, en la naturaleza hay muchas cosas que nacen y desaparecen como espirales. Este triángulo representa la pirámide del poder invertida: los poderosos abajo y el pueblo, que es la mayoría, arriba. Además, representa al ser humano, porque la naturaleza es más proclive a hacer círculos, toroides, y el triángulo es la anomalía, como el ser humano o el cerebro, el único órgano del cuerpo que trata de comprenderse a sí mismo. Y claro, cada uno tiene su historia. El momento en que lo hice, cómo me sentía. Yo no sé hacia dónde voy, hacia dónde me llevará la vida, pero si, por ejemplo, dentro de unos años me sorprendo a mí mismo trabajando como consultor de seguridad en una multinacional y dejando de lado totalmente mi anterior forma de vida, o en cualquier actividad que vaya contra mis principios, solo tengo que mirarme los brazos para recordarme quién soy y de dónde vengo.

Cómo hackear un satélite

Lord Epsylon siguió descubriéndome el fascinante modo de ver la vida del hacktivismo durante horas. De hecho, nuestra primera conversación duró dieciséis horas ininterrumpidas. Yo estaba agotado por el viaje, y por momentos me costaba mantener los ojos abiertos, pero Epsylon me había prometido una demostración práctica. Y la hora se acercaba.

—Y ahora tu próximo objetivo son los satélites… —le dije.

—Entre otros. Pero sí, claro. Es obvio. Hay que señalar todo lo que no nos guste. Y no solo lo que podemos ver. Es decir, la gente se preocupa por si le pinchan el teléfono, por si le activan la webcam, y va descubriendo la cantidad de cámaras y sistemas de reconocimiento que pueblan las ciudades y lugares… Y sin embargo, no son conscientes de que cada día pasan sobre sus cabezas y muchas veces sin permiso y para usos de control montones de satélites que hacen fotografías y mediciones. Y la verdad es que para mí este mundo de mirar hacia el cielo y buscar ahí respuestas a preguntas que no puedo responder desde la tierra fue y es todo un reto personal. Así que empecé comprobando si realmente el hombre había ido a la luna o si era un mito…

—¿Perdona?

—Ya te he dicho que cuanto más sabes, más desconfiado te vuelves, y yo ya no me creo casi nada. Así que, como mucha gente dice que lo del viaje a la luna fue un montaje, quise comprobarlo. Según la historia de la NASA, los astronautas dejaron unos espejos en la superficie de la luna. Entonces unos colegas radioaficionados y yo decidimos comprobarlo. Hicimos unos experimentos con radiofrecuencia, enviando una señal a la luna para ver si rebotaba en los espejos y venía de vuelta y es verdad. Yo he comprobado, quizá con algo más que argumentos históricos, que el hombre ha estado en la luna. Aunque de todas maneras, aún no lo tengo tan claro.

»Así que ya puestos en mirar al cielo, empezamos a investigar el tema de los satélites.[196] Porque queríamos denunciar que el espionaje no viene solo del *malware* de las agencias de seguridad o de los cables de red que transportan la gran mayoría de la información de internet. Queríamos demostrar que desde ahí arriba también nos espían, así que teníamos que encontrar la manera de pillar la señal y meternos en sus sistemas para saber qué uso se estaba dando. Ya sabes, hay mucho oscurantismo en la tecnología espacial y quizá la ciudadanía deba saber realmente por qué…

Hasta ese momento, y a pesar de que la conversación con Epsylon me llevaba de sorpresa en sorpresa, todo me parecía más o menos plausible. Pero la aseveración de que podía hackear la señal de un satélite me resultaba increíble. Lo bueno es que él estaba dispuesto a demostrarlo.

—¿Falta mucho?

—No mucho. Mira —me dijo mostrándome la pantalla de su ordenador—. El

satélite está a punto de pasar. Falta 1 minuto y 30 segundos… Te puedo decir la altitud y la velocidad a la que va. Pasará a 875 kilómetros de altitud y a 7.430 kilómetros por hora. O sea, que va a toda hostia…

Según la web, el satélite cuya comunicación estábamos a punto de interceptar pasaría sobre nuestra posición a las 5:17 de la madrugada. Por suerte el cielo estaba despejado, y nos permitía disfrutar de una luna llena preciosa. Forcé la vista intentando localizar entre las estrellas el puntito blanco que revelase la situación del satélite objetivo de la demo. Epsylon había comenzado su investigación fabricándose su propia antena, con un trozo de madera y unos radios de bicicleta. Después la perfeccionó consiguiendo una antena direccional más sofisticada y un conector específico para el ordenador.

—Esto nos calcula el efecto doppler… Okey, ya lo tenemos. Va a aparecer justo por allí. —Epsylon, señalaba con el dedo algún punto en el horizonte, sin dejar de mover el ratón sobre la pantalla y teclear comandos para mí indescifrables.

—Pero ¿esto es legal? —pregunté al tiempo que cogía la cámara de vídeo que tenía sobre la mesa, entre tazas de café—. ¿Puedo grabarlo?

—Claro. El satélite emite esos pitidos que estamos recibiendo por aquí. —Señaló un bip-bip monótono que asomaba a través de los altavoces del ordenador—. Ese sonido en realidad son datos, en este caso imagen, y lo que estamos haciendo ahora es decodificando esos datos para ver la imagen. En realidad, no estamos vulnerando el sistema, simplemente accedemos a él a través de lo que emite sin restricción de seguridad alguna.

Mientras Epsylon tecleaba en su ordenador, yo conectaba la cámara de vídeo planeando desde la computadora hacia el cielo, en un intento de seguir la conexión invisible que el hacker había establecido entre su máquina y el satélite que, puntual como un ejecutivo británico, apareció en el cielo y en la pantalla del ordenador.

—¿Y esto puede hacerse con cualquier satélite?

—No con cualquiera. Hay muchas más cosas. Pero bueno, es un comienzo para conseguir llegar a satélites modernos y otros objetos espaciales. La ISS,[197] etcétera. Yo por ejemplo tengo fichados ya todos los de televisión, transmisiones aéreas o marítimas, y demás. Y me encantan los militares, que tienen muchísimo más rango de cobertura y algunos son capaces de recibir y emitir en varios continentes al mismo tiempo. Vamos, que lo que sale en algunas pelis de cómo interceptan la señal y la solapan para que aparezca en las pantallas otro mensaje diferente al emitido por el satélite es teóricamente posible. A mí solo me falta una antena y un receptor más potente para llegar a ellos. Y conocer más en profundidad los lenguajes de bajo nivel o específicos, en los que muchos están escritos. Así que de momento y de forma casi lúdica, me conecto a los meteorológicos para experimentar. Pero tampoco hago nada nuevo. Ya lo hicieron otros hackers, por ejemplo irrumpiendo en una televisión de Reino Unido e interfiriendo la señal para poner a unos payasos bailando…[198]

No era un farol. Epsylon continuó manipulando el teclado hasta sincronizarse con

el satélite. Y cuando pasaba sobre nosotros, *clic*, sonríe al pajarito… Ufo, como si lo entendiese, o quizá solo imitando nuestro movimiento de cabeza, también miró al cielo. El lobero también quería salir en la foto.

Poco a poco la imagen comenzó a cargarse en la pantalla, componiendo, lentamente, la fotografía «robada» al satélite. Fascinante. Como todo hacktivista, Epsylon no se limitaba a denunciar una situación, sino que utilizaba sus conocimientos científicos para aportar las pruebas de su denuncia. En este caso la vulnerabilidad de los satélites que cada día sobrevuelan nuestras vidas.

—Increíble, Epsy. Pero… supongo que si esto puede hacerlo cualquiera con unos conocimientos técnicos apropiados… Uf. ¿Te imaginas lo que podría hacer por ejemplo el Ejército Islámico? Ellos también están haciendo una especie de hacktivismo del yihad, y han aprendido a usar internet como nunca antes…

—No nos mezcles con esa gente. Ellos pueden aprovechar las redes sociales o internet para difundir su propaganda, como hacen todos los demás, pero eso no es hack. Yo baso mi activismo en la carta fundamental de los derechos humanos. Y todo lo que se base en eso para mí es activismo. Lo demás es ideología, política o propaganda.[199]

Entendía su razonamiento, pero esa Carta Fundamental también podría aplicarse al hacktivismo de los «sombreros grises»:

art. 3: «Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona» (no parece compatible con lo de difundir nombres de policías).

art. 12: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia» (pero en el ordenador sí, claro…).

art. 23: «Toda persona que trabaja tiene derecho a una remuneración equitativa y satisfactoria» (salvo si los piratas deciden que no la merece si no es bajo sus reglas).

art. 27: «Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora» (pues eso mismo es aplicable a la piratería…).

Mi cerebro estaba a punto de resetearse. Agotado, pero absolutamente fascinado, entré en la casa. Necesitaba dormir, aunque antes tendría que inflar, a pulmón libre, la colchoneta de playa que Epsylon tenía como único cuarto de invitados. Allí mismo, en medio del salón cocina, intentaría descansar un poco y ordenar las ideas. Por la mañana continuaría el aprendizaje. Esta vez Epsylon me daría algunos consejos sobre seguridad en las comunicaciones alternativas a los programas bajo tutela de empresas y cifrado nivel usuario en general.

Cuando ya estaba tirado en la colchoneta, cubierto solo con una toalla de baño como única manta, sentí que alguien se acostaba a mi lado, acurrucándose contra mi cuerpo. Era Ufo. Supongo que no le caí mal después de todo… Me dormí imaginando las cosas fantásticas que aquel lobero, noble y leal, habrá visto hacer a su humano con el teclado de su ordenador.

MAYO DE 2015
LA PISTA TELEFÓNICA

«Es difícil que exista un tema que un hombre pueda pensar sin que otro hombre lo haya pensado antes.»

Adolf Hitler, recogido por su secretaria Christa Schroeder

En su email del 13 de diciembre de 2014, MarkoSS88 me había facilitado dos teléfonos de contacto. Y ante las dificultades que estábamos teniendo para avanzar en la investigación, decidimos intentar quemar también esos cartuchos.

Llegué a hacer uso de ellos. Quería escuchar su voz. Pero MarkoSS88 no me lo iba a poner tan fácil.

Busqué un locutorio telefónico. No quería que Markos tuviese mi número, pero tampoco quería que desatendiese la llamada de un número oculto, y en estos casos un locutorio es la mejor opción. El receptor solo verá un número de teléfono convencional en la pantalla de su receptor. Podría ser cualquiera.

Llamé primero al 634… y después de dar señal, la llamada era derivada a lo que parecía un fax o un módem. A través del auricular no pude escuchar más que ese característico pitido irregular. Lo intenté varias veces. Muchas. Pero nadie contestó nunca.

Probé suerte con el 668… Igual. El teléfono daba tono una vez y después

saltaba una especie de contestador automático en el que no se había grabado mensaje alguno. Todo muy misterioso.

«Está bien —pensé—. Si no quieres atender por las buenas, será por las malas».

Existen muchas formas de obtener información de un teléfono de forma legal. Hacking web. Algo tan simple como introducir el número en la casilla de Facebook Login te permite averiguar si existe alguna cuenta de Facebook asociada a ese teléfono, y de ser así ya tienes un nombre y una foto. Pero no era el caso. Markos, que lo sabía, no había asociado ninguna cuenta a ninguno de sus teléfonos.

En internet existen páginas web que pueden usarse para obtener otra información sobre teléfonos móviles. www.checkwa.com, por ejemplo, es una web que te permite introducir un número de teléfono y averiguar si utiliza WhatsApp. Y no solo eso. Te permite acceder a su foto de perfil y a su último estado actualizado…

Pero, sorprendentemente, Markos no utilizaba WhatsApp. En ninguno de sus números de teléfono. Obtuve los mismos resultados recurriendo a otras armas legales de hacking web, es decir: ninguno. Así que habría que intentarlo de otra manera.

No fue difícil averiguar a qué compañía telefónica pertenecía cada uno de sus números. En internet existen muchas páginas que revelan esa información.

El 634… pertenecía a Vodafone.

El 668… pertenecía a Parlem.

Que utilizase un teléfono de Vodafone era natural. Es una de las compañías telefónicas con mayor número de usuarios en España y lidera la captación de nuevos clientes en el mercado español desde 2004: era buscar una aguja en un campo de pajares. Parlem, sin embargo, era todo lo contario. Una pequeña empresa de telecomunicaciones con sede en el 161 de la calle Laguna, en Barcelona, activa desde 2014, y que operaba a través de la red Orange.

—¿Y ahora qué? —les pregunté a mis amigos policías—. ¿Cómo avanzamos?

—Pues si no judicializamos, malo —respondió Pepe—. Si pones denuncia, está chupado, porque con todo lo que tenemos el juez nos autorizaría la intervención de los teléfonos sin problema y enviaría un requerimiento para identificar a los usuarios. Pero ya sabes lo que pasa si pones tu nombre en un papel…

Sí. Lo sabía perfectamente. La verdad es que me planteé muy en serio interponer una denuncia contra Markos, por amenazas, solo para poder averiguar su identidad. Pero me parecía, y sé que sonará absurdo, como una

traición a su confianza. No me parecía correcto.

Además, Pepe se refería a otra cosa. Obviamente no podía interponer una denuncia con mi número de Testigo Protegido de la Fiscalía. Solo podía ponerla utilizando mi nombre real. Y si prosperaba, el abogado de Markos tendría acceso a ese documento antes del juicio y por tanto al fin descubriría lo que tanto ansiaba. Tampoco parecía una buena opción.

—Vale, y si prescindimos de la judicialización, ¿qué nos queda?

—Rezar.

No me pareció una respuesta satisfactoria.

—A menos… —añadió Álex— que conozcas a alguien que trabaje en esas compañías.

—Yo puedo mover lo de Barcelona —dijo Manu—, conozco a mucha gente, pero lo de Vodafone se escapa a mis recursos.

—Pues no se me ocurre otra manera. Si no vamos por la vía judicial, solo alguien que esté dentro de las compañías puede acceder a esa información.

Mis amigos tenían razón. Sin una orden judicial era imposible ir más allá. A menos que seas un periodista con muchos años de experiencia en el periodismo de investigación y nunca hayas quemado tus fuentes.

Capítulo 19
El oscuro futuro que nos espera

«Para cambiar radicalmente el comportamiento de un régimen tenemos que pensar con claridad y audacia, porque si algo hemos aprendido, es que los regímenes no quieren que los cambien. Tenemos que pensar más allá de lo que lo hicieron quienes nos han precedido y descubrir cambios tecnológicos que nos den valor para actuar de formas que nuestros antepasados no pudieron.»

Julian Assange

Biografía de un hacker

En realidad, ya conocía a Román Ramírez, aunque jamás habíamos intercambiado palabra. Además de en la RootedCON, me había cruzado con él en otros eventos informáticos, a los que yo siempre acudía solo y tratando de pasar lo más desapercibido posible. Por eso, aunque David Pérez o Israel Córdoba me habían preguntado en muchas ocasiones si quería que me lo presentasen, siempre les pedí discreción. Hasta el Ramadán de 2015. Una tarde de verano, un verano especialmente caluroso, David —el todavía policía de la Brigada de Investigación Tecnológica del CNP— organizó nuestro encuentro. Aquella primera reunión fue una simple toma de contacto. Yo me sentía un poco débil y preferí aguardar a que pasase el Ramadán para volver a encontrarnos, y poder charlar cómodamente y con tiempo.

Sus primeras palabras cuando nos presentaron me parecieron un ejemplo demoledor de cómo se falsea la información en la red…

—Así que tú eres Antonio Salas… Yo creía que eras el ufólogo chalado que sale en internet.

Curiosamente, Román se refería justo a la identidad que me achacaba MarkoSS88 en su blog para atraer visitas.

—Tú mejor que nadie deberías saber que no pues creerte todo lo que leas en la red.

—En eso tienes razón…

Al estrechar su mano me di cuenta de que en la cara interna del antebrazo derecho llevaba un tatuaje. Era el candado, símbolo de la Rooted, y aunque Román tiene argumentos de peso para abominar del hacktivismo, tiene más cosas en común con Lord Epsylon que un tatuaje en la cara interna del antebrazo. Quizás para recordarse quién es…

Responsable de arquitectura de seguridad en una de las multinacionales españolas más importantes del mundo y uno de los organizadores de la RootedCON —posiblemente la reunión de hackers más importante de Europa—, Román Ramírez se confiesa anarquista, y además un apasionado de la literatura. Pocos en la comunidad hacker saben que es autor de alguna que otra novela fantástica escrita bajo el pseudónimo de Jon Eldritch.

Román tampoco viste con sudadera ni usa capucha. Ni se dedica a reventar sistemas. Ni roba vidas ajenas. Es un hacker de sombrero blanco.

—¿Cómo empezaste? ¿Tú también eres de los que ya manejaban un teclado antes de aprender a andar?

—No, qué va. Yo empecé muy tarde. Mucho más que la mayoría de los hackers.

Román pulveriza el mito de que los hackers comienzan a trastear con los ordenadores siendo unos adolescentes. En su caso las limitaciones económicas impidieron que pudiese disponer de un equipo propio hasta tener una cierta edad, pero en cuanto pudo, empezó a hackear…

—Empecé a conocer a gente interesante, a visitar las BBS, FIDONet, etcétera. Empecé haciendo *trading*, a mercadear con cosas. Por ejemplo, conseguía acceso a una universidad, sacaba todas las cuentas de los profesores y los alumnos, y luego las *tradeaba* con otra gente. Así pasé mi fase de aprendizaje, pensando qué puedo hacer ahora que tengo las puertas abiertas al mundo. Por ejemplo, conseguí entrar en una máquina de la Universidad de Zaragoza, una LIA01 a la que llamábamos «la puta» porque entraba todo el mundo. Este detalle me hace gracia porque algunos amigos míos me contaban siempre historias de los hackers en la universidad, de ese servidor, etcétera, cuando llevaba ya tiempo bajo mi control. A través de esa salté a otras de otras universidades. Después me moví mucho por Canadá, Australia, y demás. Hackeé mi universidad, La Almunia de Doña Godina, en Zaragoza, ya lo puedo contar. Había una profesora llamada Sandra, cuya contraseña de correo era, cómo no, «sandra». Entré a través de su cuenta de correo en el servidor Linux y así ejecuté por primera vez un *exploit*, que para mí fue descubrir la magia.

—¿Y nunca sentiste la tentación de utilizar ese poder, esos conocimientos, para alguna causa hacktivista? Se supone que es durante la juventud cuando todos somos más revolucionarios…

—Solo una vez. Además, fue lo que me provocó una crisis moral importante. ¿Te acuerdas del hackeo que se hizo a una web que tenía ETA alojada en un servidor belga, llenándola de lazos azules? —Román sonrió maliciosamente mientras se señalaba el dedo con el pulgar.

—¡Hostia! ¿No me digas que fuiste tú?

Estaba sentado ante uno de los hackers responsables del ataque a la web de ETA en febrero de 1996… Solo unos días después del asesinato del profesor Francisco Tomás y Valiente, ejecutado el Día de San Valentín de ese año, Román y algunos compañeros de trabajo y de la universidad reventaron el servidor de Knooppunt y de la página Euskadi Information.[200] En la RootedCON de 2013, y durante su conferencia, había mencionado de pasada el tema, pero yo no lo sabría hasta esa noche.[201]

—Sí —me respondió Román con merecido orgullo—. Encontré la máquina donde estaba alojada la web de ETA con un montón de información, me puse a escanearla, encontré un acceso y descubrí un usuario *guest*. En aquella época todos estábamos envenenados por los anglicismos, pero yo pensé «es una máquina belga, así que estará en francés». Y así era. El usuario se llamaba Gast. Me metí y me saltó un programa de correo *pine* que permitía fácilmente la salida al sistema operativo (shell). Y ya me di cuenta de que el usuario invitado era el propietario de prácticamente todos los ficheros. Entonces era simplemente cuestión de retocar la web desde el propio sistema operativo. Yo lo dejé ahí, pero otros siguieron. Porque con el paso del tiempo reflexioné y vi que eso estaba mal. Y es ahí donde difiero de Anónymous y otros hacktivistas.

»Estoy muy concienciado políticamente y creo que debe haber un control férreo

de lo que hace el Estado, y aunque vivimos un periodo de corrupción e incompetencia evidente, y de gran desconfianza de las instituciones, eso no justifica que alguien que tiene el poder de hacerlo ataque servidores, censure páginas web o decida qué puede estar o no en internet. Porque al fin y al cabo ese es un comportamiento paramilitar. Es utilizar la ciberfuerza para imponer lo que tú crees que está bien. Y no te diferencia en nada de lo que hace cualquier tirano, cualquier represor o cualquier dictador. Hay otra forma de hacktivismo, como es dar charlas en colegios a menores y sus padres, u organizar una CON como Rooted donde toda la información es libre. Eso también es hacktivismo, y sin atacar a nadie.

Román acababa de asestarme un puñetazo directo a la conciencia. Jamás me había planteado esa reflexión sobre el hacktivismo. Y viniendo de uno de los hackers más influyente del país, que se confesaba anarquista, el impacto del argumento era todavía mayor.

—Lo que hicimos con aquellos lazos azules no se diferencia tanto. Lo hice porque podía. Esto es lo que debemos erradicar de las nuevas generaciones de hackers. No debes hacer algo solo porque puedas. Ni aunque lo maquilles como hacktivismo. Esto es algo bueno, es para mejorar el mundo… ¡Mentira! Lo haces porque puedes. Esa es la frontera que yo me puse hace mucho tiempo. No voy a alzar la mano contra nadie, solo porque pueda hacerlo. Tampoco fue una revelación espontánea, sino la conclusión a una reflexión de muchos años. Me pasé una temporada haciendo cosas grises, o manifiestamente negras, como todos. Pero al final te das cuenta de que aunque en su momento las justificases, no está bien. Es como el que le pega con una porra a una persona indefensa en la calle, solo porque puede hacerlo. Y esto es lo que tenemos que meterle en la cabeza a las generaciones futuras.

—Un gran poder —expresé, recordando la famosa frase— implica una gran responsabilidad.

—Spiderman —respondió Román, al reconocer inmediatamente la cita—. Pero ojo, también entiendo la rabia. Y viendo las cosas que pasan en el mundo, a veces me dan ganas de liarla. Porque las instituciones están fuera de control y los ciudadanos no están haciendo lo que tienen que hacer. No creo en el capitalismo ni en el comunismo. Como buen anarquista, creo en el mutualismo. Pero no puedo atacar la web de alguien, por repugnante que me parezca su contenido, por imbuido que pueda estar de la corrupción, porque detrás de esa web hay un administrador de sistemas que va a tener que dar la cara porque se ha caído. Habrá otra gente, seguramente mal pagada, que tendrá que levantarse de madrugada para restituir la página. O que los echarán a la calle. Le darás argumentos al Estado para criminalizar a los hackers… No, no. Es un error.

»Hay un ejemplo interesante que me gustaría añadir. Cuando trabajaba en EncomIX, albergábamos webs de mucha gente, entre ellas la web de Elkarri (una asociación que buscaba una salida pacífica a la situación de Euskadi) y la de Democracia Nacional. Es gracioso: todos los días recibíamos correos de gente que

nos exigía que quitáramos la web de Elkarri (insisto, pacifista) y *nunca* nos llegó uno exigiendo el cierre de la de Democracia Nacional. Eso también es censura y te da que pensar sobre el sesgo de los que la ejercen y cómo.

Cross al hígado, y *jab* cruzado a la mandíbula. De nuevo el director de la Rooted me machacaba con argumentos tan lógicos como irrefutables. Caí contra las cuerdas. Afortunadamente sonó la campana. El camarero se acercó a nuestra mesa para retirar la cena y preguntarnos si queríamos postre. Ni él ni yo estábamos para dulces. Él se pidió otro Nestea y yo café. Recuperado levemente del noqueo, proseguimos.

—Vale, nos hemos quedado con que estás en la universidad… ¿Qué pasó después?

—Hubo otro momento que fue importante para mí. Detuvieron a varios amigos míos por piratería. Eso también me hizo recapacitar. Yo nunca he hecho nada por dinero. Todo lo que he hecho fue por aprender o por divertirme. Y siempre me he mantenido al margen de la comunidad. Me relacioné mucho con Glaucoma o con Apostols —citados ambos en el *Hackstory.es* de Mercè Molist, recordé—, y a través de ellos con otra gente de fuera de España. Y estuve unos años haciendo cosas grises por ahí afuera. Pero nada por lucro. Por ejemplo, durante tres o cuatro años controlé todos los ordenadores de mi universidad. Todos. Me podía haber puesto las notas que me hubiese dado la gana, pero no lo hice. De hecho, avisé a los administradores de algunas de sus vulnerabilidades, aunque pasaron de mí. Y así hasta que me mudé a Madrid.

—¿Y te conviertes en profesional?

—Sí. Empecé en EncomIX, un proveedor de internet que había montado Ramón Martínez («Ender Wiggins»), uno de los apóstoles. Hasta que nos compró una multinacional estadounidense. Y ya en Madrid me relacioné más con la comunidad, pero siempre manteniendo la distancia. Monté mi propia empresa, con un amigo, Chase The Sun, y entre otros proyectos estuvimos trabajando en Marruecos, subcontratados por Telefónica. Estuve en Rabat, Mequinez, Marrakech y Fez revisando la seguridad de Meditelecom, la compañía de telefonía, después de que Al Qaeda les hubiese puesto varias bombas. De hecho, el 11-M a mí me pilló en Casablanca. Llamé inmediatamente a mi novia, en Madrid, pero no le había pasado nada. Sin embargo, a la mujer de mi jefe de proyecto la mataron en los trenes.

Por un segundo recordé aquella terrible mañana de 2004. La explosión que escuché desde el hotel, y el atroz atentado que condicionaría mi vida los seis años siguientes durante la investigación de *El Palestino.* Supongo que, como a muchos otros españoles, el sonido de ese número y esa letra me despierta muchos recuerdos.

—Yo viví el 11-M desde allí. Y recuerdo que las noticias que se publicaban en Marruecos o en la prensa internacional no tenían nada que ver con lo que salía en España. Allí tenían claro desde el minuto cero que había sido Al Qaeda y no ETA, como dijo el Gobierno hasta el día de las elecciones. Ahí terminé de perder la fe en los políticos y en ese modelo.

—Brindo por eso.

—De vuelta a España al cabo de unos años le pasé la empresa a mi amigo, y estuve un tiempo trabajando en PricewaterhouseCoopers, una de las consultoras más grandes y, bueno, resumiendo, terminé en 2009 en una gran empresa española. Donde soy el responsable de arquitectura de seguridad.

—Imagino que ahí tienes un buen sueldo, y ninguna necesidad de complicarte la vida, y sin embargo, ese mismo año te pones a organizar el evento de hacking más importante de Europa: la Rooted.

—Todo empezó una noche: charlando en un canal de IRC con Javier Olascoaga, nos quejábamos de que no había eventos de hacking de calidad en España. Me refiero a eventos abiertos, diferentes a los eventos privados a los que tenías que ir con invitación. O eventos «de cajita de power point», donde se repite siempre lo mismo. Que están muy bien y son muy necesarios, pero no es lo que nosotros queríamos. Así que después de mucho lloriquear lamentándonos de que no hubiese nada, decidimos montarlo nosotros. Nos juntamos con otros dos amigos, Raúl Jover y Román Medina-Heigl, y lo montamos. Después, por cuestiones que no vienen al caso, Román y yo no terminamos bien, en parte por mi culpa, y Román salió de la organización. En 2010 organizamos la primera edición, con 440 asistentes. Estaba claro que la comunidad de la seguridad necesitaba reunirse. Y desde entonces hemos ido creciendo. Hasta la última, que fueron 1.304 personas. Después organizamos RootedCON Valencia, y este año inauguramos RootedCON Hong Kong y ya estamos preparando RootedNordics.

Puedo dar fe de ello. El poder de convocatoria, la complicidad con los asistentes y el inmenso nivel de las ponencias me dejaron muy claro que se trata de una CON de referencia en habla hispana y en toda Europa.

—Pero Román… no sé cómo decirlo… En la Rooted los investigadores presentáis vulnerabilidades que obviamente pueden ser terroríficas en malas manos. Estoy pensando en la conferencia de Teso sobre la vulnerabilidad de los aviones, que me impresionó. ¿Nunca os han dado un toque?

—Hugo tuvo una reunión con varias agencias de seguridad aérea antes de exponer sus vulnerabilidades. Siempre que presentamos una vulnerabilidad, hemos pedido que antes se hable con el afectado, y casi nunca hemos tenido problemas. Pero a veces nos encontramos con algún idiota. Te voy a poner un ejemplo. Joxean Koret se pasó dos años sacando vulnerabilidades en Oracle a punta pala. Encontraba Zero Days a montones, y vino a contar algunas a RootedCON. Las vulnerabilidades estaban notificadas a Oracle, me consta, desde hacía por lo menos dos años, y no hicieron nada. Bueno, pues cuando las presentamos en la Rooted, ¿te puedes creer que me llamó un idiota de Oracle para amenazarme? Y lo mismo me pasó con alguna de las agencias de firma del DNI electrónico. Resulta que para algunos componentes te piden constantemente permiso de administrador para ejecutarse. José Antonio Guasch y Raúl Siles lo analizaron y descubrieron tropecientas vulnerabilidades. Las

comunicaron a los proveedores y ni puto caso. Así que las publicamos.

—Pero eso nos deja totalmente desvalidos a los usuarios. Es decir, si no corrigen los fallos, significa que estamos moviéndonos con un DNI inseguro…

—Claro. Por eso lo hacemos. Nosotros revisamos sus productos y si detectamos un fallo, se lo decimos para que lo corrijan. Pero ¿qué hacen ellos? Criminalizar al investigador por publicar la vulnerabilidad. Y por supuesto, pasar de arreglarla, porque eso les cuesta dinero y esfuerzo. Y te puedo decir que fuerzas de seguridad, como la Guardia Civil, se toman muy en serio el asunto, porque en ocasiones ellos han mediado para que una empresa reaccione cuando le comunicamos una vulnerabilidad, en lugar de acusarnos a los investigadores.

En los Estados Unidos la mayoría de las empresas importantes premian a los hackers que informan de vulnerabilidades, porque eso les ayuda a fortalecer sus sistemas. Sin embargo, en España eso no ocurre.

—Pues no lo entiendo, Román. Yo suponía que las empresas serían las primeras interesadas en esa información, porque les ayudaría a mejorar sus productos. De hecho, creo que algunas premian a los hackers que descubren vulnerabilidades.

—Sí, el Bug Bounty. Hay empresas que premian a quien les informa sobre vulnerabilidades, ¿cuántas crees que son? ¿Ocho, diez? Facebook, Microsoft, Google… pero hay muchas más empresas que pasan totalmente. Y tienen dinero para hacerlo. Si dedicasen solo un 1% de su presupuesto a esto, reducirían muchísimo los riesgos de los usuarios. Sin embargo, es mucho más sencillo bombardear con que el investigador es un irresponsable que pone en riesgo a sus clientes… por una vulnerabilidad que han metido ellos y que no quieren reparar. Genial.

En 2014, por ejemplo, Facebook aumentó el presupuesto oficial del programa Facebook Bug Bounty, iniciado en 2011, que premia el descubrimiento de vulnerabilidades en su sistema. El investigador brasileño Reginaldo Silva se hizo con 33.500 dólares tras descubrir un error a través del cual los atacantes podían acceder a los archivos XML en los servidores de Facebook.[202]

—Parece difícil ganarse la vida como hacker descubriendo vulnerabilidades.

—No es difícil. Requiere esfuerzo y dedicación. Sacar vulnerabilidades no es algo que consigas en tres minutos. En ocasiones son ocho meses de trabajo. Pero hay gente que se dedica profesionalmente a ello y le va bien. Un hacker no es solo un técnico. Que no te engañen. Existe el tópico de que uno no se puede llamar a sí mismo hacker, pero es una chorrada. Yo soy hacker. Y tú también. No se trata solo de software y hardware. Se trata de afrontar los problemas desde otra óptica. De encontrar una idea original. De forzar una cerradura, ya sea lógica, física o legal. De usar el pensamiento lateral. Hay médicos, abogados, periodistas, que para mí son hackers. ¿Conoces a Jorge Bermúdez?

—Sí, claro. El fiscal.

—Pues Jorge es un hacker de la ley. Tú mismo eres un hacker. Tú tienes que buscar la vulnerabilidad del sistema donde te quieres infiltrar, y entras. Luego tienes

que pasar desapercibido. Hacer la continuación de tu ataque, la metástasis de tu ataque y salir sin dejar huella. Son exactamente las mismas fases de un ataque a un sistema informático, pero tú lo haces en el mundo real. Luego tú también eres un hacker. Es cierto que existen unas habilidades técnicas que te ayudan a la hora de afrontar un ataque lógico. Pero para mí tiene más que ver con una forma de pensar, que con los conocimientos informáticos.

No podía verme la cara, pero creo que me ruboricé. Después de estos años explorando el mundo de la seguridad informática he aprendido a respetar y admirar tanto el cerebro privilegiado de los hackers, que me pareció un cumplido desproporcionado. Aunque entendí lo que Román quería expresar. El hacking va mucho más allá del teclado de un ordenador. Se expresa en diferentes ámbitos de nuestra vida. Es una actitud, una forma de enfrentarse a los problemas. Es la ingeniería social y el pensamiento lateral aplicado a cualquier situación a la que nos enfrentemos.

—Lo cierto es que muchos de tus compañeros en el mundo de la seguridad informática se están marchando de España —cambié de tema—. Y esa fuga de cerebros intuyo que es terrible para el país.

—Pero es lógico. Nuestros hackers son de los mejores del mundo. Se nos llena la boca con la importancia de la ciberguerra y después les quieren pagar 24.000, 35.000 euros al año, cuando deberían estar cobrando 400.000. Y claro, luego viene una empresa estadounidense, les paga 75.000 y se acabó. Pierdes el talento y la genialidad se la lleva una empresa extranjera. Para lo que saben hoy, y para todo lo que van a descubrir mañana. Mi generación ya está perdida. Nosotros estamos trabajando para las generaciones venideras. Para que en el futuro tengan las condiciones adecuadas para que no necesiten irse de España.

—¿Y cómo imaginas tú ese futuro? Me refiero a la implantación de la tecnología en nuestras vidas.

—Mal. Muy oscuro. Me temo que nos vamos a enfrentar a unos veinte años de tinieblas. Mientras los ciudadanos no tengan claro cuáles son sus derechos en internet. Y si no los tienen claros en el mundo físico, imagínate en el virtual. Me temo que va a haber muchos abusos. Ya los hay ahora, pero habrá más. Las *cookies* por ejemplo, que ya están en todas las web, vulneran tu intimidad. Si tú entras en un periódico para leer las noticias, inmediatamente se te abrirá una pantalla de publicidad ofreciéndote productos que te puedan interesar en base a tus lecturas, porque lógicamente quien abre según qué diario tiene cierta orientación ideológica… Son las *tracking cookies* que te hacen el seguimiento mientras navegas por internet. Hay un artículo del *Wall Street Journal* muy bueno que te recomiendo que te leas, contando, por ejemplo, cómo cuando utilizas un navegador de Apple te salen los productos más caros en la publicidad…

Tomé nota, y lo leí más tarde. Está disponible en su web.[203]

—Imagina, por ejemplo, que soy el dueño de Chueca.com, una web orientada a

homosexuales que estaba en Ya.com. Supón que decido meter en mi web una *supercookie* de una empresa de *tracking*. Y esa empresa después vende sus servicios a otra empresa, por ejemplo con sede en Burkina Faso. Y cuando entras en Amazon, te empieza a salir publicidad de hoteles para gays. Eso está pasando ya. ¿Y por qué tiene que saber nadie mis tendencias sexuales? Y ahora piensa: «Yo me llamo Muhammad, tengo mi servidor en árabe y ya estoy rastreado en veinte mil sitios. Y ahora en base al Acta Patriota de Estados Unidos, ya pueden utilizar la puerta de atrás de mi proveedor y me entran cuando quieren». Pero eso no es lo peor. Ahora por ejemplo se están cotizando mucho los informes médicos en el mercado negro. Las aseguradoras pagan por saber no ya qué enfermedades tienes ahora, sino cuáles puedes tener en el futuro. Y como pueden inventarse cualquier cláusula legal para no asegurarte, les interesa saber si tienes algún riesgo de tener una enfermedad que les salga cara. Son muchas cosas. Por eso creo que tenemos unos veinte años muy duros por delante. Vamos a vivir una verdadera guerra del control de la información y no precisamente para beneficio de los ciudadanos.

—Ahora que mencionas las puertas traseras… Creo que conociste a Julian Assange en 1995, mucho antes de Wikileaks.

—Coincidimos en Hamburgo, en un Chaos Communication Congress. Pero nada, intercambiamos dos palabras en un pasillo al cruzarnos, porque yo utilizaba una de sus herramientas. La primera herramienta de análisis de puertos que usé en mi vida era el Strobe, una aplicación que escribió él. Después, cuando ya había fundado Wikileaks, intercambiamos unos mensajes, porque yo quería invitarlo a España a la RootedCON, pero entró en la embajada de Ecuador y hasta hoy…

—¿Y Snowden?

—Lo que dijo Snowden ya lo sabía todo el mundo, y casos como el de «Boeing vs. Airbus» deberíamos recordarlos todos. Hacía mucho tiempo que la NSA intentaba controlar las comunicaciones. Existen casos flagrantes, como la infiltración en OpenBSD para debilitar el sistema de cifrado, que era el sistema operativo que utilizábamos porque era superseguro. Debilitaron las VPN y distintas herramientas para que fuese más fácil romper la seguridad de todo lo que hicieses con OpenBSD. Y como esa hay muchas. Lo único que consiguió Snowden es que ahora todos estemos más paranoicos. Antes solo lo estábamos unos pocos, y nos llamaban locos. Nos decían: «¿En serio crees que la NSA puede controlar todas las comunicaciones?». Yo sí lo creía. Y por eso la gente nos miraba como si fuéramos los chalados con papel de plata en la cabeza… Ahora todo el mundo lo cree.

La historia realmente parece el argumento de una película de espías, o el delirio de un tipo con la cabeza envuelta en papel de plata, pero lo cierto es que muchas historias del mundo del hacking lo parecen. OpenBSD es un sistema operativo libre tipo Unix multiplataforma, basado en 4.4BSD. Es un descendiente de NetBSD, con un foco especial en la seguridad y la criptografía muy popular entre los hackers. Hasta que en 2010 el excontratista del Gobierno estadounidense Gregory Perry

confesó públicamente que había colaborado con el FBI en la creación de «puertas traseras» en el OpenBSD.[204]

—Supongo que siempre nos quedará TOR para protegernos —dije haciendo gala de mi profunda ignorancia.

—Yo no me fiaría. El caso de Hache es un ejemplo perfecto de que ni siquiera la red TOR es segura. De hecho, Hache es la razón por la que estoy tan enfadado con la Policía Nacional y no están invitados oficialmente a la Rooted mientras no pidan perdón públicamente.

Una vez más, el nombre de Hache surgía en otra de mis conversaciones con los hackers. Pero esta vez iba a conocer más profundamente la historia del hacker español, detenido por orden del FBI por luchar contra la pedofilia en la Deep Web. Por fin.

—Hache y otros compañeros suyos habían diseñado una herramienta que rastreaba la red TOR para localizar servidores con pornografía infantil —prosiguió Román—. Pero el FBI había colocado servidores trampa con material para atraer a los pedófilos, y la herramienta de Hache entró en uno de ellos. En teoría, Hache y sus compañeros estaban colaborando con algún servicio policial, pero no estaban identificados como colaboradores ni tenían ningún tipo de certificado oficial. No eran confidentes.

«Ni siquiera les importó que lo que pasara por allí fuese una araña, un programa robot que recogía información, y no un usuario pedófilo. Lo trincaron igual», me dijo Lord Epsylon cuando hablamos de este tema.

—El hecho es que en España no está permitido que la Policía cree servidores trampa, cebos que puedan instigar a la comisión de un delito, así que quien estaba cometiendo un delito realmente era el FBI —continuó Román—. Además, en aquella época ellos habían descubierto un Data Center británico que tenía muchos sitios de TOR y mucho porno infantil, y yo creo que el FBI se asustó. Pensaron que iban a reventarles la operación y a hacer mucho ruido y mandaron un requerimiento a España para que se les detuviera. Así que aquí llega una petición del FBI pidiendo que se detenga a un tío y dando la dirección IP de su casa. Como lo oyes, de su casa. Y aquí a la Policía Nacional le da igual los derechos constitucionales de este hombre, van, lo detienen y se pasa dos noches en el calabozo. Cuando el pobre estaba colaborando con otro servicio, para hacer algo positivo, como identificar sitios de pedofilia en TOR. Así que ahora te pregunto yo a ti, ¿cómo pueden averiguar la IP de su casa si Hache entraba por TOR?

—¿Quieres decir que entonces lo de que TOR es seguro, es otro mito?[205]

—Yo lo dejo ahí. Medítalo. Hache no es el tipo de personas que comete errores. Yo lo conozco y es un tío inteligente y muy meticuloso, y además, no trabajaba solo. ¿Sabes cómo me enteré yo? Alguien subió la noticia de que se había detenido a un pedófilo en TOR a la lista de Rooted. Cuando la vi, mi primer comentario fue: «Otro hijo de puta más al que le deberían caer diez años»… E inmediatamente empecé a

recibir wasaps y telegrams diciéndome que estaba cometiendo un error. Cuando averigüé lo que pasó, lo dije públicamente: «Policía Nacional, en Rooted estáis vetados. Y hasta donde llegue mi capacidad no vais a volver a un evento que yo organice, hasta que le pidáis perdón a este tío». Para mí lo de Hache supuso un punto de inflexión. Porque alguien, por apuntarse un tanto y salir en los periódicos diciendo que habían detenido a un peligroso pedófilo junto con el FBI, decide meter dos noches en el calabozo a un hacker que solo estaba haciendo algo positivo por la comunidad.

—Sin embargo, la Guardia Civil sí está presente en la Rooted.

—Es que es distinto. La estrategia de la Guardia Civil ha sido estar cerca de los hackers. Y toda la iniciativa ha salido de César Lorenzana y su equipo, por lo que yo le estoy muy agradecido. Han demostrado que la comunidad puede confiar en ellos y gracias a esa confianza podemos colaborar para luchar contra los que de verdad son criminales.

El gueto hacker de Varsovia

—¿Qué significa el 1 de julio para vosotros, los hackers, con la entrada en vigor de la reforma del Código Penal?

—El problema es que el legislador ha legislado de acuerdo a una situación que cree crítica: la existencia de las ciberarmas. La ley depende de la interpretación de un juez. Y si yo acabo ante un juez y considera que estoy en posesión de ciberarmas que pueden utilizarse para la comisión de un delito terrorista, ay de mí. Y cualquier herramienta de seguridad puede ser utilizada como arma. Las herramientas que yo utilizo todos los días en mi trabajo para escanear máquinas o examinar redes pueden tener un uso ofensivo, es verdad. El problema es equiparar las herramientas de hacking que yo utilizo para auditar, con armas de ciberterrorismo. La diferencia entre un auditor de seguridad y un terrorista la tengo clarísima, pero no sé si los jueces también. Y el problema es que cuando descubrimos vulnerabilidades en infraestructuras críticas, esa investigación se puede interpretar como un acto terrorista…

—¿Puedes ponerme un ejemplo?

—Claro. Imagina que en la próxima Rooted se va a presentar una conferencia sobre las vulnerabilidades que tiene la central de Garoña, que está expuesta a un ataque desde internet. Imagínate, es un supuesto, que hemos descubierto vulnerabilidades tan graves como para hacer explotar la central. Imagina ahora que yo, cuando mando la nota de prensa anunciando los contenidos de la Rooted, incluyo que vamos a demostrar que hay vulnerabilidades reales en infraestructuras críticas como una central nuclear. Imagina que al Consejo de Seguridad Nuclear, o al político de turno que lleve la cartera de Industria, Fomento o Defensa, se le cruza el cable y dice «¿Qué hacen estos gilipollas de hackers hablando de la central nuclear en prensa?».

»Yo en mi ordenador tengo herramientas de hacking, y estoy hablando de cómo se puede hacer explotar una central nuclear que es Garoña. Así que interpreto esta ley como una herramienta contra la libertad de expresión, un mecanismo para censurarnos y que no podamos denunciar situaciones graves, y una forma de poder llevarse por delante a quien les dé la gana. Y como el precedente de Hache no nos ha enseñado nada…

Recordé mi reunión con Juan José Zurdo y me pregunté cómo reaccionaría el CNPIC ante una conferencia que presentase vulnerabilidades de una central nuclear como Garoña…

Con Román, además, discutí los nuevos retos legales y tecnológicos que nos impone el desarrollo de la nueva informática, obligándonos a reescribir nuestra percepción del Derecho y la investigación policial, entre otras cuestiones.

—De todas formas, es normal que se busque mejorar las leyes, y te hago esta reflexión. No puedes darle un 600 a la Policía y pretender que cace criminales que

van en Lamborghini. Las Fuerzas del Estado deben tener herramientas para luchar contra los cibercriminales en igualdad de condiciones. Si los criminales utilizan cifrado, redes de anonimato, VPN, esteganografía…, la Policía tiene que poder luchar contra eso, pero sin menoscabar los derechos de los ciudadanos. El problema del registro remoto es que tiene que estar tutelado democráticamente. ¿Hay un armario de armas? Eso tiene que estar controlado por un juez, tiene que haber un lugar físico para hacerlo, tienes que poner a disposición del defensor la herramienta que se ha utilizado para el registro. Porque ¿cómo sabes que la herramienta no ha colocado evidencias? Y si pones la herramienta a disposición del defensor, ya la estás poniendo a disposición de todo el mundo, así que esa herramienta ya no puede volver a usarse. Es muy complicado. Hay que certificar el proceso, no la herramienta…

Román había repetido el mismo argumento que me había expuesto Lucas, el genio captado por el gigante estadounidense de internet meses antes, o la inspectora Silvia Barrera, subrayando los problemas técnicos y legales para gestionar un arma tan poderosa como el registro en remoto. En definitiva, una forma de hackeo legal.

—Yo soy favorable al registro en remoto mientras haya un estricto control judicial —seguía Román—. Tutela democrática. Pero ¿cómo lo haces? ¿Sientas a un juez que no sabe nada de hacking y le vas explicando lo que haces? Tiene que haber un mecanismo de armario de armas en el que haya una serie de llaves físicas y digitales, donde se custodien esas herramientas hasta que haya allí un juez, un representante de las Fuerzas del Estado, un representante de los derechos civiles, tipo el defensor del pueblo, o sea, una serie de personas que garanticen que la herramienta se está usando legalmente. Y desde un punto de vista logístico es muy difícil, así que te tienes que fiar de que la Policía lo va a hacer bien, y eso no puede ser. Tengo muy buenos amigos en la Guardia Civil y en la Policía, pero nadie es infalible, y a cualquiera puede metérsele en la cabeza la obsesión de que eres culpable y hay que demostrarlo a cualquier precio… A eso súmale el escándalo del Hacking Team, que pillaron las herramientas que utilizaban, y que en el código fuente se descubrieron funciones del tipo «colocar evidencia de terrorismo islámico»…

—¿Cómo has dicho?—Lo había escuchado perfectamente, pero me parecía increíble lo que había oído.

—Sí, sí, una función que se llamaba «poner imágenes islámicas», y otra «poner imágenes pedofilia». ¿No lo has visto? Espera que te busco el código. —Román se lanzó a buscar algo en su teléfono móvil—. Nadie tiene muy claro que esto sea una funcionabilidad real, porque es increíble, pero ya no me asombra nada. Además, Hacking Team no son los primeros, HBGary, Gamma Group… ya hubo otros antes. Grupos de espionaje que trabajan para gobiernos, policías y servicios secretos. Y que también fueron hackeados, como Hacking Team.

La acusación es muy grave, pero Román no exageraba. El análisis de código de algunas de las herramientas del Hacking Team parecía indicar la existencia de herramientas que permitían introducir pruebas falsas en los ordenadores hackeados. Y

esa posibilidad generó un acalorado debate en la comunidad. Ernesto Corral, una de las firmas más respetadas del hacking español, dedicó una entrada de su blog a la polémica.[206]

—Pero no lo entiendo… ¿Me estás diciendo que nuestros servicios de Información externalizan, subcontratan el espionaje electrónico?

—No, te digo lo que te decía antes. Te enfrentas a un crimen organizado que tiene cifrado en todos sus equipos, botones del pánico para borrar los datos con *kill* switch y cosas así. Esto existe. ¿Cómo peleas contra eso? Tienes que ir armando a tus profesionales con las capacidades necesarias para enfrentarte a gente muy especializada, muy organizada y muy efectiva en sus delitos. Pero no a costa de que los ciudadanos se vean expuestos a excesos del poder.

Román Ramírez lo tiene muy claro. Y sus ideas, que muchos calificarían de utópicas, no se limitan a una proyección de deseos, sino que están argumentadas por una extensa formación cultural, teórica y política.

—Soy anarquista, pero en la escuela de Godwin y Proudhon, no soy bakuniano, no quiero destruir el Estado y vivir en el caos. Yo creo que debe existir un Estado mínimo, con unos ciudadanos responsables de sus actos, como dice Godwin, y entre las funciones del Estado está la protección de los ciudadanos. Esa función solo la pueden hacer la Fuerzas y Cuerpos de Seguridad. Si todo el mundo tiene armas o ciberarmas, tenemos un problema. Por ejemplo, Academi, la empresa de Blackwater, [207] si Blackwater ha cometido atrocidades en Irak, ¿qué puede hacer una empresa repleta de ciberarmas? Y esas armas las ponen al servicio del Estado. De acuerdo en que las Fuerzas del Estado tienen un control legal, pero oye, un tío que tiene sede en Burkina Faso, cuya figura fiscal legal se diluye en veinticinco sociedades… Igual que los servicios secretos reclutan especialistas para misiones concretas, eso pasa con los hackers. Mercenarios hay en todos lados. Las operaciones negras se llaman negras por algo…

—A ver si lo entiendo —recapitulé—. Lo que la nueva ley quiere hacer con vosotros es parecido a lo que ocurrió con los porteros de discoteca. Antes, se podía contratar a cualquiera como vigilante para la puerta de un local, pero ahora tienen que hacer un curso, sacarse una certificación y pasar un examen. ¿Es eso?

—Correcto. Eso es lo que pretenden, pero yo lo veo como el gueto de Varsovia. Quieren ponernos una estrella de David amarilla… Te lo explico: en el nuevo Código Penal se tipifica como delito dibujar o pintar escenas de menores teniendo sexo, pero no he oído que los dibujantes tengan que registrar sus pinceles, como armas con las que se puede cometer un delito. Sin embargo, pretenden que los hackers vayamos a un registro para «ficharnos» como expertos en seguridad. Eso es el gueto de Varsovia. Hay que tener mucho cuidado con eso. Yo tengo mis ideas políticas muy claras. Creo que tiene que haber tutela democrática para todo. Y esto lo que hará es dejarnos en una situación de inseguridad. Van a menoscabar nuestros derechos obligándonos a meternos en un registro que no solamente será un listado de sospechosos habituales,

es que seguramente costará dinero. ¿Qué va a pasar con unos estudiantes que estén diseñando una nueva herramienta?, ¿tendrán que pagar por ella? Vas a cargarte la innovación, la investigación. Yo ya se lo he advertido. Como esto prospere, voy a llamar a las armas a toda la comunidad hacker española, y voy a proponer cosas, inofensivas pero contundentes, para darles una lección. Por ejemplo, que toda herramienta que se cree en España lleve una licencia específica que prohíba su uso a la Administración pública, incluyendo Fuerzas del Estado. Una cláusula de protesta contra esa ley específica.

Román no bromeaba. El brillo de la indignación que asomaba a sus ojos verdes mientras remarcaba las palabras dejaba claro que no iba de farol. Además, yo fui testigo. Meses atrás, en la RootedCON 2015, había hecho pública esa advertencia durante la magnífica mesa redonda «¿Tiene que dar alguien el carnet de hacker?». Yo estaba allí.

—Coño, es que es la única manera que tenemos de protestar. Quieren criminalizarnos.

—¿Y cómo pretenden hacerlo?

—Todavía no lo tienen claro. He leído varios de los proyectos de ley y en unos hablan de «debidamente autorizado» y en otros de «debidamente acreditado», pero no acaban de precisar quién nos va a acreditar. Tú, si quieres ser camarero, te sacas el carnet de manipulador de alimentos, pagas 8 o 10 euros y respondes a veinte preguntas. Eso lo puedo entender. No me gusta, porque al final tu nombre está en un fichero, pero lo puedo aceptar. Pero si tienes que ir a una agencia gubernamental, pagar 90 o 100 euros, que además tienes que renovar, hacer un examen… Como vayan por ese camino, me levanto en armas para sabotear eso.

»Y está muy relacionado con la Ley de la Seguridad Privada, donde hay muchos intereses económicos metidos. Algunas empresas, y algún que otro comisario, pretenden que los expertos en seguridad informática estemos supeditados a las empresas de seguridad privada, y la reforma que pretendían era kafkiana, porque tiene muchas zonas oscuras. Y ahí es donde crecen los tiburones… Te voy a decir otra cosa, como vayan por ahí, RootedCON se convertirá en agente certificador, y voy a certificar a todo el mundo. Y anónimamente. Impidiendo el acceso a los datos de la gente registrada salvo con orden judicial. Lo tengo todo pensado…

Mayo de 2015
La vulnerabilidad del Firewall de MarkoSS88

«Lo único que queda tras la vida de un hombre son sus sombras y el recuerdo que deja.»

Adolf Hitler, citado por su secretaria Christa Schroeder en sus memorias

La siguiente pista en la búsqueda de Markos llegó de la mano de una de las CON más influyentes de la comunidad hacker. La No cON Name (NcN).

A pesar de que nació en Mallorca, allá por 1999, el primer congreso público de hacker que se celebró en España pronto se desplazó a Barcelona, y desde entonces, una vez al año, convierte la Ciudad Condal en la capital del hacking español.[208] Al frente de la NcN, entre otros, algunos de los cerebros mejor amueblados del hacking nacional, como Pedro Sitaras, Alejandro José Clarés, los «Jordis» (Serra y Vázquez) o Nico Castellano, a quien sin embargo conocí en X1Red+Segura. Y entre los colaboradores más directos, Deborah Sánchez, Óscar Queraltó, Sergi Martínez o mi colega Mercè Molist.

NcN, constituida como asociación ya en 1999, no solo organiza, sino que además colabora de forma activa con las Fuerzas y Cuerpos de Seguridad del Estado, imparte docencia, y está presente en otras CON nacionales. Y algunas de las vulnerabilidades más escandalosas, y de las herramientas más útiles se presentaron en este foro. En la edición de 2014 y ante cuatrocientos asistentes, por ejemplo, Daniel Fernández Bleda presentó Tinfoleak, un programa creado por su socio Vicente Aguilera, que geolocaliza a las personas a partir de su actividad en Twitter —algo parecido al Creppy que ya habíamos utilizado con MarkoSS88—.[209] Para que no quedasen dudas, Fernández Bleda hizo una demo demostrando dónde estaban físicamente la cantante Soraya, Javier Solana, Pepe Navarro, Xavier Trías o el aún ministro José Ignacio Wert, solo con los metadatos incluidos en sus tuits. Un ejemplo más de que hay que ser muy prudente a la hora de pulsar el enter del teclado…

En la NcN concluye lo más granado de la comunidad hacker barcelonesa. Entre ellos Ronin, a quien he conocido este año, pero con quien me une ya una gran amistad. Ronin también lidera una empresa de seguridad informática, pero como todo buen hacker se pirra por las causas perdidas, y amablemente se ofreció a colaborar de forma desinteresada en la

investigación de MarkoSS88.

A estas alturas yo empezaba a dudar. Parecía imposible conseguir su verdadera identidad. Y el hecho de que durante más de un año una decena de policías veteranos y un periodista de investigación no hubiesen conseguido averiguarla significaba que nos enfrentábamos a un adversario sorprendente. Fuese quien fuese, Markos no era un skinhead neonazi de diecinueve años.

Cuando una investigación se prolonga tanto en el tiempo, a veces es necesario buscar otros puntos de vista. Pregunté a todos mis contactos en Barcelona si alguien conocía a alguien que pudiese conocer a alguien con acceso a los clientes de Parlem. Y durante uno de nuestros encuentros le comenté a Ronin las novedades del caso. Las pistas falsas que habíamos seguido, la geolocalización en Madrid del sujeto, la pista de los teléfonos… Ronin, a quien los retos le tientan más que la bebida isotónica, no se resistió a aportar su granito de arena.

Para empezar, redactó un voluminoso dossier, sintetizando las informaciones contrastadas que teníamos, y eliminando todo el ruido de las pistas falsas que nos habían hecho perder tanto tiempo y energía. Casi cincuenta páginas de informe.

Hackear las cuentas de correo de MarkoSS88 habría sido relativamente sencillo, pero no habría sido legal. Y a pesar de que una y otra y otra vez muchos de los hackers que he conocido durante estos años se ofrecieron a hacerlo, siempre insistí en que si hacemos las mismas cosas que las personas cuya conducta reprobamos, nos estamos convirtiendo en ellos. Y puedo dar mi palabra de que todas las técnicas que se utilizaron en esta investigación eran legales. Un buen ejemplo es el meticuloso informe de Ronin.

Simplemente aplicando la estadística y el sentido común a los análisis comparativos de las cuentas en Twitter, Facebook o los posts de un blog en internet, es posible sacar conclusiones y pistas.

Por ejemplo. Tras analizar las 285 entradas incluidas en el blog de Markos, entre el 29 de enero de 2013 (primera entrada en el blog) y el 25 de mayo de 2015 (última), nos percatamos de muchas cosas. Como que durante los primeros meses, nadie interactuaba. Era como si Markos acabase de aparecer en el mundo neonazi y nadie lo conociese. En los primeros 70 posts subidos al blog solo encontramos cinco comentarios. A pesar de que Markos emplea la segunda persona del plural en su redacción, como si se dirigiese a unos lectores determinados, estos no dan señales de vida. Recordé la expresión de Rafa tras analizar su cuenta de Twitter: «Es como si hablase solo».

La primera vez que se detecta actividad en los comentarios de su blog es

en marzo de 2013, cuando Markos se entrevista a sí mismo, así que contemplamos la posibilidad de que los comentarios que aparecen en ese post también los hubiese generado él.

Haciendo un rastreo más profundo, utilizando las herramientas del hacking web, descubrimos comentarios, tuits y referencias antiguas, en las que varios miembros de la comunidad neonazi y antifascista habían manifestado su desconfianza a que Markos fuese un personaje real. Nadie había conseguido descubrir su secreto, pese a que los antifas lo intentaron enérgicamente. Llegaron a subirse a la red posts que bromeaban con la idea de que MarkoSS88 no existía. No imaginaron hasta qué punto estaban en lo cierto…

Sin embargo, el blog gozaba de buena salud. Para el 6 de febrero de 2013, se supone que llevaba 1.000 visitas. Un mes después eran 4.700; 14.000 para el 18 de abril y 35.000 a 3 de octubre de ese mismo año. Puede que un altísimo porcentaje fueran visitas de los antifas a los que Markos provocaba en las redes sociales, o de investigadores como David Docal o Esteban Ibarra, controlando la nueva web de ciberodio recién aparecida en la red de la nada. Según Ronin, alcanzó las 93.000 visitas.

Curiosamente los mayores repuntes de visitas y comentarios los tuvieron las entradas en las que anunciaba que iba a dar la dirección de Alfon y mi identidad. Ambas son falsas y Markos lo sabía, pero aquella jugada propagandística le sirvió para que se hablase de su blog en las redes y para ganar publicidad.

No obstante, la mayoría de las entradas eran insípidas. Incluyendo la supuesta «exclusiva» sobre la identidad de Antonio Salas. Copia y pega de otras páginas, artículos históricos, incluso el *Mein Kampf* de Hitler publicado por entregas. Como si Markos necesitase mantener el blog activo, pero no dispusiese de mucho tiempo para generar contenidos originales…

Y lo mismo podía decirse de su libro *¿Qué es Nacional Socialismo? Un trabajo de dedicación y entrega.* Que ni se titula así, ni es suyo.

Ante esta nueva dimensión del caso, se me ocurrió googlear algunos párrafos al azar tomados del libro que Markos afirmaba haber escrito con sus camaradas… Nueva sorpresa. Markos había plagiado el libro *Nacionalsocialismo: Historia y Mitos,* de un tal Ignacio Ondargáin, autor de otras obras sobre el hitlerismo esotérico. Le había robado el texto de su web, [210] le había cambiado la portada y el título, y había puesto su nombre como autor.

Markos había intentado cimentar la credibilidad de su personaje ante la comunidad neonazi haciendo lo mismo que yo ante los yihadistas: presentándose como un ideólogo que escribía libros. La diferencia es que yo sí escribí los que utilicé como tapadera de Muhammad Abdallah[211] en *El*

Palestino. Él, que debía de tener prisa en infiltrarse en la comunidad NS, directamente lo robó a su autor.

Ronin, además, aceptó implicarse también en la investigación del caso Roi. En cuanto escuchó el desgarrador relato de Gloria se le abrieron las carnes, y claudicó en derivar parte de los recursos de su empresa al caso. Y ya puestos, implicó a algunos de los mejores especialistas de su equipo de colaboradores, como Jorge Jiménez, una autoridad en autopsias digitales. Gloria había conseguido hacerse con un disco duro externo de Roi en casa de una de sus víctimas. Y aquello era una mina inagotable de información. Yo tuve la oportunidad de asomarme a ese disco duro y revisar algunos de los cientos de fotos y vídeos de Roi, con sus distintas personalidades, y estoy seguro de que un experto como Jorge Jiménez podrá sacar partido de aquellos archivos. Cosas que solo los ojos de un psicólogo forense pueden ver entre las líneas de código. La patología psiquiátrica de Roi, que aún no lo sabe, pero volverá a sentarse en un banquillo muy pronto… como MarkoSS88.

Pero la Providencia no solo echó mano de los hackers para facilitarme esta investigación. La identidad del teléfono de Parlem que utilizaba MarkoSS88 la consiguió alguien alejado de los códigos binarios.

—Toni, lo tengo —me dijo Manu—. Un amigo ha encontrado un acceso. Te mando los datos a tu mail.

Me metí en el primer cibercafé que encontré en Barra de Ferro, pero tenía cámaras de videovigilancia orientadas a los locutorios. No me gustó. Busqué el siguiente… Durante los años en que gestioné la página web de Carlos el Chacal aprendí lo importante que es la disciplina a la hora de salvaguardar la seguridad. En esa época todavía no sabía nada sobre el hacking, pero nunca, ni una sola vez, jamás, abrí los correos o la web desde mi ordenador. No importaba que lloviese, hiciese frío o ya estuviese en la cama. Si necesitaba salir a la red, me vestía, cogía el coche (aún no sabía lo que era una moto) y me desplazaba el mayor número de kilómetros posible para buscar un cibercafé seguro. Siempre lo hice así. Sin excepciones. Sabía que muchos servicios de Inteligencia estaban interesados en descubrir quién controlaba la web del Chacal, actualizada un día desde Caracas, otro desde El Cairo, Barcelona, Lisboa, Beirut, Madrid, Damasco o Amán, así que me convertí en un internauta muy disciplinado, y no iba a romper ahora esa disciplina.

Encontré otro locutorio árabe, con algunos ordenadores y sin cámaras de videovigilancia. Busqué el más retirado, giré la webcam y abrí mi correo.

Mi amigo tenía razón. Habíamos averiguado quién era el titular de la línea de Markos en Parlem… pero había resultado aún más astuto de lo que pensábamos…

El teléfono 668… de Parlem estaba registrado a nombre de FonYou. Un cortafuegos perfecto para borrar tu identidad.

—¡Joder! —exclamé mientras descargaba un puñetazo en la mesa del locutorio. Todos los demás usuarios apartaron la vista de sus ordenadores para mirarme—. Qué bueno eres, cabrón…

FonYou es una empresa que permitía duplicar la tarjeta SIM ofreciendo un número telefónico extra. Algo muy útil si no queremos dar a terceras personas nuestro teléfono real, disponiendo así de otro número redireccionado hacia nuestro terminal o, como en el caso de MarkoSS88, utilizado para gestionar una cuenta en Telegram y Line.

En su página web, FonYou «obliga» a los usuarios a rellenar un simple formulario con datos «veraces». De lo contrario, amenaza, y de acuerdo con la ley, se reserva el derecho a no tramitar la concesión de un nuevo número de teléfono… Pero lo cachondo del tema es que no verifica los datos. Puedes llenar las casillas de su ficha con el número de DNI, nombre y dirección que primero te venga a la mente.

Eso fue lo que hizo Markos cuando contrató el servicio para el número. Llenar el formulario con lo primero que se le ocurrió. Es decir, con el mismo nombre y número de DNI que había utilizado para registrarse en las conferencias de la Universidad Rey Juan Carlos, donde todo esto comenzó, añadiendo una dirección que a mí me costó identificar, pero a Manu, el autor del descubrimiento, y un poco mayor que yo, no.

—*Rúe del Percebe* fueun tebeo de Ibáñez, el autor de *Mortadelo y Filemón,* muy popular en mi generación. Pocos chavales de diecinueve años habrán oído hablar de ese tebeo —concluyó—. Este tío tiene que estar entre los cuarenta y los cincuenta años.

Markos nos había ganado por la mano. Se adelantaba a nuestros movimientos. Había pensado cómo podían llegar a él y se había anticipado cerrándonos el camino. Sabía que era prácticamente imposible que nadie accediese a los registros de Parlem, una compañía nueva, asentada en Catalunya. Ni siquiera la Policía tenía todavía contactos dentro, como para que le facilitasen la identidad de un usuario sin una orden judicial. Pero en el improbable caso de que alguien pudiese vulnerar esa barrera, había colocado un cortafuegos muy eficiente: FonYou.

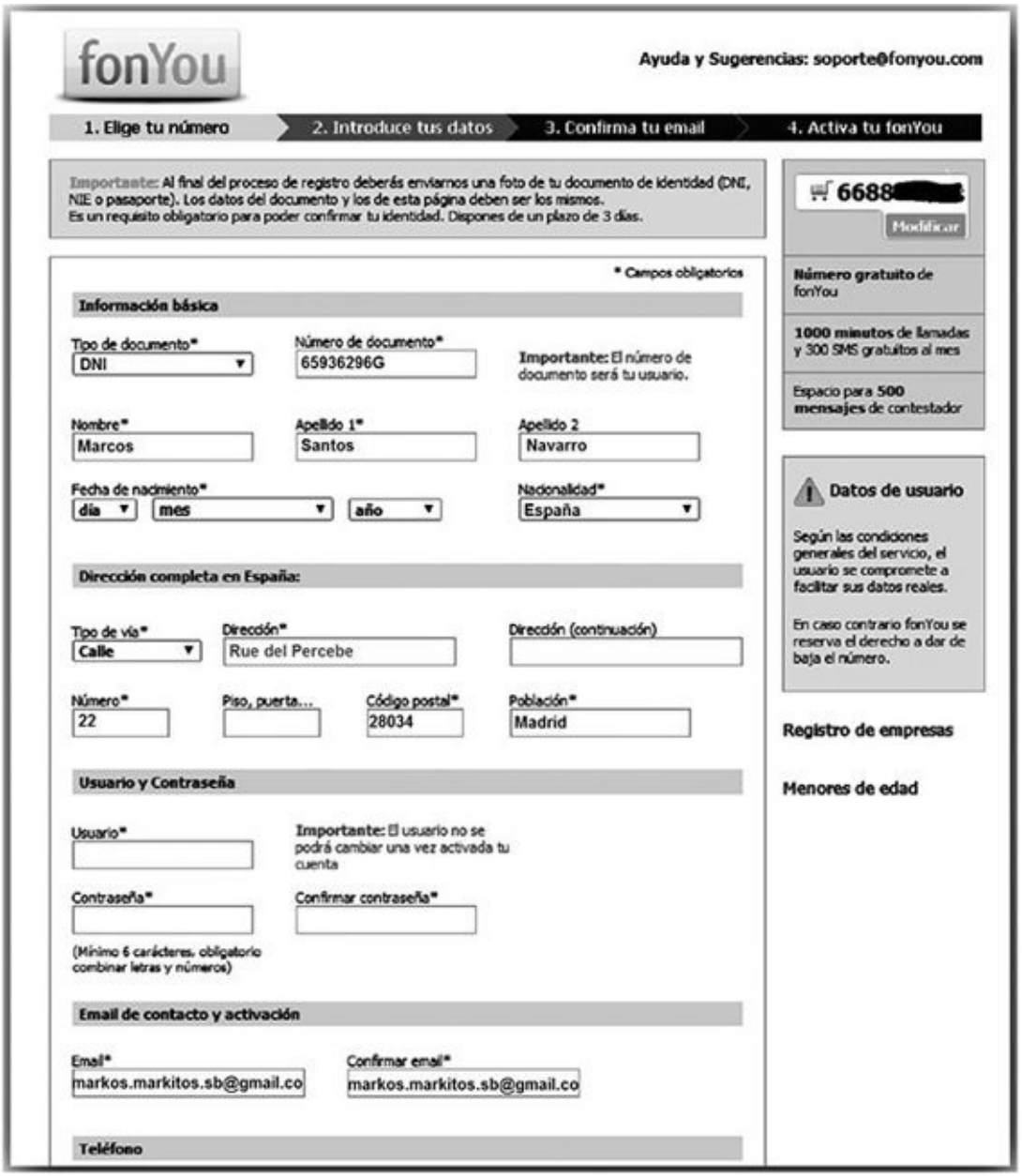
No contento con eso, había añadido otra capa de seguridad a la cebolla. En previsión de que alguien pudiese llegar hasta su contrato con FonYou, había falsificado todos los datos personales, utilizando una dirección que le era familiar y le pareció divertida: Rúe del Percebe.

Aquello me superaba. Nos superaba a todos. Era como intentar descifrar una a una todas las capas de cebolla de TOR.

Llegamos a barajar la hipótesis de que Markos no existiese. De que todo

fuese una farsa. Pero no tenía sentido, en su perfil de Facebook se interrelacionaba con otras personas, como Marga, Stefy o Soraya, su nueva novia. Y ellas eran reales. Yo había hablado con todas. Las había investigado y tenía sus direcciones, teléfonos, todo.

También interactuaba con otros perfiles de Facebook, como un tal Javier Pons, o con su entrenador. Aparecía en varias fotos posando con ellos. Como aparecía antes en las fotos con su novia Silvia Hierro.



La pista de Parlem había resultado un fiasco. Había llegado la hora de intentarlo con el número de Vodafone…

Capítulo 20
Acoso en la red

«Abandonarse al dolor sin resistir, suicidarse para sustraerse de él, es abandonar el campo de batalla sin haber luchado.»

Napoleón Bonaparte

El ventilador de miserias

Todo había empezado hacía poco más de una semana, un par de días antes de reunirme con Hervé Falciani. El 23 de mayo de 2015 desayuné con una sonrisa en la cara. Mientras degustaba el primer café de la mañana eché un vistazo a los perfiles de MarkoSS88 y Soraya, y después a las noticias informáticas del día, y un nuevo hackeo llamó mi atención. Cuatro millones de adúlteros veían peligrar sus matrimonios al salir a la luz sus identidades…[212]

La noticia, publicada en varias webs especializadas primero, y en toda la prensa internacional después, tenía su coña. Mientras exploraba la Deep Web, un investigador de Teksecurity se había encontrado una hoja de cálculo con los datos confidenciales de cuatro millones de usuarios de la web Adult Friend Finder, una página de citas y contactos sexuales extramaritales. Correos electrónicos, fechas de nacimiento, preferencias sexuales… Por supuesto, muchos de los usuarios del *site* eran solteros, pero dadas las características del servicio, la inmensa mayoría buscaba una aventura extraconyugal.

Lo mismo ocurriría dos meses después con Ashley Madison, que usa el eslogan publicitario «La vida es corta. Ten una aventura». Un equipo de hacktivistas autodenominados Impact Team se había hecho con los datos de los 37 millones de usuarios en cuarenta y seis países, de ese portal que facilita coartadas a los cónyuges que quieran ser infieles a sus parejas. España es el país europeo con más usuarios dados de alta en ese servicio.

Los hacktivistas de Impact Teamtambién hackearon la página Established Men, perteneciente a la misma compañía Avid Life Media propietaria de Ashley Madison, y especializada en buscar jóvenes atractivas a hombres adinerados. Y denomino «hacktivistas» a los chicos de Impact Team —aunque sé que Lord Epsylon no aprobaría esa definición— porque los crackers no se lucraron directamente con el ataque, sino que buscaban borrar de la red algo que consideraban inmoral. En lugar de vender la información, dejaron un mensaje en las páginas hackeadas que decía:

> Ordenamos que Avid Life Media elimine Ashley Madison y Established Men, en todos sus formatos, de forma permanente, si no vamos a publicar los registros de todos los clientes, incluidos los perfiles con las fantasías sexuales secretas de los clientes y las transacciones exitosas con tarjeta de crédito, los nombres, las direcciones, los documentos de los empleados y los emails. Las otras páginas pueden seguir funcionando.

Me imaginé a 37 millones de adúlteros maldiciendo a los puritanos hackers, por poner en peligro sus secretos más íntimos ventilando sus miserias, y confieso que se me escapó una sonrisa.

Pero la sonrisa se me congelaría en los labios unos meses después. En agosto, Impact Team cumplía su amenaza y revelaba las identidades de los usuarios de Ashley Madison, identificando a los adúlteros. Dijeron que lo hacían para

desenmascarar a la empresa, que conservaba en sus bases datos bancarios y personales de los usuarios que no tenía por qué tener. Y el ataque comenzó a cobrarse vidas.

Los dos primeros suicidios de usuarios de Ashley Madison se produjeron en Toronto (EE.UU.),[213] y recordé las reflexiones de Román Ramírez, el director de RootedCON, sobre la responsabilidad del hacker que realiza un ataque. Seguro que los activistas de Impact Team no querían esas muertes, pero su poder se les fue de las manos. Y como en todos los ciberataques al final son personas los que pagan las consecuencias.

Un mapa interactivo permitía buscar geográficamente a los usuarios de la web diseñada para las infidelidades,[214] con estadísticas escalofriantes. En Manises (Valencia), una ciudad de 30.000 habitantes, aparecen 1.623 perfiles de usuarios de Ashley Madison. Los juzgados de familia de Manises probablemente tendrán mucho trabajo en los próximos meses.

Pero no solo eso. También estaba disponible la IP del adúltero y su dirección de correo. Entre los usuarios españoles que se habían registrado, existían correos institucionales del Senado o el Congreso de los Diputados. Desde el secretario del PSPV-PSOE en Valencia José Luis Ábalos, hasta la exministra Carmen Calvo, pasando por la diputada socialista Fátima Aburto o el exportavoz de la Comisión de Defensa en el Congreso Jesús Cuadrado. Todos denunciaron que sus emails oficiales habían sido usurpados y negaron ser usuarios de la web. Y algunos, como Ábalos, pusieron la pertinente denuncia en comisaría: «Pensar que utilicé mi correo oficial para algo así es llamarme tonto».[215]

Era previsible que alguien intentara sacar partido de esa información. Así que también empezaron los chantajes. Pero si algo bueno sacamos de todo esto, es descubrir un ejemplo más de cómo empresas webs sin escrúpulos se lucran con el negocio de la soledad. Porque el mecanismo interno de Ashley Madison implicaba que el usuario tuviese que pagar para poder comunicarse con otros supuestos adúlteros. No solo eso, también descubrimos que habían utilizado a muchos famosos como reclamo para atraer a nuevos usuarios: Antonio Banderas, Gerard Piqué, Isabel Sartorius, Benzema, Jose Mourinho, etcétera, aparecían como usuarios de la web… Y no parece muy creíble que un actor de Hollywood o un futbolista de élite necesiten apuntarse en una web para tener la oportunidad de echar una canita al aire…

En el caso de Adult Friend Finder fue peor, porque el autor del hackeo, un tal ROR, no avisó a los clientes de que sus datos ya estaban en la Deep Web, y lo que es más grave, la empresa tampoco dijo nada, porque sabía que si sus usuarios descubrían que sus datos personales y preferencias sexuales eran públicas, abandonarían el servicio.

Así que aquel sábado, 23 de mayo, empezaba animado. Pero la sonrisa se me congeló en la cara cuando otra noticia comenzó a colapsar los titulares, eclipsando totalmente el hackeo de Adult Friend Finder: «Una joven de 16 años se suicida tras

sufrir *bullying* en un colegio de Madrid».

«Estoy cansada de vivir»

El 23 de mayo de 2015 me reafirmé en que era urgente terminar lo antes posible este proyecto. No hay tiempo que perder, cada día que pasa la influencia de las redes sociales es mayor en nuestras vidas, y en nuestras muertes. Y lo que es peor, en las de nuestros niños. Ahora, en este instante, mientras lees estas páginas, niños miserables, cobardes y estúpidos, humillan, se burlan y acosan a otros más pequeños, vulnerables e indefensos, en sus perfiles sociales, en sus wasaps y en los foros del colegio.

Ya había leído mucho sobre esos casos, pero el de Aranzazu me pilló más sensibilizado. Porque ahora comenzaba a comprender la infinita trascendencia de lo que ocurre en la red. Un poder digital que puede llenarnos de conocimiento o destrozarnos la vida.

Todos los informativos abrían con la noticia. Un nuevo caso de *bullying* que terminaba en suicidio. Otro más. Pero el suicidio de Arancha resultaba especialmente dramático, porque la joven sufría una discapacidad motora y otra intelectual de entre el 30% y el 40%, que la hacían comportarse como si fuera una chica de diez años. Por lo que si alguien encarnaba la vulnerabilidad y el desamparo en el instituto Ciudad de Jaén, en el sur de Madrid, era ella. A sus compañeros de clase nunca les importó.

Aquel día —se arrepentirá toda la vida—, su madre, que trabaja todas las noches como limpiadora, llegó como siempre a las seis de la mañana. Normalmente se quedaba despierta esperando a que sus hijos se levantasen de la cama para acompañarlos durante el desayuno, pero aquel viernes, 22 de mayo, se quedó dormida.

Aranzazu, Arancha, despertó a su hermano pequeño, y como cada mañana le preparó el Cola Cao. Hacia las siete de la mañana metió los libros del cole en las carteras, hizo las camas y se despidió de su padre. Al salir del piso se despidió también de su hermano y lo mandó al colegio. Pero ella no salió del edificio. Subió hasta la última planta, la sexta, y se tiró por el hueco de la escalera con la cartera todavía en el hombro. La cartera quedó colgada unos pisos por encima del zaguán. Su padre, Muhammad, escuchó el impacto del cuerpo de su hija contra el suelo de la planta baja. Tampoco se perdonará nunca. Justo antes de saltar envió un mensaje por WhatsApp: «Estoy cansada de vivir».

Aranzazu vino a sumarse a una siniestra lista de víctimas del *bullying*, que no solo acabaron con sus vidas. También destrozaron las de sus padres, amigos, compañeros y, por supuesto, las de sus acosadores. Siempre ocurre lo mismo.

El 21 de septiembre de 2004 Jokin Ceberio (14 años) tecleó en su ordenador «Libre, oh, libre. Mis ojos seguirán aunque paren mis pies». Después cogió su bici, pedaleó hasta lo alto de la muralla de Hondarrabía (Guipúzcoa) y saltó al vacío.

Mónica Jaramillo (16 años) escribió en su perfil de Tuenti antes de ahorcarse, el 9 de noviembre de 2012: «Si hacemos algo mal hoy, intentemos hacer algo bueno mañana» y «Estoy sola, nadie me defiende».

Carla Díaz (14 años) envió a su única amiga un sms en que decía que ya no aguantaba más. En las redes Ask y Tuenti sus compañeros la habían convertido en una mascota digital de la que se burlaban. El 11 de abril de 2013 caminó por la playa de San Lorenzo, en Gijón, subió al acantilado de la Providencia, y desde allí se arrojó al mar.

«Nadie me va a defender —decía en un mensaje enviado poco antes, el 15 de febrero—. No hay huevos.»

Tras la muerte de Arancha, las redes sociales se incendiaron, como siempre. Los acosadores de la pequeña y vulnerable Aranzazu comenzaron a recibir en sus cuentas de Tuenti, Facebook o WhatsApp el mismo trato que habían dado a su víctima. «Jóvenes hijas de puta», escribía Pérez Reverte.[216]

La muerte de Carla, como la de Arancha, Mónica o Jokin, eran muertes anunciadas. Anunciadas en internet. «Les obligaron a suicidarse», dijo uno de los investigadores. Ese mismo año, y solo en Reino Unido, cuatro familias demandaron a la red social Ask por los suicidios de sus hijos a causa del *ciberbullying*.[217]

Amigos y familia claman justicia, o venganza. Los responsables de los centros escolares dicen que lo sienten, que nadie lo vio venir. Los periodistas revisamos sus perfiles sociales y encontramos la historia de su desesperación ilustrada en forma de mensajes en Tuenti, Facebook, Ask, Twitter. Los líderes políticos se solidarizan con los padres, preferentemente si hay una cámara cerca. Y los compañeros encienden velas, pegan carteles y lloran a las puertas del colegio.

Resulta estremecedor tirar de hemeroteca en cada uno de esos suicidios, y comprobar que ya se ha establecido una siniestra rutina. Tras la muerte de uno de esos menores, empujado a la destrucción por las burlas, la humillación y la crueldad de sus compañeros tanto en la red como fuera de ella, siempre se repite lo mismo. Y así hasta el próximo suicidio. Que puede ser el de un hijo, un sobrino, un amigo… Alguien que nos toque más cerca, y más fuerte, que estos nombres escritos en un libro o un periódico, o esas noticias que suenan distantes en el informativo de televisión.

A mí, el caso de Aranzazu me impresionó especialmente. Tal vez porque cuando se produjo, yo estaba sumergido en la investigación sobre nuestras vidas digitales. O quizá porque un mes antes, el 29 de abril, sus padres habían presentado una denuncia ante la Policía por el acoso que sufría la niña, y habían adjuntado los mensajes que la pequeña recibía en su ordenador o en su teléfono móvil: «Guarra, ¿qué dices de mí? Voy a ir a pegarte con mis primas. Me cago en tus muertos. Me vas a dar 50 euros o voy a ir con mis primas y más gente a pegarte». Y se los dio.

Aranzazu comenzó a trabajar cuidando ancianos para pagar la extorsión de sus compañeros. Pero ellos no pararon. Continuaron las humillaciones, burlas, vejaciones y palizas dentro y fuera del colegio. Lo malo es que, en el siglo XXI, y a diferencia de lo que ocurría antes, el acoso no termina al regresar a casa. Continúa a través de la red. Los niños acosados en el siglo XXI ya no tienen un lugar donde esconderse.

La situación es tan aterradora que en diciembre de 2014 aterrizaba en España la plataforma «It Gets Better», especializada en el acoso a escolares víctimas de *bullying*.[218]

Y lo terrible es que, aunque todos esos menores fuesen novatos en el uso de las redes informáticas, ser un experto en tecnología tampoco garantiza tu seguridad. En abril de 2015, un mes antes del suicidio de Aranzazu, la programadora Rachel Bryk, conocida en la industria de los videojuegos por sus aportaciones al emulador Dolphin, se quitó la vida arrojándose desde el puente George Washington, tras soportar durante meses el acoso en las redes sociales. Transexual, los internautas no le perdonaron su cambio de sexo.

Nadie está a salvo. Ni siquiera las famosas. Más allá del Celebgate, Charlotte Dawson era, probablemente, una de las mujeres más deseadas de Nueva Zelanda. Con solo dieciséis años dejó los estudios para recorrer el mundo como modelo, y llegó a convertirse en imagen de varias marcas. En Australia y Nueva Zelanda su fama se multiplicó, cuando comenzó a colaborar en diferentes programas de televisión, hasta fichar como presentadora con varias cadenas. Sin embargo, su belleza, su fama y su reconocimiento social fueron insuficiente defensa contra el feroz y despiadado acoso que recibió en 2012 en Twitter. Charlotte cayó en una profunda depresión a causa de los brutales, crueles y malintencionados comentarios que inundaban su cuenta social, y ese mismo año protagonizó su primer intento de suicidio. Ingresó de urgencia en el hospital de San Vicente, Sidney, donde consiguieron salvarle la vida.

A punto de convertirse en la primera famosa que se habría suicidado por causa del *cyberbullying*, Charlotte aceptó asumir el liderazgo de una campaña nacional contra el acoso en internet. Pero los ataques no cesaron. En febrero de 2014 volvió a sufrir un acoso feroz en las redes sociales. Especialmente activa en ellas, sus amigos y seguidores se preocuparon cuando, el 22 de febrero de ese año, habían transcurrido diecinueve horas sin una sola actualización, algo raro. Y su preocupación estaba justificada. Encontraron su cuerpo sin vida poco después. Había ingerido una sobredosis de fármacos y esta vez los médicos del San Vicente no pudieron reanimarla. El odio y la envidia vertidos en sus redes sociales, en un momento de especial sensibilidad, pudieron más que sus ganas de vivir.[219]

Morir en la red

El primer caso que desató las alarmas internacionales sin duda fue el de Amanda Todd.

Cuando solo tenía doce años, un depredador, uno de esos adultos que patrullan la red en busca de menores a las que seducir, contactó con ella a través de un videochat, haciéndose pasar por otro menor. La pequeña acababa de mudarse con su familia a una nueva ciudad y buscaba nuevos amigos. Lo que encontró fue un infierno.

Después de varios días de charla, su nuevo «amigo» consiguió convencerla para que le enseñase los pechos y grabó la imagen. Un año después, el depredador volvió a localizarla en Facebook y la obligó a desnudarse ante la webcam bajo la amenaza de que, de no hacerlo, divulgaría las fotos de sus pechos. Aterrada, Amanda aceptó. Aun así, el hijo de mil putas divulgó las imágenes. Todas. Solo por el placer de humillarla.

La Policía se presentó en casa de Amanda porque las imágenes habían comenzado a circular entre sus amigos, entre sus vecinos, entre sus compañeros de colegio… Y ella cayó en una profunda depresión que se agravó por el alcohol y las drogas. Un año después, el depredador creo una página en Facebook utilizando las imágenes de Amanda desnuda como foto de perfil. Amanda recibió la incomprensión, el desprecio y las burlas de sus conocidos, hasta que ya no pudo más.

El 7 de septiembre de 2012, Amanda colgó en YouTube un vídeo de nueve minutos de duración titulado: *My Story: Struggling, bullying, suicide and self-harm*. Siempre que lo veo pienso en Angelucho, en X1Red+Segura y en cuántas Amanda estarán ahora mismo viviendo un infierno similar, porque nadie les advirtió de los peligros de la red. Y a sus padres tampoco.

Amanda preparó el vídeo durante horas. Escribiendo en docenas y docenas de tarjetas de cartón su historia. Ella no habla. Supongo que no tenía fuerzas. Se limita a pasar, una a una, aquellas tarjetas explicando lo que había vivido. Pero una de las características de internet es que, ante un grito de auxilio tan desgarrador, los usuarios responden con burlas, crueldad y desprecio.

Amanda continuó soportando el acoso en el colegio, en el barrio y en las redes sociales, solo un mes más. El 10 de octubre, y después de haberlo intentado anteriormente con sobredosis de antidepresivos, Amanda Todd se ahorcó. Tenía quince años. Entonces sí. Su vídeo en YouTube superó los dos millones de visitas en pocos días. Los informativos canadienses e internacionales se hicieron eco del caso. Su vídeo inspiró películas y series de televisión, y se proyecta en muchos colegios como una advertencia a las menores que reciben proposiciones sexuales en la red. Pero no cambió nada.

Antes y después de Amanda Todd, muchos otros niños y niñas, de entre once y diecisiete años, se quitaron la vida tras sufrir el acoso en las redes sociales. Los casos se cuentan por centenares en todo el mundo. En 2015 el número de suicidios anunciados en las redes sociales había aumentado tan preocupantemente que algunas,

como Facebook y Twitter, decidieron tomar medidas.

Mark Zuckerberg, fundador de Facebook, declaró que su red «está actualizándose para ofrecer más recursos, consejo y apoyo a aquellos usuarios que quizá estén lidiando con pensamientos suicidas, así como a sus familiares y amigos». Según él, su compañía «ya cuenta con equipos que trabajan en todo el mundo las veinticuatro horas del día, analizando los reportes de usuarios que avisan de la existencia de comportamientos autolesivos en alguno de sus contactos». El perfil oficial Facebook Safety comunicó que, cuando se notifique que un usuario está compartiendo mensajes que pueden denotar pensamientos suicidas, la plataforma le ofrecerá recursos de ayuda no solo por medio de expertos en salud mental de la National Suicide Prevention Lifeline, una de las organizaciones con las que trabajan en Estados Unidos, sino que también se les animará a que contacten con alguno de sus amigos en la red social y se le ofrecerá una serie de consejos para gestionar estos sentimientos.

Twitter, por su parte, anunció en su blog oficial que estaba reforzando el proceso de denunciar situaciones de inseguridad en su plataforma, y se refirió no solo a la suplantación de identidad o la filtración de datos confidenciales, sino también a las actitudes susceptibles de guardar relación con intenciones suicidas.

Twitter recordó que cuenta con un equipo de seguridad con el que sus usuarios deben contactar en caso de detectar una actitud preocupante en algún perfil o cuenta. La plataforma se pondrá en contacto entonces con la cuenta de la que se ha informado, para notificarle que alguien está preocupado por su salud emocional, y ofrecerle una lista de recursos *online* en los que solicitar ayuda. Una profunda estupidez cuando alguien está a punto de suicidarse…

Yo estoy seguro que el dramático caso de Gabriela Hernández Guerra influyó en esa decisión.

El 7 de noviembre de 2013, a las 12:00, su hermano descubrió el cadáver en su domicilio de Yecuatla, Veracruz, colgado por el cuello de una tela azul. Solo una hora antes, Gabriela actualizó por última vez su perfil en Facebook: «Adiós a todos no tengo nada nada ya no tengo nada. Julio te amooooo, nunca lo olvides. Me voy con una sonrisa de lo feliz k me hiciste mientras duro, a mi familia perdón les pido los quiere Gabi».

El mensaje iba acompañado de una fotografía. En ella aparecía la joven, estudiante mexicana de telebachillerato, de solo veintidós años, con los ojos llorosos pero con una sonrisa en el rostro. En la imagen puede verse perfectamente la misma tela azul, anudada a su cuello con la que se quitaría la vida unos segundos después de apretar en el botón «enviar».

Durante los días previos Gabi, que había roto su relación con el tal Julio, había subido a su perfil varios mensajes advirtiendo sus intenciones, siempre acompañados por fotografías en las que se podía distinguir a distancia la inmensa tristeza.

Ese mensaje del 7 de noviembre fue el último. Facebook tardó quince horas en detectar aquel grito de desesperación y cerrar el perfil de Gabi. Y durante esas quince

horas, 20.800 personas pincharon en «me gusta» a aquella terrible foto, que se compartió 12.500 veces, y recibió 10.200 comentarios. Su perfil alcanzó los 23.000 seguidores.

Una legión de internautas insensibles, crueles y miserables desbordaron la red de comentarios humillantes y burlas contra Gabi. Llegaron a publicar la foto del cadáver —colgado de la misma tela azul que aparecía en su última actualización de Facebook, y que los policías mexicanos filtraron— con comentarios que rozaban el sadismo. En Twitter los *hashtags* #posmematoy#mematocomogabriela se convirtieron en *trending topic*. Y la foto de Gabi, muerta, colgada de la tela azul, sirvió de inspiración para memes de dudosa legalidad, pero indudable crueldad.

Por desgracia, Gabi inspiró a otros: poco después, la brasileña de dieciséis años Rosana Fidencio Ribeiro siguió sus pasos. Como lo haría la británica Simone Back, el también mexicano Leonel Padilla Chávez y tantos…[220]

El caso de Gabriela Hernández Guerra invita a muchas reflexiones. Nos incita a meditar sobre la naturaleza humana, sobre la crueldad de los menores y sobre la ignorancia de los padres. Ya no se trata de que los inmigrantes digitales no familiarizados con la tecnología, como mi madre o el padre de Angelucho, puedan ser estafados o perder sus credenciales en la red. Existen riesgos mucho más graves y urgentes. Y por ello deben aprender.

Cada vez existen más programas, aplicaciones y cursos sobre el control parental. Ya existen las herramientas que permiten a los padres supervisar el uso que hacen sus hijos de las redes sociales. Entonces, ¿por qué no lo hacen? Uno de mis amigos policías estaba deseando darme su opinión sobre ese tema…

La responsabilidad parental

Y allí estaba, recién estrenado el mes de junio, impactado aún por todo lo que había leído y buscando respuestas que no tenía. Pepe me facilitó el primer contacto con su excompañero y superior. Nos reunimos en una cafetería muy cercana a los juzgados de la plaza de Castilla, en Madrid.

El jefe de Policía me permitió consultar las diligencias sobre el enésimo caso que se producía en España. Esta vez ocurrió en marzo de 2013, en Algete (Madrid). Las víctimas: tres chicas de entre dieciséis y diecisiete años, y todas ellas alumnas de uno de los mejores colegios, y más caros, de la ciudad, que se jacta de ofrecer una «educación en valores». Algo deben de estar haciendo mal, cuando, según los informes policiales a los que tuve acceso, «… sobre las 07:00 horas del día 19/02/2013, las Agentes arriba reseñadas, componentes del GAMmA (Grupo de Apoyo a la Mujer y el menor de Algete), son conocedoras de la difusión de unas fotos de contenido sexual, a través de las redes sociales de unas menores del municipio…». Es decir, que antes incluso de que las afectadas cursasen denuncia alguna, sus fotos sexuales ya estaban distribuidas por todo Algete, y hasta llegaron al conocimiento de la Policía. Y si llegaron al conocimiento de la Policía, no es de extrañar que también llegase a la prensa. En pocos días la noticia circulaba por todas las redacciones, igual que las fotos de las chicas. «Fotos porno por WhatsApp: Desarticulan un grupo en Algete» titulaba, a mi juicio con cierta exageración, el diario *Qué*. El alto estatus social de los implicados sin duda añadió morbo al caso.[221]

Supongo que cuesta imaginar cómo debieron de sentirse aquellas chicas cuando en los periódicos de toda España comenzó a airearse la historia de unas fotos que se habían hecho, en la intimidad de su cuarto, con sus propios teléfonos móviles, y de manera voluntaria. De hecho, este punto queda bastante claro en sus declaraciones recogidas en los informes.

JEFATURA DE POLICIA LOCAL
Ayuntamiento de Algete
(Madrid)

Atestado nº: 86/13
Instructor: 280092030
Secretario: 280091062

DECLARACION PRESTADA POR:

Nombre y Apellidos: [redacted]
D.N.I. o pasaporte [redacted]
Lugar de nacimiento: MADRID
Fecha de nacimiento: [redacted]
Padres: JOSE MIGUEL Y PILAR
Domicilio: AVDA DEL [redacted]
(MADRID)
TELÉFONO: [redacted]

En Madrid, siendo las 10-50 horas del día 22/03/2013, ante los funcionarios instructores, y personado en estas dependencias D. JOSE MIGUEL [redacted] con DNI: [redacted] padre de la reseñada anteriormente, el Sr. Instructor dispone se proceda a la exploración del menor, el cual manifiesta:----------
Que hace un año aproximadamente mi amigo Nicolás [redacted] (de mi colegio, [redacted] me empezó a contar sus historias sexuales con una chica, y comenzó a decirme que tenía que empezar a probar a hacer esas cosas ,a traspasar la barrera y dejar de ser tan buena (conversación que tengo grabado en mi ipod). ----------
Que Nicolás sabía que a mi me atraía su amigo Constantin y empezó a decirme por blackberry messenger, que le enviara a éste una fotografía tocándome abajo, y le dije que no. En esa misma conversación empezó a regañarme y a decirme que era una mala amiga por no hacerlo, que cómo podía estar haciéndole esto a su amigo, que no le volviese a hablar en la vida, y que nuestra amistad se había acabado. Me dejó un poco disgustada y me hizo replanteármelo. Al día siguiente hablé con Nico y le dije que me parecía alucinante que me hubiese dicho eso, y que no quería perderle como amigo. Me pidió perdón y al cabo de los días una noche me conecté por blackberry messenger con Nico y Constantin y hablando con este último, manteniendo una conversación un poco subida de tono me pidió que le enviara una foto mía en tetas y yo accedí.----------
Otro día que me volví a conectar con ellos dos, mantuve otra conversación con Constantin y en ese momento Nico me dijo que le enviara un video masturbándome, y que se lo mandara a él para hacérselo llegar a Constantin (quien no estaba recibiendo mensajes por falta de cobertura o por un fallo) y yo le dije que no.----------
A partir de ahí empecé a pensar que ambos estaban compinchados y dejé de hablar con ellos. Pasados unos días fui a hacer skype con Nicolás y yo llevaba trenzas. Ese mismo día me hice una foto de cuerpo entero desnuda y con las trenzas, y se las mande a Constantin. Al minuto Nicolás me mandó un mensaje diciéndome: "Maca quítate las trenzas" ,y fue cuando supe que mis sospechas sobre ellos eran ciertas.------

Aunque sería matizable desde el punto de vista psicológico, legalmente nadie obligó a las chicas a enviar a sus parejas de aquel momento las imágenes eróticas que se habían tomado a petición de ellos. Selva Orejón siempre reseña en sus cursos que por muy enamorada que estés de tu pareja, no tienes ninguna garantía de que esa relación dure para siempre. Y el caso Algete es un ejemplo excelente de lo que puede ocurrir cuando confías tu intimidad a una persona que no merecía esa confianza.

Uno de los jóvenes imputados, Jan (16 años), compañero del prestigioso colegio y receptor de algunas de esas imágenes, esa persona a la que la víctima confió su intimidad, reconoció en su declaración haber sido uno de los responsables de su difusión. Otros, como Ignacio (17 años), se desmarcaron argumentando en su

declaración que «le habían robado el móvil» en cuyo interior estaban las fotografías que le había enviado otra de las víctimas… Por lo tanto, dice, el autor de la divulgación debía haber sido el nuevo propietario del teléfono.

En realidad, no importa si mentía o decía la verdad. Porque incluso aunque fuese cierto que perdió su teléfono con esas imágenes comprometedoras dentro, su historia nos permite subrayar otro hecho que todas las víctimas como estas tres chicas deberían tener presente. La mejor garantía de que unas fotos eróticas no terminen siendo públicas… es que no existan.

Las fotos de las jóvenes de Algete llegaron a las pantallas de televisión. En sus declaraciones, imputados y víctimas reconocen haberlas visto en un reportaje de Cuatro TV. Con la vergüenza que ello implica para ellas y sus familias. Y ese es otro elemento que las jóvenes como ellas deberían tener también presente. Una vez salen de tu teléfono, o de tu cámara, pierdes totalmente el control. Y pasarán meses, o años, te habrás olvidado del tema, y un día, mientras estés comiendo con tu familia frente al televisor, o al abrir el periódico, o al navegar por la red, volverán a aparecer. Así que es mejor pensárselo dos veces antes de apretar el disparador.

—La culpa es nuestra —explotó Pepe, el policía, durante una de nuestras conversaciones sobre este y otros casos similares—, de los padres.

Reconozco que me sorprendió. Pepe es un tipo templado, amigo del debate y la polémica, sí, pero sereno. Y en aquella ocasión el tono de su discurso era diferente. Le conozco hace años y nunca le había visto así. Como si hubiese llegado el momento de decir algo que le venía corroyendo por dentro desde hacía tiempo.

—Te lo voy a decir, Toni, y tienes que contarlo. Detrás de esto no hay kilos de coca, ni redes de prostitución, ni peligrosos terroristas, ni esas infiltraciones tuyas tan emocionantes, pero sí los problemas del día a día de las personas normales, y nuestro sentimiento de servicio público para intentar detectar el problema lo antes posible. Y también es importante.

—Te escucho, te escucho.

—En todas las leyes, protocolos de actuación, desarrollos de ley, etcétera, aparece la puñetera frase: «El bien superior del menor». Se supone que defendemos ese bien superior del menor veinticuatro horas al día, ¿no?

Yo asentí sin atreverme a interrumpir.

—¡Y una mierda! El GRUME, con su ya clásica poca implicación, trabaja mañana y tarde, nosotros solo mañanas, servicios sociales solo mañanas, departamento de inmigración solo mañanas, padres… a ratos. ¿Por qué no hay educadores de calle trabajando codo a codo con los policías? La palabra que falta pronunciar es: *implicación*. Que no la tengan los profesionales que trabajan en este tema es malo, peligroso, preocupante y todo eso. Pero que no la tengamos los padres…, hostias.

Pepe lleva muchos años destinado en el Grupo de Actuación con Menores (GAM) de la Policía Municipal en San Sebastián de los Reyes, sabe de lo que habla.

—Cuando vamos a comprar un ordenador, un coche, una moto, esas cosas tan importantes que hacemos en la vida, echamos los restos. Consultamos a amigos, nos metemos en foros, comparamos ofertas. Pero cuando tenemos un hijo, parece que la naturaleza sigue su curso y no va con nosotros. ¿Sabes qué es lo que veo yo en las calles? ¿O cada vez que tenemos que acudir a un colegio, o a un domicilio, por un problema con menores? Padres que quieren vivir como solteros estando casados. Que quieren tener su tiempo y su espacio para ver el fútbol con los colegas, o para ir de tiendas con las amigas. Como si por tener un hijo ya lo supiésemos todo.

—Pepe, te escucho pero no sé adónde quieres llegar…

—A la tecnología. En nombre de la enseñanza y el aprendizaje, dotamos a nuestros vástagos de lo que nosotros no tuvimos. Y le regalamos una tablet, o un teléfono de última generación, que ni siquiera entendemos. Y después presumimos orgullosos delante del vecino: «Mi chaval es la hostia, no veas cómo maneja el ordenador. Un día de estos le vemos hablando con la NASA». Porque mientras está entretenido con el ordenador, o con el teléfono, nos deja tranquilos y podemos disfrutar de nuestro tiempo, como si volviésemos a estar solteros un ratito más.

Empecé a comprender su discurso. Durante varias de las tertulias en casa de David Madrid o en el restaurante de Madrid, la problemática del menor había acaparado el debate. Y Pepe tiene una dilatada experiencia en todo lo relacionado con el mundo del menor. Desde las bandas juveniles (latin king, skins…), al *ciberbullying*, pasando por el absentismo escolar.

—No te imaginas las cosas que hemos visto. Madres de menores flirteando con los contactos de una red social de su hija, y mandándoles fotos que no le permitiría hacerse a ella. Otras denunciando que su hija está siendo acosada en una red social, cuando no tiene edad para abrirse un perfil. Otras divulgando en internet fotos y datos de sus hijos menores, que cualquier acosador o ciberdelincuente pagaría por tener. Y se los dan gratis. Les preguntas si saben lo que es el control parental, y te miran con cara de alucine… Y sin embargo, su hija de ocho años, ocho años, Toni, sí sabía lo que era el Snapchat. ¿Por qué una niña de ocho años va a usar el Snapchat si su madre ni siquiera sabe lo que es?

Snapchat es una aplicación gratuita para teléfonos iPhone y Android que permite enviar fotos, vídeos o documentos que se «destruyen» entre uno y diez segundos después de que el receptor los vea. Teóricamente solo mayores de doce años pueden utilizarla… teóricamente. Su uso se popularizó para el envío de imágenes íntimas o comprometidas, al menos hasta que en enero de 2014 la seguridad de Snapchat fue hackeada y se filtraron los datos de sus 4,6 millones de usuarios en todo el mundo (nombre, número de teléfono, zona geográfica y demás). Parece que no todas las imágenes se destruían por completo…

Ángel Pablo Avilés, «Angelucho», aboga por la urgencia de una asignatura sobre seguridad informática en los colegios. Y yo estoy de acuerdo con él. Porque los niños, como los inmigrantes digitales, son los más vulnerables. *Ciberbaiting*,

ciberbullying, sexting, grooming… son anglicismos recientemente adoptados por todos los habitantes del planeta para referirse, no a nuevos delitos, sino a la nueva expresión de viejas conductas como el acoso, la pedofilia, el chantaje, la pederastia, etcétera. Internet no ha inventado a los violadores, a los extorsionadores ni a los abusadores, simplemente les ha facilitado las cosas. Les ha dado un arma muy poderosa para acercarse a los niños.

—Les damos la mano para cruzar una calle —prosiguió el policía del GAM—, les ponemos estrictos horarios, les decimos con quién deben ir o no, pero luego por dejadez de funciones, les dejamos que cuenten su vida a extraños, que se relacionen a saber con quién, que visiten con cualquier edad las cientos de miles de páginas porno que existen, que se enamoren y, lo que es peor, que se relacionen con aparentes iguales que resultan ser pedófilos que los chantajean. Nosotros estamos hartos de verlo todos los días. Rafa te lo puede decir.

Rafa, el compañero de Pepe, asentía con el rostro circunspecto. Le conoce bien, han llevado muchos casos juntos, y sabía que la rabia de su amigo estaba justificada en tantos años de calle. Y lo peor estaba por venir.

—Para nosotros esas redes sociales también son útiles. Cuando llega a la oficina un chaval que tiene perfil en Ask, ya lo sabemos todo de él. No nos hace falta que tengan antecedentes. Los antecedentes, hoy, están en la red. ¿Y sabes por qué? Porque lo necesitan. Hoy, para un niño o un adolescente, no tener presencia en las redes sociales significa ser un paria. No tener muchos *likes* o seguidores significa ser un fracasado, un raro. Como llevar gafas o aparato en los dientes en mi época, pero multiplicado por mil. Y ahora viene lo peor, agárrate…

Y me agarré. Iba a necesitarlo. Pepe no va de farol. Puede ser sarcástico, irónico y un rival feroz y apasionado en el debate, pero tiene los suficientes conocimientos y experiencia como para no necesitar faroles. Y había venido preparado. Al momento empezaron a desfilar ante mis ojos las fotos que me enseñaba en su móvil. Nunca me las habría imaginado… Fotos de niñas de diez, doce, trece años, posando en actitud sexy, lanzando besos a la cámara, vestidas con pequeños shorts… Todo muy inocente, salvo a ojos de quien no lo es. Muchas de esas fotos, tomadas por sus propios padres orgullosos de la belleza de sus hijas, sin duda acabarán en las páginas de pedófilos de la Deep Web. Y Pepe continuó abriéndome nuevos frentes.

—¿Sabes cuál es el insulto favorito entre las féminas púber en los mejores colegios de Madrid? «Gorda.» Y no te imaginas cuánto daño puede hacer esa palabra. Cuando hemos empezado a hacer el seguimiento de algunos casos en redes sociales, nos hemos quedado aterrorizados por lo que está pasando ahora con las chicas de diez, doce, dieciséis años… ¿Sabes qué es el *thigh gap*?

—No tengo ni la menor idea. ¿Una nueva red social?

—No. Es… no sé cómo explicártelo… El triángulo ese que tienen que tener entre las piernas que deja pasar la luz, porque si no, nunca serás nadie…

Pepe lo ilustró con una de las fotos en las redes sociales de moda entre las

adolescentes: se trata de tener las piernas tan delgadas, que al unir las rodillas continúa quedando un espacio entre los muslos. Para las jóvenes era la última moda, y el mundo se dividía entre las que no tenían *thigh gap* y las que sí. Aunque para ello tuviesen que dejar de comer y rozar los límites de la bulimia y la anorexia.

—Joder, Pepe, no sé qué decir… Estoy alucinando.

—Mi reflexión es: ¿qué hacemos los padres? Si en los colegios hay recortes y nosotros les damos un teléfono de última generación para que no nos molesten… ¿Quién los educa? Pues internet. Y todo lo que ellos ven lo imitan. Ahora empezamos a encontrarnos con los primeros casos de *achante* o *cutting* en España. Yo llevo años en la Policía y nunca había visto esto. ¿De dónde crees que lo sacan? Pues de internet. Y deberías ver las fotos que tenemos en la Jefatura del reconocimiento médico de algunos de esos niños. Es lo mismo que ocurre con las «princesas», que adelgazan, y adelgazan siguiendo los consejos que encuentran en las páginas pro anorexia y bulimia. ¿En serio que los padres no se dan cuenta? Yo puedo entender que cuando un padre abre un perfil en Facebook, su hijo emigre a otra red social, pero nuestra responsabilidad es protegerlo, vaya donde vaya.

El discurso de mi amigo me había dejado exhausto. Aquel torrente de reproches, evidente catarsis del policía que necesitaba desahogarse, podía ser matizable, debatible, discutible… pero estaba lleno de argumentos.

Cuando el menor es culpable… y el padre también

Emilio Calatayud Pérez es el titular del Juzgado de Menores número 1 de Granada, y le guste o no, se ha convertido en un juez mediático. No por el éxito de sus libros, como *Legislación básica sobre menores infractores* o *Reflexiones de un juez de menores*, ni por la actividad del blog que realiza con el periodista Carlos Morán.[222] Lo que realmente ha catapultado al juez Calatayud a los titulares de los informativos son sus creativas y originales sentencias, en las que trata de conmutar la cárcel por servicios a la comunidad.

- Impartir 1.000 horas de clases de informática a estudiantes a un joven que había crackeado varias empresas granadinas provocando daños por valor de 2.000 €.
- 100 horas de servicio a la comunidad patrullando junto a un policía local por haber conducido temerariamente y sin licencia.
- 50 horas dibujando un cómic de 15 páginas, en el que cuenta la causa por la que le condenaban.
- Visitas a la planta de Traumatología de Granada por conducir un ciclomotor sin seguro de circulación.
- Para un joven que circulaba borracho, visitar durante un día entero a parapléjicos, hablar con ellos y sus familias para elaborar más tarde una redacción.
- Trabajar con los bomberos por haber quemado papeleras.
- Trabajar en un centro de rehabilitación por haber acosado a una anciana.
- 200 horas en una tienda de juguetes por haber robado ropa.

Sus conferencias, lo digo por experiencia, son tan divertidas y desternillantes como las del fiscal Bermúdez o «el Maligno» Chema Alonso. E igual de profundas. Porque su discurso se basa en los mismos pilares: un hondo conocimiento teórico de su área profesional, y una dilatada experiencia. He asistido a conferencias de Calatayud en las que, sin esbozar en ningún momento la más mínima sonrisa, podía hacer que toda la audiencia se desternillase, antes de arrojarnos un jarro de agua fría cortando todas las carcajadas con el filo de la dura realidad a la que se enfrenta cada día en su juzgado.

—Yo también soy padre, y no puedo decirle a otro padre lo que tiene que hacer para educar a su hijo —decía el juez en una de esas estupendas conferencias—. Pero utilizo este pequeño decálogo para explicarle a los padres lo que sí tienen que hacer si quieren crear a un pequeño delincuente:

1. Comience desde la infancia dando a su hijo todo lo que pida. Así crecerá convencido de que el mundo entero le pertenece.
2. No se preocupe por su educación ética o espiritual. Espere a que alcance la mayoría de edad para que pueda decidir libremente.
3. Cuando diga palabrotas, ríaselas. Esto lo animará a hacer cosas más graciosas.
4. No le regañe ni le diga que está mal algo de lo que hace. Podría crearle complejos de culpabilidad.
5. Recoja todo lo que él deja tirado: libros, zapatos, ropa, juguetes. Así se acostumbrará a cargar la responsabilidad sobre los demás.
6. Déjele leer todo lo que caiga en sus manos. Cuide de que sus platos, cubiertos y vasos estén esterilizados, pero no de que su mente se llene de basura.

7. Riña a menudo con su cónyuge en presencia del niño, así a él no le dolerá demasiado el día en que la familia, quizá por su propia conducta, quede destrozada para siempre.
8. Dele todo el dinero que quiera gastar. No vaya a sospechar que para disponer del mismo es necesario trabajar.
9. Satisfaga todos sus deseos, apetitos, comodidades y placeres. El sacrificio y la austeridad podrían producirle frustraciones.
10. Póngase de su parte en cualquier conflicto que tenga con sus profesores y vecinos. Piense que todos ellos tienen prejuicios contra su hijo y que de verdad quieren fastidiarlo.

Con un particular sentido de la ironía, Calatayud afirma que desde su puesto como juez de menores ha percibido tres cosas buenas de la crisis económica: que los niños han vuelto a la escuela —porque ya no tienen ladrillo en el que trabajar—; que los padres están más en casa —porque hay mucho paro—; y que ya no hay víctimas, porque no queda nada que robar. Esos tres factores, dice Emilio Calatayud con una ironía no exenta de realismo, han ayudado a que baje la delincuencia. Sin embargo, hay dos delitos que están subiendo como la espuma, y son los que empiezan a abundar en su juzgado: el maltrato de los hijos a los padres,[223] y los móviles, «el internet», como él dice.

—Ahora los padres le regalan a sus niños los móviles de última generación. Y yo creo que igual que se hacen móviles para gente mayor, con algunas funciones limitadas, deberían fabricarse móviles para los chavales. Y esto es una droga… —dijo el juez al tiempo que levantaba su teléfono móvil con la mano, y repitió—: Esto es una droga. Yo juzgo casos de menores que cometen delitos entre los catorce y los dieciocho años. Y a nosotros no nos llega ningún caso de menor drogadicto, nos llegan maltratadores. En los últimos quince días nos han llegado cinco casos como este: niño que llevaba tres meses casi sin dormir, enganchado a un juego en red. La madre se dio cuenta y le quitó el móvil. Pues al niño le dio el mono. Le dio tal paliza que le rompió la nariz, y su madre era invidente… El otro día, una chavala de quince años, la madre le quita el móvil y le dio una paliza brutal a la madre y luego se intentó autolesionar… Esto es una droga.

El juez Emilio Calatayud, que no es un nativo digital y tampoco tiene demasiada vocación de inmigrante, se ha dado de bruces con esta nueva realidad social que afecta a su ámbito de trabajo. Y que nos enfrenta a otra dimensión de las nuevas tecnologías en el ámbito legal:

—Cuando decretamos el internamiento terapéutico de un menor tenemos que especificar si el internamiento es por salud mental o tóxicos. Y esto —insistió Calatayud volviendo a levantar su teléfono móvil— ya lo consideramos un tóxico.

»Y otra cosa: es un instrumento muy peligroso para cometer delitos. De hecho, este es el otro gran delito que está subiendo como la espuma. Yo creo que los centros escolares deberían prohibir su uso en el interior del centro. Amenazas, coacciones, chantaje, acoso, injurias, delitos contra la intimidad, delitos contra el honor, delitos sexuales… Y también es un instrumento de captación, donde el menor es la víctima. Pero yo de eso no me ocupo, yo me ocupo cuando el delito lo comete el menor… y

está subiendo como la espuma.

—Todos nos planteamos cómo reaccionaríamos si somos los padres de la víctima… Todos nos hemos sentido un poco los padres de Mariluz, de Sandra Palo… pero sería bueno saber cómo reaccionaríamos si somos los padres del niño autor. Antes los padres estábamos todo el día preocupados por nuestros hijos, hasta que llegaban a casa. Ya está en casa, ya está a salvo… Ahora no. Ahora el peligro puede empezar cuando está en su cuarto pegado al ordenador. Porque ahí puede estar cometiendo un delito o siendo víctima de un delito. Y ojo, los padres son responsables de los delitos cometidos por sus hijos. Cuando yo condeno a un menor, también condeno a los padres. Y si el delito se comete en el recinto escolar, también a los responsables del centro.

Desde hace un tiempo el juez Calatayud recomienda a los padres de los menores que procesa que se lean un documento. Es el contrato que una madre norteamericana hizo firmar a su hijo antes de comprarle un iPhone. Yo no lo conocía, lo descubrí gracias a él. Las cláusulas de ese contrato, según Emilio Calatayud, deberían tenerlas en cuenta todos los padres[224]:

1. Es mi teléfono. Yo lo compré. Yo lo pagué. Yo te lo presto. ¿A que soy genial?
2. Yo siempre sabré la contraseña.
3. Si suena, cógelo. Di «hola». Sé educado. Coge siempre, siempre, la llamada de mamá y papá.
4. Entregarás el teléfono a mamá o a papá a las 7:30 de la mañana cada día de colegio y a las 21 horas durante el fin de semana. Estará apagado toda la noche y se volverá a encender a las 7:30 de la mañana. Si no llamarías al teléfono fijo de alguien, porque pueden responder sus padres, tampoco llames o envíes mensajes al móvil. Respeta a las otras familias como nos gusta que nos respeten a nosotros.
5. No te llevarás el iPhone al colegio. Conversa y habla con la gente y con tus amigos en persona. Los días de media jornada, las excursiones y las actividades extraescolares requerirán consideraciones especiales.
6. Si el iPhone se cae, se golpea o se estropea, tú eres el responsable. Por tanto, asumirás los costes de la sustitución o de la reparación. Para ello ahorra dinero de tu cumpleaños o realiza otros trabajos: corta el césped, haz de canguro… Si el iPhone se rompe, tendrás que estar preparado.
7. No uses el iPhone para mentir, hacer tonterías o engañar a otro ser humano. No te involucres en conversaciones que sean dañinas para los demás. Sé un buen amigo.
8. No envíes mensajes, correos electrónicos o digas nada a través del iPhone que no dirías en persona.
9. No envíes mensajes, correos electrónicos o digas a alguien algo que no le dirías en voz alta y en presencia de sus padres. Autocensúrate.
10. Nada de pornografía. Busca en la web información que compartirías abiertamente conmigo. Si tienes alguna duda sobre algo, pregunta a alguien. Preferiblemente, a tu padre o a mí.
11. Apágalo o siléncialo cuando te encuentres en lugares públicos. Especialmente en restaurantes, en el cine o mientras hablas con otro ser humano. No eres una persona maleducada, no dejes que el iPhone cambie eso.
12. No envíes ni recibas imágenes íntimas tuyas ni de otras personas. No te rías. Algún día estarás tentado de hacerlo, a pesar de tu gran inteligencia. Es arriesgado y puede arruinar tu vida de adolescente, joven y adulto. Es siempre una mala idea. El ciberespacio es más poderoso que tú. Y es difícil hacer que algo de esa magnitud desaparezca, incluyendo una mala reputación.
13. No hagas millones de fotos o vídeos. No hay necesidad de documentar todo. Vive tus experiencias. Quedarán almacenas en tu memoria para toda la eternidad.
14. A veces conviene dejar el iPhone en casa. Siéntete seguro de esa decisión. No es un ser vivo ni una ninguna extensión de tu cuerpo. Aprende a vivir sin él. Tienes que vencer el miedo a perderte algo

que está ocurriendo y a estar siempre conectado.

15. Bájate música que sea nueva o clásica o diferente de la que millones de chicos como tú escuchan, que es siempre lo mismo. Tu generación tiene un acceso a la música mayor que cualquier otra de la historia. Aprovecha ese don. Expande tus horizontes.
16. De vez en cuando puedes jugar a juegos de palabras, puzles y rompecabezas.
17. Mantén los ojos abiertos. Observa el mundo que te rodea. Mira por la ventana. Escucha a los pájaros. Date un paseo. Habla con un desconocido. Pregúntate si es necesario buscar en Google.
18. Meterás la pata. Te quitaré el teléfono. Nos sentaremos y hablaremos sobre ello. Volveremos a empezar. Tú y yo siempre estamos aprendiendo. Somos un equipo. Estamos juntos en esto.

La autora de este lúcido documento es Janell Burley Hofmann, una madre estadounidense con cinco hijos. Lidera un movimiento que pretende educar en el uso responsable de las nuevas tecnologías en la familia. El contratante era su hijo Gregory, de trece años. No quiero resultar melodramático, pero probablemente, si los padres de muchos niños víctimas del *ciberbullying*, *sexting*, *grooming*, etcétera, hubiesen hecho firmar a sus hijos un contrato parecido, hoy seguirían vivos.

Me vinieron a la cabeza las últimas palabras que me había dicho Pepe antes de despedirnos:

—Lo que nuestros hijos suben a la red, como esas fotos «inocentes» que has visto, estará ahí para siempre. No se borra nada. La información que tengan los servidores de las grandes empresas se venderá a otras que desarrollen programas para cruzar datos y metadatos. Por no hablar de los ciberdelincuentes… Control parental, y educación en valores entre padres e hijos. No, no son juguetes.

Estábamos a punto de descubrir hasta qué punto esas palabras reflejaban una terrible realidad. Subir cualquier foto a internet, cualquiera, puede encerrar unos riesgos insospechados. Nosotros al menos jamás lo habríamos sospechado. Pero MarkoSS88 había descubierto el filón…

JUNIO DE 2015
EL LADRÓN DE VIDAS

«El hombre tiene una tendencia natural a mostrarse ingrato.»

Adolf Hitler, citado por su secretaria Christa Schroeder en sus memorias

—Toni, soy Álex. Tenemos que vernos.

—Estoy en Girona, con un hacker que…

—Tenemos que vernos. Hemos encontrado algo de Markos. Es importante.

No hizo falta decir más.

Rafa fue quien lo descubrió, mientras revisaba una vez más, la enésima, las fotos que MarkoSS88 tenía publicadas en Telegram y Line a través del teléfono 668… Una fotografía en la que Markos aparecía posando con un uniforme de un equipo de fútbol local, rodeado de compañeros con la misma equipación verdiblanca. Lógicamente no precisaba cuál, aunque se parecía mucho a la del Real Betis, y por un momento pensamos que podría estar en Sevilla. Olía a pista.

Rafa compartió la foto con varios de nuestros amigos policías implicados en la investigación. Código hacker: diez cerebros piensan mejor que uno. Y funcionó.

Fue Rubén, el miembro de las UIP que había sufrido en sus propias carnes las palizas del 22-M, el que se dio cuenta de que en la camiseta aparecía un patrocinador: «Concesionario D. Domínguez Tecno». Fue fácil averiguar que se trataba de una empresa balear. Nada que ver con Sevilla. A partir de ahí resultó sencillo dar con el equipo en cuestión. En uno de sus emails Markos me había dicho que se estaba quedando en casa de un camarada «con el que juego al fútbol». Y parecía que era cierto. Solo lo parecía…

El uniforme verdiblanco que vestía Markos en las fotos no era del Betis. Pertenecía a un pequeño club, de un barrio del norte de Palma de Mallorca. El Son Oliva tenía su propio espacio en la página de la Federación de Fútbol Balear, una web propia y un blog. En todas se incluían muchas fotos de los jugadores, así que no hizo falta buscar demasiado. En un par de *clics* apareció MarkoSS88 regateando al equipo contrario, o posando con sus compañeros. Parecía que no nos había mentido después de todo… Solo lo parecía.

Escrupuloso, como buen policía, Rafa continuó buscando en las web deportivas, a la caza de alguna noticia o artículo en que se identificase a los

jugadores por su nombre. Y lo encontró. Concretamente en el blog. Una de las entradas estaba dedicada a la plantilla de la temporada 2010-2011, con la goleada de cada uno de los jugadores, su nombre y su foto.[225]

—Ahí lo tienes —me dijo el policía cuando nos reunimos en Madrid para ponerme al día del descubrimiento—. Tu MarkoSS88.

Era él, no había duda. Conocía aquella cara como si fuera la de alguien de mi familia. Llevaba casi año y medio obsesionado con él. Pero había algo que no encajaba. El joven que aparecía en las fotos del equipo de fútbol no se llamaba Marcos. Sino Jordi. Lógicamente no divulgaré sus apellidos ni los de su novia y familia.

Y Rafa se dio cuenta de algo más. En su blog, Markos había dicho que salió de prisión el 25 de junio de 2013. Meticuloso hasta la obsesión, como buen policía, Rafa había seguido el rastro de nuestro futbolista y había encontrado una referencia, en la página www.ffib.es, a una sanción recibida en un partido, el 15 de mayo de 2013, mientras supuestamente estaba en prisión.

—O sea, que es cierto que nunca estuvo en la cárcel. Manu tenía razón…

—Espera, no te precipites —me cortó Pepe—. Hay más.

—¿Qué es lo primero que harías al tener su nombre? —me preguntó Rafa con evidente ironía.

—¿Buscarlo en Facebook?

—Exacto. Pero agárrate fuerte. Nosotros ya lo hemos hecho.

Abrí la web de Facebook, introduje mis credenciales, y tecleé el nombre y los dos apellidos de Jordi en el buscador. El gestor de perfiles fue directo. No existía ningún usuario más con su nombre. Y de pronto lo entendí todo.

Fue una revelación. La iluminación de Siddharta. La manzana de Newton. En un instante el rompecabezas había cobrado sentido.

Allí, ante mis ojos, en el perfil personal de Jordi, estaban todas las fotografías que MarkoSS88 llevaba año y medio utilizando en sus redes sociales. No solo eso. Allí estaba su novia Silvia Hierro, la estudiante madrileña de diecinueve años que no existía en el censo de población español. Porque no se llamaba Silvia, sino Sara, era la novia de Jordi y quería ser modelo. Al menos tenía un perfil en una web especializada. Por eso Markos y Silvia parecían una pareja de postal es sus perfiles neonazis… es que lo eran.

Era un caso de manual. Un ejemplo perfecto de robo de identidad digital. MarkoSS88 había hurtado la vida de esos dos chicos para construir la suya propia en internet.

Ahora lo entendía todo.

Ahora comprendía por qué cuando MarkoSS88 publicaba fotos de sus heridas no se le veía el rostro… porque Jordi no tenía las heridas que

Markos necesitaba para fortalecer su relato del skin que se pegaba con los antifas, y al que acosaba la Policía.

Ahora entendía por qué Silvia Hierro, la chica que no existía, había roto su relación con MarkoSS88 y había desaparecido de la red. Porque Sara y Jordi iban a ser padres, y en las fotos de los últimos meses Sara aparece orgullosa y radiante, presumiendo de su tripita. Un bebé no encajaba en la historia de MarkoSS88, así que eliminó a Silvia Hierro de su ecuación, y abandonó los perfiles que había creado para interactuar con los de Markos, dando credibilidad a su personaje.

Ahora sabía por qué las fotos que MarkoSS88 subía a internet estaban tomadas en Mallorca, pero subidas a la red desde Madrid, según delataba la geolocalización de sus tuits. Porque Markos se nutría de las imágenes que Jordi iba subiendo a su perfil de Facebook, escogiendo las que más le convenían para reforzar su historia.

Al comparar los perfiles sociales de Jordi y Markos, todo tenía sentido. Jordi, un joven deportista y bien parecido, colaboraba en varios proyectos infantiles. Las fotos de menores que MarkoSS88 y su álter ego Silvia Hierro habían utilizado en sus perfiles sociales, presentándolos como sus sobrinos o primos para afianzar su historia, estaban también allí, en el perfil de Jordi, abierto de par en par para que cualquier internauta pudiese robar sus fotos y hacer con ellas lo que quisiese. Nunca las advertencias de Silvia Barrera, Selva Orejón, Angelucho, Israel Córdoba, David Pérez o César Lorenzana me parecieron tan claras y acertadas.

En el perfil legítimo de la pareja había también fotos de Jordi posando sonriente y abrazado con amigos y compañeros de raza negra. Esas lógicamente Markos nunca las utilizó. No servían para sus propósitos.

También estaban las fotos que tanta credibilidad dieron a la historia de MarkoSS88 como miembro de UltraSSur. En ellas es Jordi quien posa, con una camiseta del Real Madrid, en las gradas del Bernabéu. Fueron tomadas en octubre de 2013.

Cualquiera podía leer explorando sus perfiles de Facebook, totalmente abiertos, que Jordi y Sara viajaron a Madrid para ver un partido del Real Madrid contra Juventus que se jugó el 23 de octubre, y aprovecharon para hacer turismo en la capital. Se alojaron en un hotel de La Latina. Visitaron el museo del Bernabéu, la Plaza Mayor, el parque del Retiro… y también el Vicente Calderón. Pero MarkoSS88 nunca utilizó las fotos de Jordi en el Calderón. No encajaban con su historia de un ultraSSur…

Allí estaba todo. A disposición de cualquiera. MarkoSS88 solo tenía que pasarse por el Facebook de Jordi con la cesta de la compra y llevarse todas las imágenes que necesitaba para componer su personaje. Y como Jordi y Sara continuaban alimentando sus perfiles sociales, abiertos y sin ningún tipo

de control, Markos podía seguir ilustrando su falsa vida digital indefinidamente. Al menos hasta que mis amigos se interpusieron en su camino.

Allí estaba también la foto que MarkoSS88 había escogido para su perfil. En realidad era Jordi en ese viaje a Madrid. En la foto original, en color, Jordi aparecía con un chándal, posando serio en el estanque del Retiro. Markos la había volcado a blanco y negro y había utilizado un programa de edición digital para sobreimpresionar en el chándal de Jordi unas palabras en alemán y una cruz céltica. De pronto, vestía una sudadera nazi.

Pero había más. Descubrimos la identidad del entrenador, de su amigo Javier Pons, y de otros supuestos «camaradas» que no solo se interrelacionaban con Markos en las redes sociales, sino que demostraban conocerlo personalmente, y que aparecían a su lado en varias fotos. Fotos que no encontramos en el perfil de Jordi… ¿Cómo era posible?

No tuvimos que investigar mucho. Rastreando a los amigos de Jordi en Facebook llegamos a los perfiles de su padre, su madre y de su hermano. Markos también los había desvalijado. Y después había creado otros perfiles falsos, como el de ese tal Javier Pons, para poder colocar en él fotos en las que se vería a Markos con su camarada Javier. Cuando en realidad se trataba de imágenes de Jordi con su hermano robadas de internet. Podía comentarlas, etiquetarlas, y todos verían que Markos era una persona de carne y hueso, con amigos con los que quedaba y se fotografiaba… Todo mentira.

Jordi tenía su perfil de Twitter protegido, pero el de Facebook estaba totalmente abierto. Ese fue su pecado. Casi podía escuchar la vocecita de

Angelucho susurrando en mi oído: «¿Ves? ¿Qué decimos en los cursos de X1Red+Segura? Los perfiles sociales son para los amigos, no para que los vea todo el mundo… O te puede pasar esto».

Y esto es grave. Muy grave. Durante más de un año yo viví obsesionado con el joven de las fotos, al que identificaba con el skin que confesó haber intentado matarme. Pero durante mucho más tiempo, MarkoSS88 provocó la ira y el odio de los antifas en acalorados debates que solían terminar con amenazas de muerte por ambos bandos. Amenazas que llegaron a salpicar a la novia de Markos, la inexistente Silvia Hierro, que sin embargo tenía el rostro de Sara. ¿Qué habría ocurrido si Jordi o Sara vuelven a viajar a Madrid, y por desgracia se cruzan con un grupo de antifascistas que los reconocen como MarkoSS88, el asesino de latinos, y su novia Silvia?

La próxima vez que pienses que proteger tu vida digital, la de tus hijos o las de tus padres no es tan importante, recuerda a MarkoSS88.

Capítulo 21
El hacking y la ley

«Bajo esta máscara hay algo más que carne y hueso, bajo esta máscara hay unos ideales, señor Creedy, y los ideales son a prueba de balas… El pueblo no debería temer a sus gobernantes, los gobernantes deberían temer al pueblo.»

V de Vendetta, James McTeigue, 2006

Ciberjusticia

Llegué pronto. Ya conocía la Facultad de Telecomunicaciones de la Universidad Politécnica porque allí había asistido anteriormente a otros eventos sobre seguridad informática, pero me gusta tener un rato para buscar el lugar más adecuado en la sala, cerca de la puerta, antes de que otros asistentes me pillen el sitio.

Acomodé mis cosas en uno de los asientos y volví a salir al pasillo en cuanto me sonó el teléfono. Era mi madre. Entusiasmada. Creía que me había encontrado el trabajo de mi vida. Nunca le gustó demasiado lo que hago.

—Este sí, hijo, me lo han mandado por email. Vas a ganar mucho más que con eso que haces y no vas a tener que meterte en esos líos. Que nos das unos disgustos a tu padre y a mí…

—Que no, mamá, cómo te lo tengo que decir, que nadie regala nada, y menos por internet.

—Pero por lo menos léete la oferta. ¡Que son 3.000 euros al mes solo por tramitar los pagos de sus agentes! Y la empresa es de verdad que ya lo he googleado como me enseñaste…

—Vale, me la leo, reenvíame el email. ¡Pero no pinches en ninguna letrita azul! Me da que es para hacerte mula.

—¿Mula? ¿Me estás llamando burra? Un respeto a tu madre…

Como suponía, con cinco millones de parados dejándose la piel en las calles cada día, en busca de cualquier tipo de trabajo, empleos como este que aterrizan en tu buzón de correo solo pueden ser una trampa.

Pero cree el ladrón… Y mi madre, que es buena persona, cree que el resto del mundo también es de su condición. Como millones de internautas que, a causa de esa presunción de inocencia para con todo lo que llega a sus emails, caen diariamente en las redes del cibercrimen.

La oferta no podía parecer más inocente y tentadora. 3.000 euros al mes, más comisiones, por recibir los pagos de los clientes de una prestigiosa empresa y reenviarlos a sus mánagers de atención al cliente. Además, en teoría, no tenemos nada que temer sobre el origen del dinero. La oferta especifica que «todos los clientes han de pasar el control de verificación, nos preocupamos por la seguridad de nuestra empresa».

Esta es solo una de las mil caras con las que los ciberdelincuentes reclutan «mulas» para mover el dinero negro. Ante la aparente inocencia de esta oferta laboral se esconde un delito. La mula recibe el dinero robado en su cuenta y lo retira para mandarlo a través de servicios como MoneyGram o Western Union, entre otros, o reenviándolo por PayPal, su propio banco, etcétera.[226]

Los estafadores son muy hábiles, el email puede ir personalizado y argumentar que se trata de una oferta laboral solo para tu provincia, porque utilizan programas

automáticos que identifican tu IP. Incluso pueden usar empresas que existen realmente, para dar mayor verosimilitud a la trampa. Tanto Chema Alonso como Angelucho dedicaron también un post de su blog a este tema que tan cruelmente se aprovecha de la angustia que genera el paro.[227]

Por desgracia, la crisis económica hizo que miles de ciudadanos honrados cayesen en la trampa, convirtiéndose en mulas del cibercrimen y siendo procesados como tales. Porque la pista del dinero llegaba hasta ellos.

Ante el terrible incremento de este tipo de engaños, que se produjo en 2015, la empresa Adecco creó un decálogo de medidas para quienes buscan trabajo a través de internet, y caen en trampas como las mulas.[228]

1. Utilizar solo webs fiables y de confianza en búsqueda de empleo. Estas web garantizan que todos nuestros datos estarán protegidos de acuerdo a las leyes españolas o internacionales en protección de datos.
2. Nunca proporcionar datos bancarios ni números de tarjetas de crédito.
3. No pagar por participar en un proceso de selección. Ninguna oferta ni empresa seria pide dinero para participar en una oferta vacante.
4. Experiencia: en su gran mayoría, las empresas siempre solicitan experiencia y/o formación previa para postularse a una vacante. Huir de aquellas que ofrezcan grandes salarios sin ningún tipo de experiencia.
5. Todo proceso de selección debe tener una parte de entrevista personal anterior a la contratación. Contrataciones *online* o únicamente telefónicas no suelen ser muy comunes.
6. El salario ofrecido no puede ser demasiado alto; si es superior a la media del mercado, es mejor desconfiar.
7. Los bonos y compensaciones extras no pueden ser superiores a lo que dicta la ley.
8. No enviar email con el currículo de forma indiscriminada, ni dejar copia del CV en ordenadores públicos.
9. Asegurarnos de que detrás de las ofertas hay empresas serias y que darán un trato confidencial a nuestros datos.
10. Estar alerta y utilizar el sentido común. No rechazar todas las ofertas de empleo que nos lleguen, pero sí asegurarnos de su fiabilidad.

Di aviso del correo a las unidades de ciberpolicía y preparé la grabadora. Los ponentes de las V Jornadas del Foro de la Gobernanza de Internet en España estaban entrando en la sala. Y yo tenía especial interés por una de ellos.

David Pérez me había insistido mucho: «Tú dile que vas de mi parte, y dile que este año la esperamos de nuevo en Navaja Negra. El año pasado se lo pasó genial…». Y así lo hice.

La fiscal Elvira Tejada participaba en las nuevas Jornadas del Foro de la Gobernanza de Internet. Compartía panel con Francisco Pérez Bes (INCIBE), Fernando Cocho (H4dm) y Francisco Javier García (Iberdrola). Todos ellos moderados por José de la Peña.

Cuando terminó el acto la esperé a la salida, y la abordé directamente.

Elvira Tejada de la Fuente es fiscal de Delitos Telemáticos de la Fiscalía General del Estado y una de las redactoras de la nueva ley que trae de cabeza a los hackers. Ley que ella defiende con uñas y dientes, a pesar de que contempla situaciones

realmente polémicas.

—Es fundamental que el ordenamiento jurídico sea capaz de evolucionar, para irse adaptando a las nuevas situaciones que la evolución tecnológica está produciendo, pero sin olvidar los principios y valores esenciales sobre los que se sustenta el ordenamiento jurídico que son la base del Estado de derecho. Por ejemplo, en las Leyes Orgánicas 1 y 2 de 2015 que entrarán en vigor el próximo 1 de julio… Se modifican las penas por delitos de pornografía infantil, para adaptar nuestra normativa interna a la normativa internacional. Concretamente la directiva 93/2011 de la Unión Europea y Convención de Lanzarote del Consejo de Europa… Se tipifica como delito el acceso *online* a pornografía infantil y se contempla la opción del juez de retirar contenidos ilícitos, acordar la interrupción de servicios o el bloqueo… Se modifican sustancialmente los delitos contra la Propiedad Intelectual, páginas de enlace, básicamente… Incorporación a la legislación española de la directiva 40/2013 sobre ataques a los sistemas de información. Por una parte descubrimiento y revelación de secretos y por otra daños informáticos.

Esta reforma aparece reseñada ya en el Boletín Oficial del Estado del 31 de marzo de 2015.[229]

—Se tipifica —continúa la fiscal— una figura muy interesante: la elaboración, adquisición o puesta en circulación de herramientas e instrumentos que posibiliten la comisión de informáticos. Es adelantar la barrera de protección. En la directiva de la Unión Europea, se habla de los ataques masivos a través de redes de ordenadores infectados, como un riesgo muy serio, porque puede perjudicar de forma grave sistemas de informador muy sensible. Y en esos casos el legislador decide no esperar a que se produzca el ataque, sino criminaliza la conducta previa, porque es tan peligrosa, que merece la pena tipificar la fase preparatoria, en que se crea la red de ordenadores infectados. Y por eso se penalizan las herramientas que se utilizan para eso.

»En cuanto a los delitos de terrorismo se tipifica como delito, y es una figura compleja, el que con la finalidad de formarse, de capacitarse dice el código, accede de forma habitual a contenidos que incitan a la integración en grupos terroristas o la facilitación de sus actividades y fines. Y se agravan específicamente todos los delitos relacionados con el terrorismo, por ejemplo la humillación de las víctimas o la enaltecimiento del terrorismo a través de redes sociales.

Esta reforma también aparece reseñada ya en el Boletín Oficial del Estado del 31 de marzo de 2015.[230]

—Tan importante como definir adecuadamente los tipos penales es definir los mecanismos de investigación criminal. Por qué los delitos cometidos con estas herramientas —dijo la fiscal mientras levantaba su teléfono móvil— no se pueden investigar con las técnicas policiales tradicionales. Tenemos que usar las mismas que ellos. El problema es que tenemos una Ley de Enjuiciamiento Criminal del siglo XIX. Y otro problema aún más serio es que la investigación sobre sistemas y medios de

comunicación o de dispositivos de almacenamiento personal puede incidir sobre derechos fundamentales, como el derecho a la intimidad, al secreto de las comunicaciones, libertad de información, libertad de expresión, etcétera. Tenemos que ser eficaces en la lucha contra el ciberdelito, pero no a cualquier precio. Por eso es tan importante que el legislador establezca unos mecanismos que nos permiten llegar al autor del delito, pero sin afectar las libertades de los ciudadanos.

»En cuanto a la necesaria reforma de la Ley de Enjuiciamiento Criminal —que en ese momento estaba en fase de enmiendas en el Parlamento—, las ideas esenciales son: un paquete de medidas sobre la interceptación de comunicaciones, recogiendo toda la doctrina del Tribunal Supremo, el Constitucional y el Tribunal Europeo de Derechos Humanos. Se regulan temas como la identificación de IP, el registro de sistemas informáticos, la figura del agente encubierto *online*, y el registro de dispositivos electrónicos de forma telemática, es decir, desde fuera y sin conocimiento del dueño. Esta medida ha generado mucha polémica porque es muy invasiva, por supuesto, pero está pensada para delitos gravísimos, como terrorismo o contra la seguridad del Estado, y siempre con un control judicial permanente, pleno y constante.

Estas reformas se veían venir. Y a pesar del exquisito tacto con el que Elvira Tejada enuncia la nueva situación legal del hacking, otros fiscales, como Jorge Bermúdez, matizan estas reformas.

Jorge Bermúdez es fiscal delegado de Delitos Informáticos en Guipúzcoa y, desde octubre de 2007, miembro del Servicio de Criminalidad Informática de la Fiscalía General del Estado. Pero también es un miembro más de la comunidad. Sus charlas, en diferentes CON, planteando el hacking desde el punto de vista de la ley son tan divertidas y didácticas como formativas.

Bermúdez, que se mueve a medio camino entre la judicatura y la comunidad, ha criticado durante años algunas de las leyes dictadas en España. Dictadas por políticos.

«… como el artículo 197/3 del Código Penal, tristemente célebre para la comunidad hacker, porque se conoce como el tipo penal que criminalizaba el hacker ético. Porque en 2001, en Budapest, España suscribió el Convenio de Lucha contra la Cibercriminalidad. Sin embargo, nuestro Código Penal no recogía los principios de ese convenio, porque decía que había que proteger las intrusiones en los sistemas informáticos, independientemente de cuál fuera la intención de esas intrusiones…» Aunque la frase es original del abogado Carlos Sánchez Almeida, conocido por haber defendido a muchos hackers, Jorge Bermúdez está asociado por toda la comunidad a la expresión «hackear la ley».

Un ejemplo de ese hackeo de la ley es el uso de los artículos 1.888 a 1.894, vigentes en el Código Civil desde finales del siglo XIX, donde se menciona el «cuasicontrato de gestión de negocios ajenos», como una herramienta legal válida para justificar la intromisión en un sistema informático del siglo XXI, cuando la intención es lícita y no existe dolo.

—Imaginemos que estamos en nuestro domicilio, en un bloque de pisos de cualquier ciudad. De repente, una mancha de humedad aparece en el techo, y al poco comienza a gotear. El vecino del piso superior se ha ido de vacaciones al extranjero, está ilocalizable y tiene un escape de agua. ¿Qué hacer? En teoría, si entramos en su domicilio, estamos cometiendo un allanamiento de morada. Pero no es así, ya que no buscamos un fin ilegítimo, y tenemos una ley que nos ampara: el cuasicontrato de gestión de negocios ajenos nos autoriza, por ejemplo, a llamar a un cerrajero y a un fontanero, entrar en el piso afectado por el escape de agua, hacer que lo arreglen, y no solo no ser acusados de nada, sino que le podemos pasar la factura al propietario. Pues bien, hoy en día, una vulnerabilidad en un sistema informático es al menos tan potencialmente dañina como un escape de agua. Así que la aplicación mesurada del cuasicontrato de gestión de negocios ajenos nos puede permitir separar el grano de la paja, y dejar a los expertos en seguridad informática fuera del campo de acción de esta contundente norma penal que es el nuevo párrafo tercero del artículo 197 del Código Penal.

En 2011, Bermúdez desarrolló el caso en un memorable artículo titulado «Steampunk: el siglo XIX acude al rescate de los hackers», publicado en el blog de referencia Security by Default.[231] A este tipo de cosas se referían César Lorenzana o Román Ramírez cuando dicen que Bermúdez puede «hackear la ley».

Precisamente por su activa participación en la comunidad, quizá la percepción que tiene Bermúdez sobre los ciberdelitos es diferente a la de la mayoría de sus colegas. De hecho, ha recurrido en alguna ocasión sentencias absolutorias, por ejemplo en el caso de las mulas de *phishing*, por entender que la poca familiaridad de los juristas con las nuevas tecnologías en muchas ocasiones redunda en contra de la justicia.

En la RootedCON de 2014 Bermúdez pronunció una conferencia titulada «Los hackers son de Marte, los jueces son de Venus», que expresa perfectamente la percepción que los dos actores de este drama tienen de un mismo fenómeno… la red.

Zero Day

A medida que se acercaba el 1 de julio de 2015, fecha en que oficialmente entraría en vigor el nuevo Código Penal, las conversaciones entre los hackers parecían dejar de ser tan técnicas, para concentrarse en el futuro incierto que los aguardaba a partir de ese día cero. El Zero Day de la nueva ley.

En esos meses yo viví uno de los momentos más desagradable de toda la investigación. Pillé a la Providencia desprevenida el día que intenté contratar a un miserable *blackhat* como profesor de hacking particular. La última vez que lo vi fue el día que pagué por adelantado el curso. No dedicaré más de un párrafo «al miserable», porque fue la excepción que confirma la regla. Toda la comunidad, absolutamente toda, se posicionó de mi lado. La BIT del CNP y el GDI de la Guardia Civil fueron informados y la amenaza neutralizada. Es el único garbanzo negro que yo encontré entre los hackers. Y además, me sirvió para conocer a otros investigadores estupendos. Como el abogado sevillano Luis Jurado.

Se había enterado de la historia a través de David, el policía de la BIT, y se puso en contacto conmigo para ofrecerse a mediar. Ni siquiera tuve que buscarlo yo. En mi caso, él no podía aportar nada que no se hubiese ocupado ya de solventar la comunidad, utilizando sus propias reglas, pero cuando supe que era el abogado que llevaba el caso de Hache, y que estaba especializado en delitos informáticos, sí tuve mucho interés en conocerlo.

Tenía que desplazarse a Madrid unos días más tarde para atender a unos clientes, y acordamos reunirnos allí. En la estación de Atocha. No muy lejos de donde cambió mi vida el 11 de marzo de 2004, tres días después de la publicación de *El año que trafiqué con mujeres*. De hecho, intencionadamente acudí a la estación de Atocha antes de la hora. Quería pasarme unos minutos por la sala subterránea situada bajo el monumento a las víctimas del 11-M.

Siempre me impresionó ese lugar. Allí están los nombres de todas las víctimas del atentado más brutal de la historia de Europa. Y mensajes por la paz en todas las lenguas del mundo. También en árabe. Con más razón en árabe… El saludo en árabe, *as-salām'alaykum* (عليكم السلام)significa «que la paz esté contigo». Identificar a toda una raza con las miserias de unos terroristas es tan injusto como identificarlos con toda una religión.[232]

Tras unos minutos en aquella sala volví al vestíbulo y busqué una cafetería que me ofreciese cierta confianza. Escogí la mesa más alejada, en un rincón, de cara a la entrada, y envié un sms al abogado señalando dónde le esperaba.

No solo su aspecto, impecable, elegante, recordaba la flema británica. También su puntualidad. Luis Jurado Cano es un nativo digital. Nació, creció y se formó rodeado de tecnología. Quizá por esa razón, cuando en 2014 se licenció en Derecho en la Universidad de Sevilla, decidió hacerse penalista y especializarse en la criminalidad

tecnológica. Tal vez fue por eso, o porque antes incluso de terminar la carrera, ya era un nombre conocido en la comunidad. Participando en CON tan prestigiosas como Navaja Negra o Sh3llcon, con charlas sobre los aspectos legales del hacking. Todo ello sin descuidar su trabajo como voluntario en la ONG Solidarios para el Desarrollo, y como socio del bufete sevillano Perseus Legal Corporation.[233]

Cuando nos conocimos estaba preparando su migración a La Coruña, por cuestiones personales. Pero desde Galicia, con nueva oficina de Perseus, continuaría ejerciendo el Derecho, y participando en eventos de seguridad informática. De hecho, ya estaba preparando su conferencia para la edición 2015 de Navaja Negra en Albacete.

En cuanto entró en la cafetería lo reconocí por su foto en Linkedin. Le hice una señal y nos estrechamos la mano.

—La reforma del Código Penal del próximo 1 de julio de 2015, ¿en qué afecta a nuestra seguridad informática?

—Me gusta mucho esta pregunta porque es precisamente de lo que va mi próxima charla en Navaja Negra. La reforma del Código Penal es tan brutal que sus dimensiones hoy son difíciles de predecir. Hay que tener en cuenta que va unida a un paquete más amplio de reformas, a lo que se suma la reforma de la Ley de Enjuiciamiento Criminal que entra en vigor el 28 de octubre de 2015, después de 132 años. Y la tan «afamada» Ley Orgánica 4/2015, conocida como Ley Mordaza. Estas reformas son complejas, estando siempre sujetas a interpretación y cambios en la respuesta doctrinal que hay que aplicar al caso concreto, dependiendo del momento procesal en el que nos hallemos. En lo referente al Código Penal nuevo, hay varios artículos interesantes que a mí particularmente me llaman la atención. Por citar uno que afecte a expertos en seguridad informática, el artículo 197.6 CP dice que en el peor de los casos una persona encargada o responsable de ficheros o soportes informáticos que tenga la feliz idea de vender datos reservados de personas que revelen su ideología, origen racial o salud, por ejemplo, le puedan caer siete años de prisión. Eso bajo mi punto de vista es un desatino, que espero que mediante jurisprudencia se vaya corrigiendo.

—¿Por qué es un desatino? Si alguien reserva datos personales de otra persona, parece claro el dolo, ¿no?

—Un delito es un acto típico, antijurídico y culpable, eso es lo que nos dice la teoría jurídica del delito. Pero no me refería a eso, sino a que en este caso en concreto la pena con la que se grava esa «acción dañina», por así llamarlo, es a priori desproporcionada si la comparamos con delitos de sangre. O sin ir más lejos con delitos societarios o relacionados con los mercados, donde el beneficio obtenido y la cantidad de afectados puede ser cuantioso. Personalmente creo que siete años de vida en prisión no es ninguna broma, por eso soy partidario de la expresión latina *in dubio pro reo* (ante la duda, a favor el acusado).

El camarero nos interrumpió para tomar nota del pedido. Dos cafés, un zumo de

naranja, unos bollos… Continuamos.

—Gracias por la aclaración. Volviendo al Código Penal…

—Si seguimos avanzando en la lectura del Código Penal, en el artículo 264.2.4 CP se habla de infraestructuras críticas del Estado o de la Unión Europea y de que si las atacas mediante un sistema informático, puedes ser penado entre dos y cinco años y su correspondiente multa por valor de diez veces del daño ocasionado, casi nada. Un ejemplo teórico podría ser un DDoS —ataque de denegación de servicios— contra los servidores de la Agencia Tributaria o el borrado de los mismos. Hay que aclarar que un hacker ético siempre actúa dentro de la legalidad y eso incluye tener el consentimiento previo del cliente que quiere auditar sus sistemas. Por eso aunque hay varios preceptos del Código Penal que si bien penan de forma contundente a quienes no tienen el consentimiento del cliente para penetrar en su sistema, premian a quienes sí lo tienen, como los consultores de seguridad por ejemplo, que evalúan la seguridad de la empresa intentando vulnerarla. El legislador intenta de esta forma paternalista polarizar entre hackers buenos, que sí tienen el consentimiento, y cibercriminales malos que no lo tienen. Los problemas llegan cuando no todo está tan claro.

Cada día, 1,5 millones de personas se convierten en víctimas de delitos cibernéticos. Pero el cibercrimen es solo una de las facetas legales de las amenazas que suponen las nuevas tecnologías a nuestra vida. Hay otras.

—Creo que unos colegas tuyos fueron los impulsores del derecho al olvido en internet…

—Exactamente. Fueron Pablo F. Burgueño y Joaquín Muñoz de Abanlex. Ellos fueron los pioneros contra las políticas abusivas de Google y su inoperancia a la hora de querer ser borrados por diversos motivos de su motor de búsqueda. Todo el mérito es suyo.

—¿Y es real? Quiero decir, durante el Celebgate miles de fotos íntimas de famosas fueron subidas a la red, y aunque denunciaron y ganaron, las fotos continúan circulando por internet. Yo, que soy un usuario bastante torpe, las he encontrado, y si las encuentro yo, cualquiera puede. ¿Realmente se puede ejercer ese «derecho al olvido» en la red, o todo lo que sube se queda ahí de una u otra manera?

—El derecho al olvido en internet de forma absoluta en muchos casos no existe, eso es algo utópico. Cualquier usuario deja rastro, lo sepa o no. Pero con esta herramienta legal de que ahora disponemos, gracias a los compañeros, se puede mitigar de forma medianamente controlada los efectos no deseados de nuestro paso por internet.

Un buen ejemplo de que ese éxito es relativo son las fotografías del Celebgate o los *fakes* de Pilar Rubio. Incluso con una denuncia interpuesta y con una sentencia condenatoria, incluso aunque el proveedor, de buena fe, borre esos contenidos de sus servidores, miles de internautas los habían grabado ya y volverían a subirlos a la red una y otra vez. Como si una orden judicial prohibiese a una naviera faenar en el océano con unas redes de malla ilegal, que capturan a las crías de los peces, afectando

a la continuidad de los bancos, en lugar de atrapar solo a los ejemplares adultos… Es posible que esa naviera obedezca la orden judicial y deje de utilizar esas redes. Pero en la inmensidad del océano, miles de navieras y pescadores particulares continuarán empleando esa técnica, porque no existe ningún juez marítimo que pueda controlar todos los mares del planeta. Y la red es un océano mucho mayor.

Si subes algo a internet, ten por seguro que ningún juez podrá garantizar tu derecho al olvido.

—Durante los últimos años me he encontrado muchas referencias al caso de Hache y su detención, en diferentes entornos de la comunidad. Es tu cliente, ¿no? ¿Qué pasó?

—Lo siento, de mis clientes no puedo comentar nada. Solo decir que confío plenamente en su inocencia; si no, no hubiese aceptado ese asunto.

Entendí perfectamente el argumento del abogado, pero insistí. Era mi obligación como periodista. Y él insistió en no decirme ni una palabra. Era su obligación. Así que nos pedimos otra ronda, y yo continué insistiendo. Luis es un tipo responsable, y no conseguí sacarle ni un miserable dato, pero, ante mi insistencia, se brindó a hacer una cosa por mí… Llamar a su cliente y consultarle directamente si quería hablar conmigo.

—Genial, muchísimas gracias. ¿Y podría ser ahora mismo? Por favor…

Luis sonrió y encogió los hombros con resignación. Se había dado cuenta de que puedo ser un tocanarices insoportable inasequible al desaliento, y no atentaba contra ningún secreto profesional que telefonease a su cliente para consultarle si quería hablar con un periodista. Así que sacó su móvil y buscó en la agenda.

Sé que no está bien escuchar conversaciones ajenas, pero estábamos compartiendo mesa en una cafetería de Atocha, y yo estaba realmente interesado, así que me esforcé por convertir mis orejas en parabólicas, como si se tratase de las antenas de Lord Epsylon intentando interceptar la señal de los satélites…

Luis y su cliente conversaron unos minutos. Hache había quedado muy tocado con su experiencia en los calabozos y no quería remover el tema. Ni siquiera para contar su versión. Lo único peor que ser acusado de un delito de pedofilia es ser acusado injustamente de un delito de pedofilia. Luis disculpó a su cliente y me pidió comprensión. La tuve. Y continuamos charlando sobre otros aspectos legales del hacking. Poco después, rastreando la hemeroteca, descubrí una entrevista, creo que la única, donde Hache relataba el infierno que vivió durante su detención. Si sabes buscar, todo está en la red.

«Yo odio a los pedófilos y lo único que quería era ayudar a desmantelar este tipo de páginas —decía Hache en la entrevista—. Ahora ya no se me vuelve a ocurrir hacer nada por nadie. Fue en noviembre [de 2012] cuando desarrollé un programa que rastreaba e indexaba esas web ocultas y lo tuve ejecutándose un par de meses, en los que obtuve más de 100.000 webs catalogadas por diferentes etiquetas para identificar el tipo de páginas que eran… Aparecieron multitud de páginas y foros de pederastas, incluso te encontrabas con mensajes de los administradores regocijándose porque llevaban x años *online* y nunca les había ocurrido nada… como si fuera una ciudad sin ley donde pueden campar a sus anchas…» Dos meses más tarde, siete agentes de la Policía Judicial le esperaban en el garaje de su domicilio con una orden de registro en la mano prestos a realizar la detención.[234]

—Cuando empecé esta investigación —le dije a Luis retomando la entrevista en otro punto—, creía que un hacker era un pirata informático, un delincuente. En la red encuentro, sin buscar demasiado, anuncios de personas que se ofrecen para hackear sistemas, robar contraseñas, etcétera, y anuncios de personas que buscan a esos hackers… ¿Todo esto es legal?

—No es legal, pero eso no quita que no sea posible con cierta facilidad acceder a ese tipo de servicios. Debemos comprender que siempre habrá gente que quiera acceder a esos servicios y gente que se los proporcionará. Dicha actividad llevará de la mano una problemática asociada. Y yo, como abogado, lo único que puedo hacer es trabajar para que el cliente que se ve envuelto en tal torbellino de problemas salga lo mejor parado respecto de su situación inicial.

—*Grooming, bullying, sexting…* ¿En la facultad os han preparado para enfrentaros a estos nuevos tipos de criminalidad?

—En la Facultad de Derecho de Sevilla en la que estudié, aprendí buena parte del amor por la investigación y querer ir más allá de los conocimientos de los que se examinaban. En las distintas asignaturas de Derecho Penal que cursé, se hablaba en

primer lugar de las distintas teorías que subyacen bajo el sistema penal español y luego de los distintos tipos (artículos) que hay en el Código Penal. El *grooming, bullying, sexting* son variantes de tipos penales que se conocen desde antiguo. La maldad humana viene siendo la misma; la única diferencia es que encuentra nuevas vías de expresión; en este caso a través de medios telemáticos. Adaptarse a estas nuevas formas de expresión de la maldad requiere de una formación continua tanto para los abogados como para jueces, fiscales y demás miembros relacionados con la justicia. Habría que hacer una labor de indagación profunda desde todas las piezas de ese puzle que compone dicha problemática, para proteger de un lado a los afectados y de otro salvaguardar los derechos de las personas que estén siendo objeto de investigación.

El camarero volvió a interrumpirnos para traernos los desayunos. Luis instintivamente dejó de hablar. Los dos nos quedamos en silencio mientras componía sobre la mesita de Atocha el *collage* de tazas, platos y cubiertos.

Entonces una escena llamó mi atención. A mi derecha, a solo un par de mesas de distancia, una familia desayunaba sin hablarse, supongo que mientras esperaban la salida de su tren. El padre leía absorto un periódico deportivo. La madre hablaba animadamente por teléfono. Y la hija, no tendría más de quince o dieciséis años, como Aranzazu, tecleaba compulsivamente en su móvil mientras su rostro cambiaba de expresión entre mensaje y mensaje. Obviamente estaba discutiendo con alguien a través del WhatsApp. Los tres configuraban un perfecto monumento al aislamiento. En la era de las telecomunicaciones estamos más solos que nunca.

Pero, de los tres, la pequeña era la más vulnerable. En el siglo XXI, una red social encierra más riesgos que una conversación telefónica o un periódico deportivo…

—Luis, hace poco Aranzazu, una joven de dieciséis años, se suicidaba tirándose por el hueco de la escalera después de sufrir acoso en su colegio y en sus redes sociales. ¿Realmente está habilitada la ley para enfrentarse a estos nuevos tipos de delito?

—La ley está habilitada, la que no está preparada en muchos casos es la escuela ni los profesores que ven de forma continua situaciones parecidas y no actúan de forma efectiva. Tampoco en la mayoría de los casos hay una conciencia entre los alumnos de que determinadas actitudes y actos pueden conducir a la víctima a un sufrimiento que le pueda hacer cometer algo irreversible como es quitarse la vida. Por eso creo que grandes iniciativas bajo mi punto de vista como X1Red+Segura o el programa Agente Tutor de la Guardia Civil (@GcTutor) son necesarias y deben ser potenciadas aún más si cabe en la sociedad que actualmente vivimos.

—¿Y cómo se ve desde el otro lado? Quiero decir, imagino que tú tendrás la obligación de defender a los *blackhats*, a quienes han decidido vivir del cibercrimen… ¿Cómo se ve el hacking desde ese lado de la ley?

—Hay que dejar claro que no tengo obligación de defender a todo tipo de personas, es el abogado quien elige al cliente, no al revés. Si no me siento cómodo,

no trabajo con ese cliente. Dicho esto, cada cliente es un mundo, y dentro del cibercrimen, como tú lo denominas, hay una variedad enorme de maneras de formar parte de él. Para la ley no hay cibercriminales, hay criminales a secas. Con las nuevas reformas acaecidas en estos años, ser un cibercriminal cada vez es más fácil. Hay conductas que antes no estaban tipificadas porque simplemente no existían, y que hoy en día se empiezan a regular de una manera un tanto caótica sin saber muy bien el legislador cómo llevarlo a cabo. La seguridad informática es un campo muy técnico que requiere de un estudio y una preparación continua, actualizándose diariamente. La ley sin embargo se elabora de una forma mucho más lenta y en la que intervienen muchas personas y poderes. Llegar a un punto en común es complejo y siempre hay daños colaterales. ¿Quiénes son los principales perjudicados? Los investigadores y auditores en seguridad informática que buscan en los fallos su modo de vida y que gracias a ellos hacen que estemos más seguros día tras día.

—Solo una pregunta más. Acabo de recibir un aviso de mi proveedor para actualizar una app en el móvil. En vez de darle a aceptar, aceptar, aceptar como he hecho siempre, he preferido leerme las condiciones… Joder, son ochenta y dos páginas de contrato… ¿Esto es legal? ¿Que las empresas después vendan nuestros datos a terceros para establecer nuestro perfil como compradores? ¿Las *cookies* que rastrean las páginas que visitamos en internet? ¿Todo esto es legal? ¿De verdad estamos tan desamparaos antes las grandes compañías que controlan la red?

—Se suele decir que cuando no pagas por un producto, el producto eres tú. Actualmente la regulación en materia de protección al usuario final es bastante tímida. Tenemos leyes como la LOPD y la LSSI que intentan regular un campo en continuo cambio, pero no hay que dejar de recordar que estamos en un mundo globalizado. Esto quiere decir, por ejemplo, que una aplicación rusa pueda utilizarse en España a los pocos minutos de su creación. O que un terminal móvil chino lo usamos como si se hubiese creado en Madrid. El precio de esta comodidad es tu privacidad y los datos que se pueden extraer que sirven para seguir retroalimentando a las grandes empresas. Una gran empresa no está atada a un territorio. Si las leyes de un país no son de su agrado, se marcha a otro donde sí lo sean. Como hay tantas leyes como países, y tantas interpretaciones de las mismas como personas, es un campo abonado para que cada uno haga lo más provechoso para sí mismo. ¿Qué podemos hacer? Pues actuar sobre nosotros mismos y si no estamos de acuerdo, no participar de la rueda corporativa. Algunos amigos hablan de irse al campo, aunque creo que eso lo dicen porque nunca han ido a vendimiar.

Falciani y el servicio secreto de Ada Colau y Manuela Carmena

Luis y yo pasamos un buen rato charlando sobre diferentes aspectos legales de la Seguridad Informática en aquella cafetería de Atocha. Pero el abogado resultó ser más paranoico aún que yo. Como Román, Lord Epsylon, Lucas, David, Israel y el resto de miembros de la comunidad, parece que la paranoia crece proporcionalmente a tu incursión en el mundo de la (in)seguridad informática.

—¿Te parece que nos movamos? —me dijo—, ya llevamos mucho rato aquí, y el tío que estaba en la mesa de atrás no me ha dado buena espina. Te juro que creía que era tu escolta…

Salimos de Atocha, cruzamos la plaza del Emperador Carlos y seguimos hasta el Museo de Arte Reina Sofía. Luis conocía la cafetería del museo y aseguraba que era un lugar discreto y tranquilo para continuar charlando… y tenía razón. Tuvo la amabilidad de ponerme en contacto con otros miembros de la comunidad, estableciendo él un primer contacto telefónico con ellos. Pero en medio de nuestra conversación recibí un mensaje que me hizo soltar una exclamación de sorpresa.

—Pero ¿qué ha pasado? —se sobresaltó—. ¿Estás bien?

—¿Bien? ¡Es Falciani! Está en Madrid y quiere verme.

—¿Falciani? ¿El que hackeó la banca suiza?

—Ese mismo. Lo siento muchísimo, Luis, estamos en contacto, pero ahora tengo que irme.

Me habría gustado disponer de más tiempo para continuar profundizando con Luis en los aspectos legales de la tecnología, pero me levanté de un salto y salí corriendo del Reina Sofía, dejando al abogado todavía perplejo.

Salté sobre la moto y salí a toda velocidad, esquivando el maldito tráfico de Madrid, zigzagueando entre los coches, mientras intentaba adivinar qué se ocultaba tras el mensaje del informático que había hackeado la banca.

La verdad es que no esperaba volver a tener noticias de Hervé Falciani. Nuestro primer encuentro había sido estupendo, y el hecho de que conociese mi trabajo y la amable dedicatoria que me obsequió en su libro me hicieron albergar ciertas esperanzas un tiempo. Pero Falciani se enfrenta a enemigos gigantescos y su agenda es endiablada. Sinceramente, creía que se había olvidado de mí, y lo comprendía.

Así que lo había intentado por mi cuenta. Tras probar suerte en la embajada de Rusia en Madrid, tras haber conseguido el mail de su abogado en Moscú a través de una amiga que en su día colaboró con los servicios soviéticos, y tras intentarlo también a través de Glenn Greenwald, Falciani parecía mi última baza para tratar de reunirme con Edward Snowden en Rusia, pero no podía obligar a Hervé a invertir su tiempo en hacer esa gestión.

Ahora, aquel mensaje que había interrumpido mi reunión con Luis Jurado me

devolvía la esperanza.

Cuando llegué al lugar donde me había citado, Falciani me esperaba sonriente en la puerta. Aparqué sobre la acera, y me reuní con él. Un abrazo sincero y entramos juntos, buscamos una mesa que a ambos, profundamente paranoicos, nos pareciese segura. Y pujamos por ver quién se sentaba de espaldas a la pared, para tener una mejor perspectiva de la entrada al local. Gané yo.

Por desgracia, las noticias eran malas. Según me explicó, se había puesto en contacto con el abogado de Snowden para plantearle la posibilidad de que un periodista español se reuniese con él en Moscú. Pero mi propuesta no podía llegar en peor momento. Al parecer justo en esos mismos instantes los abogados de Snowden estaban reunidos en Senegal con la NSA, intentando negociar el regreso del filtrador a los Estados Unidos con una pena de cárcel mínima. Imposible que Snowden se reuniese con ningún periodista. La NSA no quería que hiciese más ruido, y sus abogados tampoco… No tengo forma de contrastar esta información, pero así es como me lo relató Falciani. Supongo que no llegaron a un acuerdo, porque a la hora de escribir estas líneas Snowden sigue en Rusia. En septiembre inauguró su cuenta personal en Twitter: *@Snowden* que en 24 horas alcanzó un millón de seguidores,y yo sigo intentando llegar a él…

Sin embargo, la mayor sorpresa estaba por venir. Porque ahora era el informático quien quería algo de mí.

No era ningún secreto la excelente relación que mantenía con Podemos, la formación liderada por Pablo Iglesias, y con el Partido X. Él mismo lo relata así:

> El 10 de febrero de 2015 tuve un primer contacto con el secretario general de Podemos, Pablo Iglesias. Estuvimos hablando por videoconferencia sobre la forma en que yo podía poner mis conocimientos a disposición de su movimiento. Encima de la mesa hay distintas propuestas que esperamos aplicar durante los primeros 100 días de Gobierno en caso de que Podemos consiga la victoria en las próximas elecciones generales. Se está hablando de medidas que contemplan el uso de sistemas de control para vigilar a quienes desempeñen cargos públicos o de poder, no a las personas corrientes.[235]

Pues bien, de eso quería hablar conmigo Falciani.

Al parecer, y para mi sorpresa, Hervé Falciani ya estaba colaborando con los ayuntamientos de Madrid y de Barcelona en la creación de una especie de servicio de Información ciudadana. Un concepto que yo hasta entonces solo había escuchado en Cuba y Venezuela.

Según me relató Falciani, inmediatamente después de ganar las elecciones municipales, el mes de mayo anterior, Manuela Carmena y Ada Colau se habían puesto manos a la obra para intentar llevar a la práctica esos «sistemas de control a quienes desempeñen cargos públicos» de los que había hablado con Pablo Iglesias.

El informático, que conocía mi trayectoria, sabía que por mis diferentes investigaciones había coincidido, y con frecuencia competido, con funcionarios de diferentes servicios de Información internacionales durante el trabajo sobre el terreno. Y mostró interés por algunos de ellos. Como David R. Vidal, alias el «agente Juan».

Yo me desmarqué del proyecto. No me sentiría cómodo trabajando para ningún servicio de Información, ni siquiera uno «ciudadano», pero me comprometí a transmitir su interés a David Vidal, que ya es mayorcito, para que él decidiese por sí mismo.

Lo que ocurrió en las semanas posteriores volvió a evidenciar, en mi experiencia personal, la sucia guerra por el poder que se libra en los mentideros políticos, con la colaboración de la prensa de uno y otro bando. Transmití a David el interés de Falciani por contactar con él, y le facilité la dirección de correo electrónico que me pasó. Y ahí terminó mi cometido. David continuaba encerrado en su batcueva trabajando en el programa Globalchase ORAK, su ambiciosa Plataforma de Análisis de Inteligencia e Investigación de Futuros, y no mostró un excesivo interés por el proyecto de Falciani. Sé por él que tardó varias semanas en escribirle.

El lunes 13 de julio se me indigestó la tostada del desayuno cuando me encontré, en la primera página del diario *La Razón*, el siguiente titular: Ada Colau prepara un «servicio de Inteligencia» con Falciani.[236]

Que una información tan supuestamente sensible hubiese llegado a la portada de *La Razón* resultaba de por sí llamativo. Pero lo que me resultó de veras desconcertante es que en el extenso artículo, que firmaba J. M. Zuloaga, solo se mencionaba el nombre de uno de los supuestos colaboradores de Falciani en el «servicio secreto» de Ada Colau: mi amigo el «agente Juan».

Llamé a David inmediatamente para saber si era él quien había filtrado a *La Razón* la historia del servicio de Información ciudadano de Falciani. David me aseguró que de ninguna de las maneras. Y yo le creo. Lo conozco como si le hubiese parido, y David R. Vidal no pierde el tiempo jamás. Es el pragmatismo y el sentido práctico hecho carne. «Yo gano siempre», recuerdo que me dijo al poco de conocerlo. Y con aquella filtración no ganaba nada. Al contrario. Si el texto de Zuloaga no intentase ningunear las capacidades de Vidal, como si fuese un desconocido, podría sospechar otra cosa. Pero el periodista obviaba que tras la publicación de su libro *Diario de un espía*, cuya publicación omitía intencionadamente, Vidal se había convertido en un personaje muy mediático en España. Y cada vez que una cadena de televisión quería la opinión de un «espía» sobre un tema de actualidad, acudía a él. No, aquello olía realmente mal.

Lo más sorprendente de todo es que el «agente Juan» me asegura que después de meses concentrado en su plataforma, por fin había escrito a Falciani el viernes anterior, 10 de julio. Es decir, solo tres días antes de la publicación de la noticia. ¿Cómo es posible que en el transcurso de esas cuarenta y ocho horas del fin de semana *La Razón* hubiese vinculado a David R. Vidal con Falciani? Sobre todo porque Falciani nunca llegó a responder al email del «agente Juan». Imagino que pensaría que la filtración había venido de él. Yo sospecho que, en este caso, el filtrador está más cerca del Ayuntamiento de Barcelona o del mismo Falciani…

Porque si alguien se ha beneficiado de las vulnerabilidades de internet, son los

espías. Como David Vidal.

Aquí, portada de *La Razón*:

JUNIO DE 2015
MARKOS NO ES JORDI

«De la dignidad al ridículo hay solo un paso.»

Adolf Hitler, citado por su secretaria Christa Schroeder en sus memorias

Habíamos avanzado mucho. Muchísimo. Ya sabíamos quién no era MarkoSS88.

Sabíamos que no era Marcos A., el ultra del Hogar Social de Madrid, ni Marcos N., el guardia civil. Instituciones Penitenciarias y el Grupo de Homicidios de la Policía nos demostraron que MarkoSS88 no había matado a ningún latin king y que jamás había estado en prisión. Habíamos descubierto que no era el chico de las fotos de su perfil, y que sus amigos, su exnovia Silvia y todas y cada una de las personas que decían conocerlo personalmente eran perfiles falsos en internet que gestionaba el mismo MarkoSS88 con las vidas digitales robadas a otros usuarios. Y tampoco era el autor de ningún libro sobre nacionalsocialismo, simplemente había robado el texto de *Nacionalsocialismo: Historia y Mitos,* uno de los publicados por Ignacio Ondargáin, que el autor había subido íntegro a su web, Markos le cambió la portada y el título y puso su nombre como autor.

La campaña de apoyo en Change la había montado él mismo utilizando docenas de falsas identidades en internet para las primeras firmas de apoyo, o para referenciarlas en blogs, como Grande y Libre, que también fabricó él, y que desapareció tras haber cumplido su función: hacer creer a todos que Markos era real.

En el colmo del cinismo, Markos estaba tan seguro de que su tapadera en la red era inexpugnable, que se permitía la ironía. Cuando un tal Nicolás preguntó al perfil de Silvia Hierro en Ask «¿Qué nombre le pondrías a tu hijo o hija?», respondió «Si es chica, Sara». Macabro sentido del humor. Porque Markos, travestido de su novia Silvia Hierro, había hecho exactamente eso… había hurtado la vida de una pareja que a esas alturas ni se lo imaginaba.

Ahora solo faltaba saber quién era realmente.

Pasaron semanas hasta que por fin un amigo de un amigo nos llamó con buenas nuevas sobre el segundo teléfono que me había facilitado Markos. ¡Aleluya!

Avisé a todos.

—Creo que ya lo tenemos. Un amigo de un amigo mío trabajó en la

compañía y todavía tiene contactos allí. Me ha dicho que le han pasado el titular del teléfono. Me lo está enviando ahora por email…

Expectantes, los policías aguardaron a que abriese el correo. Pero mi cara de decepción habló antes que mis labios.

—Este cabrón es un puto genio… No hay manera.

El segundo teléfono de Markos era un número institucional. Es decir, pertenecía a una gran multinacional de la energía. Quizá la más importante del país.

—Os lo dije —apuntó Rafa—. Este tío no es un chavalito, es un tipo hecho y derecho y muy astuto. Esto es otro cortafuegos. Como lo de FonYou. Toni, olvídate, nunca vas a llegar a él. No vale la pena perder más tiempo.

—Ni de coña —respondí molesto de verdad—. Esto no es solo por mí. Se ha burlado de Marga, de Stefy, de Soraya, de todos los que nos preocupamos por él sinceramente. Pero sobre todo de Soraya, y vete tú a saber de cuántas chicas más. Deberías ver los mensajes que le deja en Facebook, joder, está totalmente enamorada de un fraude. Y si no lo desenmascaramos nosotros, ¿quién lo hará?

—Pero ¿cómo pretendes averiguar quién es? —apuntó con mucho acierto otro de los CNP del grupo—. Es un teléfono de empresa. Es como si yo te doy mi número de móvil del curro. Suponiendo que pudieses llegar a averiguar quién es el propietario, te saldría que es el Cuerpo Nacional de Policía. Y se acabó. O tienes a alguien en la administración de la Policía, o nadie te dirá que ese número de teléfono está derivado a mí…

—Claro, joder, eres un genio… Solo necesitamos a alguien dentro de esa multinacional y ya lo tenemos.

Capítulo 22
Juegos de espías

«El supremo arte de la guerra es someter al enemigo sin luchar.»

Sun Tzu

De Stuxnet al Hacking Team

Dos años después de la visita a su batcueva, con la que se inició este viaje, las cosas no habían cambiado mucho. Salvo por el hecho de que, tras la publicación de su libro *Diario de un espía*, el «agente Juan» se había convertido en un personaje mediático.

Durante 2014 y 2015 David visitó todos los platós de televisión del país. La actualidad mandaba. Desde el *affaire* del «Pequeño Nicolás» al crimen de Asunta Basterra, pasando por la inmigración ilegal o las revelaciones de Snowden. En su página web todavía pueden verse muchas de esas intervenciones televisivas.[237]

Ahora era yo quien quería su opinión sobre los últimos escándalos relacionados con el mundo del hacking que habían surgido desde mi visita a su base de operaciones, dos años antes.

David R. Vidal aún seguía enfrascado en la programación de GlobalChase ORAK, la herramienta de inteligencia y análisis de futuros en la que estaba trabajando. Nadie dijo que la programación fuese una tarea sencilla. Y que dos años después, el agente Juan todavía no hubiese terminado su última obra informática, ilustra perfectamente la complejidad y el tiempo que requiere.

Este verano Wikileaks continuó aireando las miserias de los servicios de Inteligencia. Desde su «prisión», en la embajada de Ecuador en Londres, y a punto de perder la cordura por casi tres años de encierro, Julian Assange mantiene su pulso contra la CIA publicando informaciones que, de ser veraces, ponen en muy mal lugar a las agencias de Inteligencia norteamericanas. Aunque los medios de comunicación ya apenas le presten atención. La última, los cables que parecen sugerir la implicación de los intereses norteamericanos en la creación del conflicto sirio…[238] Un asunto realmente sucio.

Sin embargo, el gran escándalo internacional en el mundo del hacking se había producido un par de meses antes. Cuando la empresa italiana Hacking Team recibió el golpe más duro de su historia. 400 Gb de datos internos de Hacking Teamhabían sido robados de sus servidores y publicados en un archivo.torrent que cualquiera puede descargar y husmear. Wikileaks publicó un directorio de un millón de emails recibidos y enviados por Hacking Team, organizados con un buscador interno, para facilitar la localización de cada correo. La compañía italiana ofrecía sus servicios a gobiernos y agencias de todo el mundo en tareas de vigilancia, espionaje y control de objetivos.[239]

Sin embargo, un nuevo grupo de hackers ucranianos pretendía revolucionar los medios en julio de 2015.

El grupo CiberBerkut habría surgido tras la disolución del Berkut, una unidad especial de la Policía, tras las revueltas de Ucrania en 2014. En realidad, el Berkut pertenecía a la *militsiya*, algo más que un servicio policial. La *militsiya* tiene su origen en un servicio de orden instaurado por los bolcheviques para la «auto-

organización» del pueblo, diferenciándolo de la «Policía protectora de la clase burguesa». Y durante años este servicio existía en la mayoría de los países del Pacto de Varsovia.

Pues bien, tras la disolución del Berkut surgió un grupo de hackers que adoptó su nombre, y sus símbolos, pretendiendo continuar en el ciberespacio las actividades de vigilancia y control de la antigua división de la *militsiya* en Ucrania. Su página web[240]aspiraba a convertirse en el Wikileaks del Este.

Yo no había oído hablar de ellos anteriormente, pero investigando un poco pude rastrear sus ataques, documentados en medios de comunicación reales, al menos desde enero de 2015. Y esto es importante porque significa que tanto si son hacktivistas genuinos, como una campaña de desinformación, estaban preparando la gran revelación desde principios de año.

En enero CiberBerkut ataca los ordenadores del Bundestag y la Cancillería alemana.[241] En febrero y marzo dirigieron varios ataques DDoS contra sitios web de la OTAN.[242] En marzo filtraron conversaciones privadas del exprimer ministro de Ucrania y líder del partido Batkivschyna, Yulia Tymoshenko.[243] En mayo anunciaron la destrucción del sistema informático electoral ucraniano.[244] Existen muchos más ejemplos de ataques atribuidos a CiberBerkut reflejados en la prensa ucraniana e internacional, pero fue en julio de 2015 cuando soltaron la gran bomba.

En junio, una delegación senatorial norteamericana, encabezada por el candidato republicano a la presidencia de los Estados Unidos, el senador John McCain, visitó Ucrania para reunirse en Kiev con el presidente Petró Poroshenko. Unos días más tarde, el sábado 11 de julio, CiberBerkut subía a su web una nueva filtración. La más escandalosa de todas las publicadas hasta la fecha.

CiberBerkut aseguraba que habían conseguido hackear el teléfono móvil de uno de los congresistas que acompañaban a McCain y se habían llevado toda la información que habían encontrado. Entre otros, un vídeo en el que se demostraría, según ellos, que las decapitaciones del Ejército Islámico estaban rodadas en un plató de cine…

En el vídeo, profundamente desestabilizador, se distingue con claridad a nueve personas en un estudio de grabación. Además de los cámaras, técnicos de sonido y un director, aparece un set de rodaje en el que un supuesto terrorista del ISIS ensaya la decapitación de un hombre arrodillado ante él, vestido con un mono naranja.

Los hackers de CiberBerkut dejaron un mensaje en su comunicado al candidato republicano a la Casa Blanca: «Estimado senador McCain, le recomendamos que la próxima vez se abstenga de llevar documentos confidenciales en sus viajes al extranjero, ¡sobre todo al territorio de Ucrania!».

Es imposible saber, al menos para mí es imposible, si el vídeo es un documento genuino que los hackers realmente encontraron en el teléfono de un congresista norteamericano, o si se trata de una operación de Inteligencia rusa para menoscabar la credibilidad de los norteamericanos o sembrar dudas en cuanto a su relación con el

ISIS. Supongo que solo las nueve personas que aparecen en el vídeo podrían responder a eso. Pero resultó extraño que, pese a la aparente espectacularidad de la filtración, casi ningún medio se hiciese eco.

En España, la agencia prorrusa RT,[245] cuya objetividad periodística algunos (no es mi caso) tratan de cuestionar, publicó el vídeo de CiberBerkut. También *Periodista Digital* se hizo eco.[246] El resto… silencio.

Si la intención de CiberBerkut al publicar ese vídeo era que nos cuestionásemos toda la información que se publica en los medios occidentales sobre el Estado Islámico, no lo consiguió. Algunos ya nos la cuestionábamos antes.

—¿Qué te parece? —le pregunté a David tras mostrarle el vídeo de CiberBerkut —. ¿Le das crédito?

—El mismo que a la teoría conspiranoide de que el hombre nunca fue a la luna, que todo era un montaje de plató, con la diferencia de que es muy triste frivolizar con las ejecuciones del ISIS y una absoluta falta de respeto hacia las víctimas. El problema no es si un congresista llevaba o no el vídeo, que no tengo ni idea y lo considero irrelevante, sino la retorcida lectura que se pretendía extraer de ello. En cualquier caso, yo no lo daría mucha importancia a estos grupos de hackers o como quieras denominarlos, que aparecen y desaparecen, ávidos de notoriedad. Digamos que por sus objetivos los conoceréis, es decir, puedes intuir quiénes son, qué es lo que buscan y quiénes los apoyan. Al fin y al cabo, la propaganda no es algo precisamente nuevo. Los peligrosos de verdad no son los que quieren destacar sino los que actúan de manera sigilosa y son destructivos.

—¿Y Hacking Team? La información que ha publicado Wikileaks demuestra que vendían ciberarmas (herramientas) o al menos estaban en negociaciones para ello, al CNP, los Mossos d'Escuadra, el CNI… ¿Cómo es posible?

—Verás, estoy seguro de que nadie se sorprenderá si digo que los vehículos que conducen a diario los espías no los fabrican ellos sino más bien la industria del automóvil. Vamos, que el Aston Martin de James Bond, no lo construía el MI6 precisamente, aunque el sempiterno Q le añadía algunos gadgets divertidos. Pues bien, lo mismo ocurre con los programas. Es muy poco práctico que un servicio de Inteligencia o policial desarrolle la totalidad de su software, sobre todo en un nicho tan complejo y específico como son las herramientas para interceptar datos o introducirse en ordenadores ajenos. Es mucho más práctico encargar fuera herramientas o módulos para realizar tareas específicas y luego ensamblarlos y llevarlos a la práctica para unos objetivos que obviamente no se divulgan.

»Imagina, Toni, que necesitas sabotear una centrifugadora que produce uranio. Necesitas considerar muchos aspectos: cómo infiltrar el programita en el portátil de alguien, cómo atacar desde ese portátil a un servidor, cómo alterar el funcionamiento del servidor, cómo distribuir y replicar el programa malicioso hasta llegar al ordenador objetivo, cómo deshabilitar las alertas y, finalmente, cómo alterar la centrifugadora para que rompa tras unas semanas. En fin, que puede haber… no sé,

tal vez cien o doscientas tareas que realizar. Algunas no son del todo informáticas: necesitas hablar con los ingenieros que conocen la centrifugadora para que te digan dónde tocar. Algunos de estos módulos se pueden hacer «en casa», mientras que otros se pueden, mejor dicho se deben, encargar. Estados Unidos es un caso un poco especial porque tienen un presupuesto ingente (creo que US Cyber Command maneja algo así como 500 millones de dólares anuales), y un modelo de colaboración público-privado con la figura del «contratista» que da envidia. Pero imagínate el caso español y suponte que quieres crear el 100% del software, además del dinero e infraestructuras. ¿Dónde vas a encontrar a los «figuras» que lo hagan? Esto me recuerda, amigo Salas, que el poder de la CIA nunca residió en la cantidad de funcionarios que tienen encerrados en Langley sino en la legión de espías dispersos por todo el mundo y que son «externos». Es como el chiste del enviado de Bush de la CIA para infiltrarse en el País Vasco, que hablaba euskera sin acento, que conocía todas las costumbres locales pero que no conseguía que le sirvieran en la herriko taberna porque era negro.

Rompí a reír. Conozco a David R. Vidal desde hace mucho, y estoy familiarizado con su incisivo sentido de la ironía, pero reconozco que continúa sorprendiéndome.

—Te lo pongo más fácil —prosiguió sin dejar de mirar de reojo la pantalla del ordenador—. Se supone que para descubrir nuevos métodos de ataques informáticos hace falta un «gurú», vamos, un genio informático, algo que no es fácil encontrar en un servicio gubernamental. Y digo que no es fácil porque, por ejemplo, para entrar en un servicio policial, el «hacker» tendría que superar unas oposiciones. Si toma abundante Coca-Cola y pasa muchas horas sentado delante del ordenador, puede que ni siquiera pase la prueba física. Aunque el problema principal es otro. Si eres un genio informático, tienes fácil el conseguir un excelente salario en cualquier empresa. Además, la creatividad va algo reñida con la disciplina y no a todo el mundo le hace gracia estar en un cuerpo suprajerarquizado como un servicio policial o de Inteligencia. Vamos, yo mismo jamás me he planteado cursar una solicitud para ser funcionario del CNI o hacer unas oposiciones para poli. Y militar ni te cuento, dicho sea con el debido respeto. Vamos, que no sirvo. Soy consciente de mis limitaciones. O sea, ¿cuántos genios informáticos estarían dispuestos a trabajar para el Estado, ganando diez veces menos que en el sector privado, en un sitio donde la palabra del jefe se acata sin debate, y en donde los horarios, indumentaria y otros aspectos son dogma de fe? Hay que tener vocación, o ser un patriota… o ser gilipollas.

Uno de sus teléfonos móviles comenzó a sonar. David lo apagó sin mirar quién llamaba y continuó hablando. Eso siempre es una buena señal. Cuando está cómodo y con ganas de hablar, suele decir cosas interesantes.

—Yo entiendo que un policía o un militar quiera pasarse al CNI donde ganan más dinero por el tema de complementos y llevan una vida más relajada (a cambio de ceder parte de su vida privada), o que sueñe con eso un tipo normalillo que no destaque especialmente en nada. Pero para un gran profesional… no sé. Yo es que no

lo veo. Muy distinto es hablar de colaboraciones, que sí resultan sumamente interesantes, pero es lo mismo que ir a comprar fuera. Volviendo al tema, empresas como Hacking Team son tan imprescindibles como una fábrica de armas, con la diferencia de que cualquiera puede montarla si encuentra los profesionales adecuados. No se almacena pólvora, sino herramientas informáticas que pueden ser inofensivas o no dependiendo del uso que quieras darles.

Para David R. Vidal, que trabajó durante doce años para el CNI, y que antes y después de eso trabajó para otros servicios, no hay nada escandaloso en la conducta del Hacking Team. Forma parte de su mundo. El negocio de la información. David también ha programado troyanos y herramientas de espionaje, ha reclutado informadores, ha coordinado fuentes… Es parte del día a día de los espías. Sin embargo, al menos esta fue mi percepción, empresas como Hacking Team nunca estuvieron bien vistas en la comunidad, que los consideraba mercenarios en venta al mejor postor. Pero en lugar de empuñar M16, empuñaban teclados de ordenador.

—Los hackers se han convertido en el mayor dolor de cabeza de los servicios de Inteligencia, aunque no todos sean tan conocidos como Snowden, o Wikileaks. En 2014, un tal Chris Coleman[247] revolucionó las redes al revelar información sensible sobre el Gobierno marroquí en Twitter. Tú seguiste el caso muy de cerca y rescataste esa documentación que después desapareció de Twitter cuando su cuenta fue anulada… ¿Qué pasó? —le pregunté a David.

—Snowden no es un hacker —precisó él, molesto por mi apreciación—, sino el informático que trabajaba para un contratista encargado del mantenimiento de los equipos, y se las apañó para robar información. Lo de Chris Coleman, un personaje ficticio que publicaba en redes sociales documentos de los servicios marroquíes, es un caso diferente. En realidad, en ambos casos no es que se haya descubierto nada que no se supiera en el mundillo, sino que su impacto es la trascendencia en la opinión pública. Ahora la gente ha descubierto que los espías se dedican a espiar… a todo el mundo, no solo a los malos. Y eso es porque los terroristas no llevan una equis en la espalda de forma que se les pueda espiar solo a ellos. En Inteligencia no hay amigos, solo intereses compartidos. Dos naciones pueden llevarse muy bien y compartir información sobre un terrorista, pero a la vez ser competidoras, por ejemplo, en una licitación internacional donde participan empresas multinacionales. O por ejemplo, ¿acaso crees que no interesa saber lo que piensa hacer Tsipras en una reunión antes de que esta tenga lugar? A todo el mundo le gustaría jugar con las cartas marcadas.

»Con respecto a Chris Coleman, su aparición tuvo lugar cuando Francia y Marruecos no atravesaban su mejor momento diplomático y desapareció cuando volvieron a ser amigos. Tampoco apareció ninguna filtración que perjudicase al país vecino. Con todo, no creo que los servicios de Inteligencia franceses estuviesen detrás, aunque sí creo que tuvieron algo que ver con su desaparición. No se llegó a saber quién era Coleman, aunque supongo que algún joven con fuertes vínculos

franceses, tal vez descendiente de inmigrantes o algo así. El caso es que Coleman pirateó algunas cuentas de correo, probablemente gracias a instalar un troyano en un ordenador de un gerifalte de la DGED. Aparecieron cientos de correos con material muy entretenido, donde se notaban los esfuerzos de la DGED para defender los intereses marroquíes. En especial, el punto más recurrente era el conflicto del Sahara. En los documentos quedan «con el culo al aire» una docena de periodistas a los que se les pagaba para que minimizasen cualquier asunto referente a terroristas de origen marroquí y que enfatizasen hasta la saciedad incidentes con miembros del Polisario, poniéndolos como un nido de criminales.

Las revelaciones de Coleman fueron consideradas el Wikileaks marroquí. Hoy es posible examinar la repercusión mediática de esas filtraciones a través de una web aún operativa: «Los papeles de Coleman» donde fueron compilados.[248]

—Con todo lo que publicó —continúa el agente Juan— se podía hacer un libro. El más perjudicado fue Ahmed Charai, director del semanario *L'Observateur du Maroc*, ese que publicó aquello de que José María Aznar era el padre de la hija de la exministra francesa Rachida Dati a modo de *vendetta*, y que fue condenado por la justicia tras la querella del expresidente. En los documentos aparecen pagos de transferencias a periodistas norteamericanos y franceses principalmente. Al parecer se pagaban unos 6.000 euros por artículos promarroquí, aunque algunas transferencias alcanzan montantes importantes, de unos 60.000 dólares. También aparece de refilón un conocido periodista español, muy promarroquí, pero solo en una invitación.

La acusación de que importantes periodistas españoles y norteamericanos estarían trabajando a sueldo del régimen marroquí, para intentar polarizar a la opinión pública, por ejemplo contra el pueblo saharaui, también motivó gran indignación en la comunidad periodística.[249]

—Pero para mí —continúa el agente Juan— uno de los documentos más didácticos, que pasó desapercibido y su vida en internet fue efímera, fue un documento confidencial de un «Centro americano-marroquí» titulado «Plan estratégico 2012». En él se establecen claramente los objetivos de este centro, que no son otros que influenciar en la política exterior norteamericana de la Administración Obama, de forma que se apoye la anexión progresiva del territorio saharaui a Marruecos. Para ello, el documento, que es una especie de guía, plantea el objetivo de que el Gobierno norteamericano financie de manera tangible políticas de «hechos consumados» o, si no lo consiguen a ese nivel, que existan proyectos específicos de congresistas en ese mismo sentido. Aparte de las iniciativas diplomáticas, se buscan otros esfuerzos, incluyendo al Congreso, *think tanks* y los medios de comunicación norteamericanos. El resultado esperado, según el documento, era ni más ni menos poner a Marruecos como el modelo a seguir en la región, tanto en temas de derechos humanos, como cooperación en materia de seguridad y de «reforma democrática pacífica».

En diciembre de 2014 se publicó la noticia de que un grupo de hackers autodenominados Hawks Moroccan Sahara habrían identificado a Chris Coleman como «Mohammed Mahmoud Mbarek, un agente de Inteligencia argelina que viaja a muchos países europeos con el fin de escapar de la persecución». Su cuenta de Twitter fue cerrada, y Coleman desapareció de la red tan misteriosamente como había llegado.[250]

Aproveché la ocasión para insistir a Vidal en el tema de la filtración a *La Razón* del servicio de Inteligencia del que me había hablado Falciani. Todavía no podía entender de dónde había salido la información.

—¿Filtraste tú a *La Razón* el proyecto del servicio de Inteligencia ciudadana de Falciani? ¿Y por qué aparece solo tu nombre en el artículo?

—Para nada —me repitió David desmarcándose del asunto—. La primera sorpresa fue mía, ya que ni siquiera supe en qué consistía el proyecto, puesto que no he llegado a hablar con Falciani. Te diré que a mí me da la sensación de que hay algún malentendido con lo de llamarle «servicio de Inteligencia» y seguramente quieren, o querían, montar otra cosa aunque lo llamasen así. Vamos, que sin conocer el proyecto, te diré que las competencias de las administraciones locales son muy escasas. A nivel de seguridad, no sé, no se me ocurre lo que pretenden…

»Otra cuestión muy diferente, Toni, sería que el proyecto partiese de una Comunidad Autónoma. Ahí sí que lo veo interesante y recomendable. Inteligencia no es hablar de espías, sino apoyo a la toma de decisiones. En una Autonomía se puede usar tanto para diseñar estrategias de seguridad (siempre que tengas tu propia Policía, claro), pero también estrategias económicas. Es una pena que no exista más cultura en esta línea porque todas las Comunidades deberían preocuparse de evolucionar en este sentido y no esperar a que otros resuelvan los problemas, lo que puede que no pase nunca… o que no interese, pues los intereses del Estado son para el conjunto del Estado. Te diré algo para que reflexiones: el CNI está al servicio del Estado y no necesariamente al servicio de los ciudadanos como tales, lo que puede coincidir… o no.

El asunto de Falciani no suponía la primera ocasión en que el nombre de David Vidal se asociaba en la prensa nacional o extranjera con alguna supuesta trama de espionaje. Poco antes varios medios marroquíes especularon con la posibilidad de que mi amigo fuese el programador de uno de los virus espía más notables de los últimos años.

—¿Por qué en Marruecos te acusaron de ser el autor de Careto?

—Supongo que al bloguero se le fue la olla y confundió churras con merinas. Vamos a ver, es cierto que el CNI me dijo, en un momento dado, que proporcionase teléfonos de «personas de interés» en Marruecos, ya que podían «trabajarlos». También es cierto que diseñé un «troyano» que fue probado en un país extranjero, lo cual no tiene relación alguna con lo anterior. Yo no tengo ni idea de para qué se usan los teléfonos que he proporcionado, pero veo altamente improbable que el objetivo

fuera la interceptación de datos digitales o que hubiera una relación con Careto. Dicho esto, mi opinión personal es que Careto se encargó a una empresa especializada. ¿Quién está detrás? Pues, dependiendo de los intereses, está claro que los servicios españoles o los franceses son los principales sospechosos.

Sin embargo, ni CiberBerkut, ni Hacking Team, ni Coleman, ni Careto pueden hacer sombra a la que continúa siendo la operación de hacking y espionaje más notable de todos los tiempos. A pesar de los años transcurridos, Stuxnet continúa siendo un referente. Y para informáticos como David Vidal, una fuente de inspiración.

Stuxnet fue un gusano informático, descubierto en 2010, cuyo objetivo era presuntamente interferir en el programa nuclear iraní. Se supone obra del Mosad y la CIA.

—El gran caso de aplicación del hacking a una operación de Inteligencia fue Stuxnet. Creo que tú lo has estudiado a fondo…

—Verás, Toni, Stuxnet tiene la misma función que Wikileaks: aporta las evidencias de aquello que crees saber pero que no puedes probar. Te voy a decir solo dos cosas con respecto a Stuxnet. La primera es que es un virus «ensamblado», es decir, un proyecto donde han participado muchas personas. En sus módulos incluso aparecen diferentes lenguajes de programación. Esto refuerza lo que te dije antes de que no tiene nada de especial subcontratar un módulo específico.

»La segunda es que, al margen de lo bien o lo mal diseñado que estuviera, hay cosas que solo puede hacer un servicio de Inteligencia. De hecho, en internet está el código de Stuxnet con lo que cualquiera puede adaptarlo, pero conseguir una herramienta peligrosa no es fácil. Necesitas dos ingredientes fundamentales para cocinar la diferencia entre el éxito y el fracaso: vulnerabilidades del día cero, es decir, aquellas vulnerabilidades que se descubren en los sistemas y que son tan recientes que todavía no se han solucionado, es decir que no hay «parches» disponibles. En el mercado negro, dependiendo de su importancia, se pueden pagar tranquilamente cifras de 10.000 o 15.000 €. Estas vulnerabilidades solo duran días o semanas, porque más pronto que tarde se solucionan. Pues bien, cualquier hacker que conozca a tiempo una de ellas es el rey del mambo. Stuxnet tenía una docena.

»El segundo ingrediente que necesitaba era una firma digital. Es decir, que el virus se instalaba solo porque llevaba un modulito firmado con un certificado de Realtek Semiconductor, que se suponía de confianza. Sin firma no hay instalación y por tanto el virus es inútil. ¿Cómo se obtiene ese certificado? Fácil, si eres Tom Cruise en *Misión Imposible*. Entras por la noche en el cuartel general de Realtek sito en el Parque Científico e Industrial de Hsinchu en Taiwán, te saltas sus supermedidas de seguridad antiespionaje industrial y lo robas. Dado que los certificados pueden ser revocados, nadie puede percatarse de que el robo se ha producido.

»Para más inri, una vez que el virus fue descubierto, apareció una nueva versión del mismo firmada con otro certificado, esta vez de JMicron, sustraído igualmente en

Hsinchu, ya que entre el edificio de Realtek y el de JMicron apenas hay unos cientos de metros. Ya puestos a robar, mejor llevarse un par. Esta segunda versión de Stuxnet no tenía ningún objetivo más allá de ser descubierta. Es decir, una demostración de poderío: no es que sus creadores pudieran hacerse con un certificado sino con los que hiciera falta. La moraleja es que, salvo en las películas, no es suficiente con ser un hacker muy bueno para hacer guerra cibernética, sino que necesitas tener una potente organización detrás, lo que solo está al alcance de aquellos servicios de Inteligencia con grandes medios.

Cada vez que salgo del búnker de David R. Vidal tengo la misma sensación. La de ser un títere. Un ciudadano que paga unos impuestos abusivos, gestionados por políticos que me mantienen en la más absoluta ignorancia de lo que realmente está ocurriendo en el mundo. Quizá es que ellos también lo ignoran. Porque por encima de los gobiernos, que rotan cada cuatro años, existen otras formas de poder que permanecen siempre. El dinero y los secretos.

Como si en una inmensa partida de ajedrez, que es nuestra historia, los ciudadanos fuésemos simples peones, y los políticos alfiles, caballos y torres. Sin embargo, por encima de ellos hay fichas más importantes. Y por encima de todas ellas, los verdaderos jugadores.

Los hackers, como Assange, Snowden, Falciani o Coleman nos han revelado algunas de las jugadas en las que nos mueven de una casilla a otra. En las que los medios de comunicación y la propaganda en la red polariza nuestros sentimientos y emociones, en función de los intereses de uno u otro jugador. Pero por muchos secretos que se filtren, tengo la sensación de que solo vemos la punta del iceberg. Lo malo es que no tenemos forma de comprobar si ese iceberg es realmente un trozo de hielo sólido, o un espejismo.

Impotentes para detener a los hackers —que descubrieron que un invento de origen militar, internet, podía emplearse contra los conspiradores que lo idearon—, las agencias de Inteligencia decidieron que la mejor forma de combatir la información no deseada era mezclarla con desinformación. Por eso internet plantea cada día un reto a nuestra capacidad de discernimiento para adivinar qué es real y qué es falso. No es una tarea sencilla. Como simples usuarios, la mayoría de las veces nos resulta imposible dilucidar si esas grandes conspiraciones son tales, o un nuevo bulo en nuestra red social, o en nuestra bandeja de correo. Y aunque cosas que parecen tan lejanas —como el conflicto en Siria, el gusano Stuxneto el terrorismo yihadista— tarde o temprano llegan a nuestras vidas, para afectarlas, hay otras amenazas más urgentes.

Y si alguien tiene una visión global y actual de todas ellas, y podía cerrar mi viaje con un resumen final es él: el Maligno.

El Maligno

Como en todas mis investigaciones, empecé mi viaje al mundo del hacking desde cero y con muchos más prejuicios que conocimientos. Un lastre pesado en la mochila del que te vas desprendiendo a medida que vas adquiriendo más perspectiva. Y cuando tecleas en Google «hacker español», la primera imagen que aparece en el buscador es la de un tipo con el pelo largo y un gorro de lana, de color azul y marrón. Es el doctor don José María Alonso Cebrián, licenciado en Ingeniería Informática y doctorado en Seguridad Informática por la Universidad Rey Juan Carlos de Madrid (donde comenzó mi aventura personal con MarkoSS88).

Sin embargo, es posible que hasta para algunos iniciados en el mundo del hacking el nombre del José María sea poco familiar, porque Alonso Cebrián se apeó de protocolo en cuanto cambió su birrete de doctor por su emblemático gorro de lana. Pero si digo que estoy hablando de Chema Alonso, «el Maligno», todo el mundo sabrá inmediatamente a quién me refiero.

Chema Alonso es sin duda el hacker español más conocido dentro y fuera de nuestras fronteras.[251] De hecho, viaja por todo el mundo para participar en algunas de las CON más importantes del planeta. Y por eso es la persona que sabe lo último que se está cociendo en el mundo del hacker a nivel internacional.

Chema proviene de una familia humilde. Un matrimonio roto que le obligó a trabajar para pagarse sus estudios superiores. Con veinticuatro años montó su primera empresa: Informática 64, una consultoría de sistemas y seguridad informática en su Móstoles natal, que dirigió durante catorce años. Informática 64, hoy parte de Eleven Paths (filial de Telefónica), continúa su actividad. Formación, herramientas, consultoría, además de mantener en 0xWord.com, una prolífica editorial donde han visto la luz las primeras obras de algunos de los expertos españoles más relevantes. Yo empecé allí mi viaje. En cuanto la descubrí, viajé a Móstoles para comprar una docena de títulos que me parecían una buena manera de comenzar a familiarizarme con el hacking. Fracasé en el empeño. La inmensa mayoría eran libros técnicos escritos por y para expertos en seguridad informática. Así que, a pesar de mis esfuerzos, no conseguía pasar del primer capítulo. Y no porque las obras que compré[252] fueran malas. Todo lo contrario. Eran demasiado buenas. Textos profesionales para lectores profesionales. Pero es que yo no lo soy. Afortunadamente, de vez en cuando, aparecían títulos como la novela *Hacker épico* (recientemente versionada en cómic) o el ensayo *Microhistorias: Anécdotas y curiosidades de la informática,* a los que ya me he referido varias veces, que lectores tan torpes como yo podíamos disfrutar mientras aprendíamos. De hecho, fueron los primeros libros que leí sobre informática en mi vida.

De espíritu renacentista, el Maligno es un tipo inquieto. Lo demuestra su canal en YouTube,[253] donde se recogen todas sus intervenciones televisivas y conferencias.

Absolutamente desternillantes. No importa que, como era mi caso, no entendiese ni una palabra de los aspectos técnicos que comentaba. Hasta sus críticos más feroces se ven obligados a reconocer que como comunicador no tiene rival. De hecho, durante un tiempo, diez años atrás, Chema no tuvo problema en presentarse como el «Torrente de la Informática»,[254] en su faceta como monologuista.

El filósofo, poeta y filólogo alemán Friedrich Nietzsche decía: «La potencia intelectual de un hombre se mide por la dosis de humor que es capaz de utilizar». Y si algo caracteriza las conferencias de las CON a las que he podido asistir durante estos años, es el sentido del humor que salpica cada una de las ponencias. Hacer llorar es fácil. Hacer reír requiere mayor creatividad. Pero conseguir que la audiencia se desternille en una disertación técnica sobre seguridad informática es algo que solo consiguen los cerebros mejor amueblados. El fiscal Bermúdez, el juez Calatayud, el Maligno…

De alguna manera ha estado presente a lo largo de toda la investigación. No solo porque su nombre salía a colación una y otra vez en mis entrevistas con diferentes miembros de la comunidad, para bien en unas ocasiones y no tan bien en otras (aunque siempre sospeché que Chema Alonso se había convertido en lo que muchos hackers querían ser cuando fuesen mayores…). No solo porque en algunos foros, como en la mesa redonda de la última Rooted, llegó convertirse en objeto del debate público. Es que además me topé con él, en situaciones a veces un poco kafkianas, en diferentes eventos durante los últimos años.

En una CON me lo tropecé en los lavabos, pero tenía algo importante entre manos y no me pareció oportuno interrumpirlo. En una edición de X1Red+Segura se plantó en la sala sin previo aviso y se sentó detrás de mí, pero pronto fue sepultado por una legión de fans que buscaban un autógrafo y/o una foto con el Maligno. Así que nunca encontraba la oportunidad para abordarle.

Sin embargo, debo confesar que me imponía un poco entrevistarle. En 2013 le escuché soltar un chiste en una conferencia. Todo el mundo rompió en carcajadas, pero yo no lo entendí, y decidí que no entrevistaría a Chema Alonso hasta que comprendiese qué había de gracioso en que un tipo le enviase un email preguntándole cuántos megas ocupa una *botnet*. Hoy ya lo entiendo. Actualmente Chema Alonso simultanea sus inagotables intervenciones televisivas y radifónicas, sus publicaciones y su participación en las CON, con su trabajo en Telefónica Digital. Y allí me convocó cuando pedí una audiencia con el Maligno.

Quedamos en la cafetería situada entre los tres edificios del bloque oeste de la ciudad de Telefónica, en Las Tablas (Madrid). Llegué un rato antes, como siempre, para echar un vistazo al local y escoger la mesa que me pareciese más conveniente. Una al fondo, en el rincón. Me senté de espaldas a la pared y con la mejor perspectiva de la entrada, y allí le esperé repasando las notas que había preparado.

Me costó un poco reconocerle cuando se asomó a la puerta. El tipo que se había plantado allí llevaba el pelo recogido en una coleta, y ningún gorro bicolor de lana

cubría su cabeza. Desde la puerta miraba hacia todas las mesas ocupadas por una sola persona, pero lógicamente él no podía reconocerme a mí. Sin embargo, en cuanto identifiqué en su camiseta el logotipo rosado de FOCA, la primera herramienta de *pentesting* y análisis de metadatos que yo utilicé, supe que era él.

Supongo que algunos amigos comunes, como David Pérez, Román Ramírez o Selva Orejón, le dieron buenas referencias. Porque aunque me habían asegurado que era un tipo muy generoso, su primera frase, nada más conocernos, me desarmó:

—Hola, Toni, dime qué puedo hacer para ayudarte.

—Caray… pues ojalá te hubiese conocido hace un par de años… Seguro que me habría ahorrado muchos quebraderos de cabeza. Ahora me basta con que me des un poco de tu tiempo para responderme a unas preguntas.

Y como me había ocurrido antes con los mejores cerebros de la comunidad hacker, solo encontré amabilidad, colaboración y una disposición absoluta para ayudarme en que mi libro expusiese la realidad de la cultura hacker, más allá de los estereotipos y etiquetas tan consolidados por el cine, la literatura o la prensa.

Alonso es un personaje mediático. Mientras charlábamos en la terraza de la cafetería, resultó inevitable que algún admirador le reconociese y se acercase a nuestra mesa para felicitar a Chema por su blog, para hacerle alguna consulta o para sacarse una foto con el Maligno. Yo esperaba pacientemente para pasar a la pregunta siguiente. Pero uno de aquellos fans espontáneos le hizo una sugerencia que me pareció muy interesante. ¿Por qué no dedicar una entrada de su blog, «Un Informático en el Lado del Mal», a la seguridad informática en los dispositivos domóticos?

El internet de las cosas

—Pues no me parece una mala idea, Chema —dije, haciendo mía la pregunta del admirador que acababa de hacerse un selfi con el Maligno—. Yo estoy muy preocupado por mi madre. Primero fue el teléfono móvil, después el WhatsApp, luego el mail, ahora el Facebook… Y para una inmigrante digital, el internet de las cosas puede ser el nuevo peligro.

Cómo explicarle a mi madre que esos flamantes electrodomésticos de última generación que tanto envidia pueden suponer un peligro a nuestra privacidad. Cómo hacerle entender que durante las Navidades de 2013, 100.000 neveras, televisores y otros aparatos domésticos con acceso a internet enviaron más de 750.000 emails desde las casas en las que estaban instalados. Y aunque algunos, como los televisores inteligentes Samsung, ya advierten en su manual de instrucciones que «Por favor tenga en cuenta que si sus palabras habladas incluyen información personal o confidencial, esta formará parte de los datos capturados y transmitidos a un tercero a través de su uso de la función reconocimiento de voz»,[255] ¿cómo pretenden que en el salón o en el dormitorio de nuestra propia casa no incluyamos información personal o confidencial en nuestras conversaciones familiares?[256]

—A mi madre cosas como estas puedan parecerle ciencia ficción. Pero ¿hasta qué punto podemos estar todos nosotros seguros con neveras, televisiones o lavadoras que tienen acceso a internet? —le pregunté.

—Es difícil decir ahora, en este estadio tan temprano del despliegue de las tecnologías del hogar en el mundo tecnológico. Lo cierto es que las grandes empresas se están posicionando para ser las que gestionen desde la nube todos los datos que se generen de una casa con el objeto por supuesto de poder hacer negocio. ¿Por qué ir a comprar huevos a la tienda de la esquina si una empresa como Apple puede saber que te faltan huevos y enviártelos desde algún remoto lugar de la ciudad a cambio de una pequeña comisión?

»En el mundo de la seguridad personal, Toni, los problemas de tener dispositivos que se conecten fuera pueden ser muchos. Desde que un atacante acceda al panel de administración de tu casa y pueda vigilarte a todas horas (y ya hemos tenido muchos casos de *ciberstalkers*), hasta que un ladrón pueda saber si estás o no en casa por la curva de consumo eléctrico de tus dispositivos sacada de los *smartmeters* para perpetrar un asalto, o llegar a producir un accidente doméstico manipulando los electrodomésticos. Pero es que también se gestionan las alertas de humos, de incendio, de detección de gases de una caldera, las puertas de acceso, etcétera, etcétera. Si esto lo llevamos a entornos de personas con alguna discapacidad, la cosa puede ser aún peor. Yo veo esto como el principio de meternos en esa capsulita de Matrix. Primero los datos de nuestras necesidades en el hogar, y luego ya nos conectan a Matrix… o no, ¿quién sabe?

El internet de las cosas (IoT, por las siglas en inglés de «Internet of Things») preocupa a la comunidad hacker. De hecho, en la mayoría de las CON se presenta al menos una conferencia que aborda este inquietante fenómeno.

En 2009, el ingeniero informático Kevin Ashton —que ya había propuesto el concepto «internet de las cosas» durante una reunión del MIT en 1999—, publicó un artículo en el diario *RFID* en el que venía a concluir que «el internet de las cosas tiene el potencial para cambiar el mundo tal y como hizo la revolución digital hace unas décadas. Tal vez incluso hasta más».

Ashton tiene razón, el internet de las cosas, que cada vez está más presente en nuestras vidas, puede cambiarlas, pero no sé si necesariamente para bien. Se calcula que todo ser humano está rodeado de entre mil y cinco mil objetos; neveras, televisores, impresoras, microondas, termostatos, vitrocerámicas, lavadoras, coches, motos… y cada vez más y más de esos objetos llegan con una conexión a internet. Según la empresa Gartner, en 2020 habrá en el mundo aproximadamente 26.000 millones de dispositivos con un sistema de adaptación al internet de las cosas.Abi Research, por otro lado, asegura que para el mismo año existirán 30.000 millones de dispositivos inalámbricos conectados a internet. Con la próxima generación de aplicaciones de internet (protocolo IPv6) se podrían identificar todos los objetos, algo que no se podía hacer con IPv4. Este sistema sería capaz de identificar instantáneamente por medio de un código a cualquier tipo de objeto: zapatillas deportivas, marcapasos, vasos, botellas, platos, paquetería, lámparas, botiquines…

Igual que ahora ya podemos conectar la calefacción, la lavadora o el horno antes de llegar a casa, o seguir nuestro teléfono móvil si nos lo roban, e incluso borrar los datos o inutilizarlo a distancia, en el futuro podremos localizar cualquier objeto a través de programas de geolocalización. El internet de las cosas puede facilitarnos la vida, pero también complicárnosla, porque todo dispositivo electrónico es hackeable.

Después del estreno en la cadena estadounidense CBS, el 6 de octubre de 2000, la serie CSI se convirtió en un éxito mundial. La serie original, *CSI: Las Vegas*, relata las aventuras de un grupo de criminalistas que resuelve los casos aplicando el método científico. Con grandes audiencias, alcanzó la impresionante longevidad de quince temporadas en antena. Pero además inspiró otras series *spin-off* paralelas y simultáneas: *CSI: Miami* (2002-2012) y *CSI: Nueva York* (2004-2013).

En 2015 los productores deciden renovar el producto y escogen el único tema posible: la ciberdelincuencia. El 4 de marzo se estrena *CSI: Cyber,* las peripecias de una unidad de ciberpolicía del FBI liderada por una ciberpsicóloga; la doctora Avery Ryan (Patricia Arquette).[257] Tras mucho debatir sobre el contenido del primer capítulo de la serie, que tenía que enganchar a la audiencia y mantener el prestigio de la franquicia CSI, productores y guionistas llegaron a la conclusión de que el tema que más preocupa a los norteamericanos actualmente es el internet de las cosas. Y en su primer episodio el equipo de hackers de la doctora Avery Ryan tiene que enfrentase a una mafia internacional que piratea los dispositivos de vigilancia de

bebés que millones de padres tienen en los dormitorios de sus hijos, con el fin de escoger a los niños que serán subastados *online,* para luego ser secuestrados. Y ese peligro, el internet de las cosas, sería explotado en los siguientes capítulos de la serie.

Montañas rusas que pueden ser hackeadas para provocar un accidente, impresoras que pueden incendiarse a distancia… En otras palabras, un ejemplo tras otro de cómo los dispositivos electrónicos ya implantados en los niveles más íntimos de nuestra vida doméstica pueden volverse contra nosotros. Exactamente como me explicaba Chema Alonso.

El *hacking* en el siglo XXI

—¿El nombre del Maligno es el legado de un tiempo en que la comunidad hacker hispanoparlante estaba más dividida qué ahora? ¿Eres el Diablo disfrazado de John Lennon?

—Sí, de ahí viene. De que uno me comparó con el Maligno disfrazado de John Lennon. Mi admiración por el personaje de Lennon es tal, que no dudé en quedarme con Maligno. Antes la comunidad estaba dividida entre malos (los que usaban Microsoft) y buenos (todos los demás). Hoy en día esa polarización no es tanta. Movimientos como el software libre se utilizaron políticamente para crear una guerra que nunca debería haber existido. El Software Libre y el Open Source son unos movimientos preciosos que respeto, valoro y apoyo. Yo mismo he liberado algunas de nuestras herramientas como Open Source y/o Software Libre. Sin embargo, no me gusta que nos dividieran entre buenos y malos como corderos, llegando a auténticas situaciones kafkianas. Yo vi a un chaval de quince años que vino a hablar conmigo en la puerta de un evento de Microsoft TechED para decirme que Windows era el diablo. Hoy siguen existiendo grupos radicales, pero creo que todo se ha normalizado y entendemos todos el valor de los diferentes tipos de licencia en el software. Mientras, las empresas se han llevado el código a la nube… y adiós muy buenas.

—Recuerdo una conferencia tuya en la que proyectaste unas fotos de tu juventud. Bueno… digamos que tenías un aspecto muy diferente al que tienes ahora. Has mejorado con los años. Pero aunque siempre fueses el empollón de clase, parece que el espíritu hacker, rebelde, transgresor, es incompatible con trabajar para una gran multinacional. O al menos eso te reprochan algunos amantes del software libre y el PGP… ¿Cómo terminó aquel joven emprendedor de Móstoles fichado por un gigante como Telefónica?

—Acabé en Telefónica casi sin darme cuenta… y estoy muy contento. La mayoría de los grandes hackers españoles han acabado trabajando en grandes multinacionales. Tenemos compañeros de la comunidad trabajando en Google, Microsoft, Facebook, Salesforce, Yahoo!, Kaspersky, HP, IOActive, Repsol… La lista de grandes hackers españoles que trabajan en equipos de seguridad y desarrollo de empresas multinacionales es brutal. El nivel de nuestro país en su comunidad de investigadores es altísimo. Yo no quería dejar España, y tras tener alguna oferta de Microsoft y Google, seguía dando charlas por todo el mundo. La historia fue sencilla.

»Di una conferencia en la Ekoparty 2011 en Buenos Aires sobre mi FOCA. Entre los asistentes estaba un miembro de FIRST y me llamaron para ir a dar una conferencia en Perú. Allí, entre los asistentes estaba el entonces director del Vertical de Seguridad de Telefónica a nivel global. Me vio y pensó que yo era la persona ideal para concienciar al Top, 150 de directivos de Telefónica, de la importancia de la seguridad. Me contrató para una charla y entre los asistentes se encontraba don José María Álvarez-Pallete (actual CEO de Telefónica). Tras montar Wayra en España me

llamó para ayudarle a traer talento a las *start-ups* y… el 1 de febrero de 2016 hará cuatro años que estoy en Telefónica. ¿Por qué acepté? Porque me dijo: «Chema, ficha a los que quieras y haz productos de seguridad que tú quieras». Era una oferta irrechazable que me permitió traerme a grandes profesionales a trabajar conmigo en Eleven Paths.

—Hace unos meses, Wikileaks liberó cuatro millones de emails de Hacking Team. He encontrado a la comunidad muy dividida en cuanto a la valoración de esta empresa italiana. ¿Héroes o villanos? Es que no sé si ponerlos del lado de Cálico Electrónico o del Gran Dimitri…[258]

—Al gran Cálico Electrónico hay que dejarle fuera de estos saraos, que ya tiene bastante con sus problemas de financiación para seguir adelante. Lo de Hacking Team es un caso muy controvertido. Son herramientas que permiten hacer un «registro virtual de terminales móviles y ordenadores». Yo lo suelo ver como los micrófonos, las cámaras de seguridad, los sistemas de interceptación telefónica o las herramientas que usan los cuerpos de seguridad para hacer registros físicos en viviendas o aeropuertos, algo que usado por un juez puede ser para bien o para mal. Por supuesto, creo que el debate debe ser más maduro y asumir que si un pederasta o un asesino de niños o un terrorista se esconde en sistemas informáticos invulnerables, tendrá toda su privacidad intacta, pero la sociedad habrá perdido la oportunidad de proteger el derecho a la infancia o el derecho a la vida. Dicho esto, el gran problema es que alguien utilice estas herramientas de forma abusiva y sin control judicial, como hemos visto en los Estados Unidos con el caso de la NSA. En muchos países hay legislación que permite el uso de estas herramientas para determinados tipos de delitos y bajo supervisión judicial pueden hacerlo.

»Por otro lado, las leyes que dan cobertura a la seguridad nacional, igual que dejan usar armas de otro tipo, autorizan a cuerpos de inteligencia a usar cosas similares a Hacking Team. Yo creo que el derecho a la privacidad no es el centro de los derechos de nuestra vida, y por eso dejo que me registren todo lo que llevo en las maletas cuando viajo. Eso sí, siempre sujeto a legalidad y bajo control para que no haya abusos.

A pesar de la indignación que había generado en otros veteranos, como Román Ramírez (RootedCON) o Pedro Candel (Navaja Negra), la reforma de la ley no había despertado ninguna reacción especial en el Maligno, así que se lo pregunté directamente.

—Supongo que a ti no te ha afectado mucho la reforma de la ley que entró en vigor el 1 de julio pasado… Sin embargo, ha habido mucho revuelo en algunos foros de hacking, porque algunos lo consideran un conflicto con el trabajo de los consultores de seguridad. ¿Tú cómo lo ves?

—Hay que ver cómo se implementa en la realidad. La verdad es que he hablado con muchos compañeros y hay opiniones controvertidas. Yo creo que habrá que modificarla a corto plazo porque nos quita flexibilidad a todos.

—Javier Marcos, fichado por Facebook en los Estados Unidos; César Cernuda, que lleva Microsoft en Asia; Bernardo Quintero, que trajo Google a Málaga; Lucas, que es un común amigo… Hay muchos españoles en la élite de las grandes empresas de internet. Tú has participado en algunas de las CON más importantes del mundo. ¿Qué opinión se tiene fuera de los españoles? Si sois tan buenos, ¿por qué estáis tan mal pagados?

—Fuera de España estamos muy bien pagados, y en España muchos también, pero no es comparable con los salarios en esos países. Todos los que has citado, a los que tengo el honor de conocer personalmente, son una pequeña muestra, pero tenemos a Fermín en Google, a Ángel Prado en Salesforce, a Marc Vilanova en seguridad en Facebook, etcétera. En España los salarios son menores, pero porque tenemos un capitalismo mucho menos agresivo que el de allí. Los impuestos en empresas y personas son muchos más altos. Aquí, alguien como yo pudo estudiar en los colegios públicos y en la universidad. Yo escribí un artículo que se titulaba «Por qué estoy agradecido a España y a la Universidad», donde comparaba los sueldos de un pintor de brocha gorda en Estados Unidos y en España y los costes de la Universidad y la Sanidad en esos dos países. Por supuesto, mi hermano y yo no habríamos podido estudiar ni de broma. Sigo prefiriendo cobrar un poco menos en España y tener un capitalismo más social como el que tenemos aquí y en Europa que lo que hay en los Estados Unidos. Y dicho eso, en España hay puestos muy bien pagados en tecnología para la gente buena. Hay que desarrollar más nuestra competitividad empresarial para que esto vaya aún mejor.

—Hoy toda nuestra vida pasa por la red. Cada vez más, la administración nos exige facturas digitales, declaraciones de la renta *online,* DNI electrónico… Entiendo que es más ágil y cómodo para los gestores de esos datos, pero ¿realmente se toman las medidas de seguridad necesarias, o cada vez estamos más desprotegidos?

—Es una pregunta de difícil respuesta. ¿Cuáles son las medidas de seguridad necesarias? Digamos que la administración pública toma medidas, innova y es puntera en e-administración en el mundo, pero decir que son las necesarias y oportunas es difícil para mí, para ti y para ellos. Siempre se puede hacer más, pero me consta que están preocupados por ello.

El blog «Un Informático en el Lado del Mal» tiene muchos lectores jóvenes. Muy jóvenes. Y yo todavía estaba tocado por la historia de Aranzazu, así que saqué el tema.

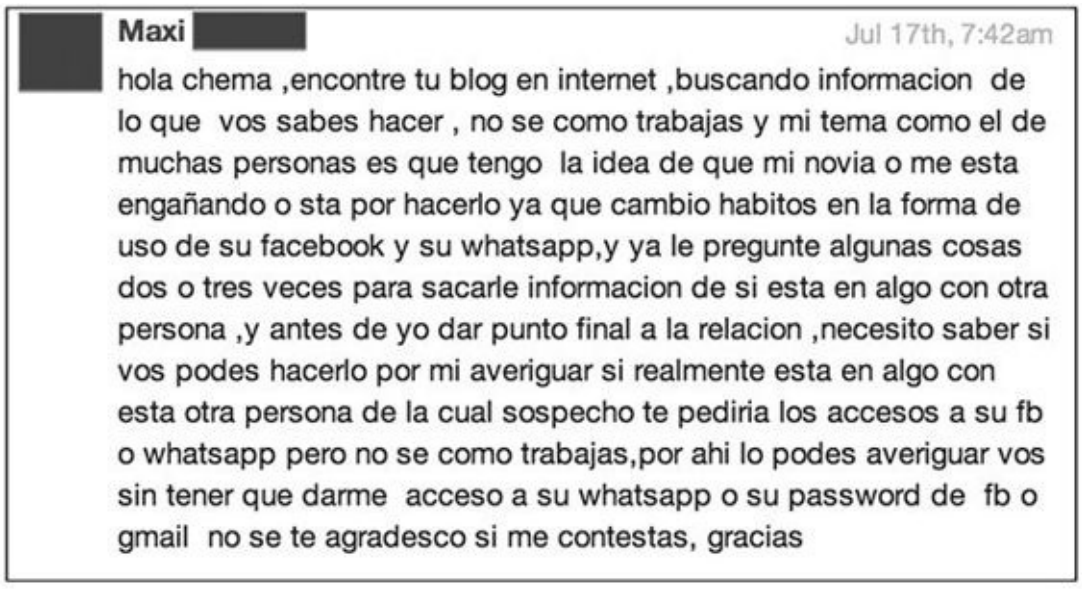
—¿Sabes Chema? De todos los capítulos de este libro, el que más me ha costado escribir es el relativo a los casos de *ciberbullying* que han terminado en suicidio. El último, Arancha, el pasado mayo… Tú eres un nativo digital con conocimientos privilegiados. ¿Qué puede hacer un padre que no está familiarizado con la tecnología con la vida digital de sus hijos?

—Acompañarlos. Yo siempre les recomiendo que los acompañen. Que igual que los llevan al colegio en coche o los vigilan en los parques, cuando estén con el

ordenador, el iPad o el teléfono móvil, estén con ellos. Que sepan qué usan, con quién y cuáles son los riesgos de lo que hacen sus hijos. Si los padres no saben, entonces el hijo o la hija aprenderá más que ellos y se saltará cualquier control que le hayan puesto de vigilancia. Lo he visto muuuchas veces. Al final, el menor con trece años acaba controlando al padre y saltándose cualquier protección.

—Me consta que para muchos jóvenes aspirantes a hackers eres un referente. Lo he visto en muchos eventos. Yo estaba entre el público y escuchaba lo que decían de ti. Y me consta también que los hackers tenéis cada vez más poder, en una sociedad tan tecnificada. Esos chavales podrán hacer grandes cosas con ese poder dentro de cinco o diez años… pero también cosas terribles. ¿Te preocupa cómo influyes en las futuras generaciones, o cómo pueden emplear los conocimientos que les entregas con cada post o con cada nuevo libro?

—Yo intento transmitirles el amor que tengo por la tecnología. La pasión que siento por estos cacharros desde que vi *Tron* y la de cosas maravillosas que se pueden hacer. Mezclar conocimientos de hacking y adolescencia siempre es un riesgo, pero yo estoy contento con la generación de hackers que nos está relevando. Son geniales. Hay chavales de dieciséis a veinticinco años con una capacidad grandiosa de hacer cosas maravillosas. Por supuesto, hay algunos que cruzan la raya, pero es más común ver a gente que hace cosas malas sin venir de la comunidad hacker que lo contrario. En nuestros eventos se respira transgresión, límites en la línea, pero no maldad o cibercrimen.


Maxi [redacted] Jul 17th, 7:42am

hola chema ,encontre tu blog en internet ,buscando informacion de lo que vos sabes hacer , no se como trabajas y mi tema como el de muchas personas es que tengo la idea de que mi novia o me esta engañando o sta por hacerlo ya que cambio habitos en la forma de uso de su facebook y su whatsapp,y ya le pregunte algunas cosas dos o tres veces para sacarle informacion de si esta en algo con otra persona ,y antes de yo dar punto final a la relacion ,necesito saber si vos podes hacerlo por mi averiguar si realmente esta en algo con esta otra persona de la cual sospecho te pediria los accesos a su fb o whatsapp pero no se como trabajas,por ahi lo podes averiguar vos sin tener que darme acceso a su whatsapp o su password de fb o gmail no se te agradesco si me contestas, gracias

Precisamente muchos de esos lectores se acercan al blog de Chema Alonso buscando alguna técnica secreta para cometer delitos, como espiar el WhatsApp de un vecino, acceder al Facebook de una novia, hackear el correo de un jefe, alterar las notas de un examen…

En sus conferencias es habitual que Chema utilice algunos de esos mensajes, tuits o wasaps que recibe casi a diario, doy fe. Sobre todo inmediatamente después de alguna intervención televisiva. Y más allá de lo hilarante de algunas peticiones, este fenómeno ilustra de maravilla la percepción tan distorsionada que el gran público tiene sobre lo que es un hacker.

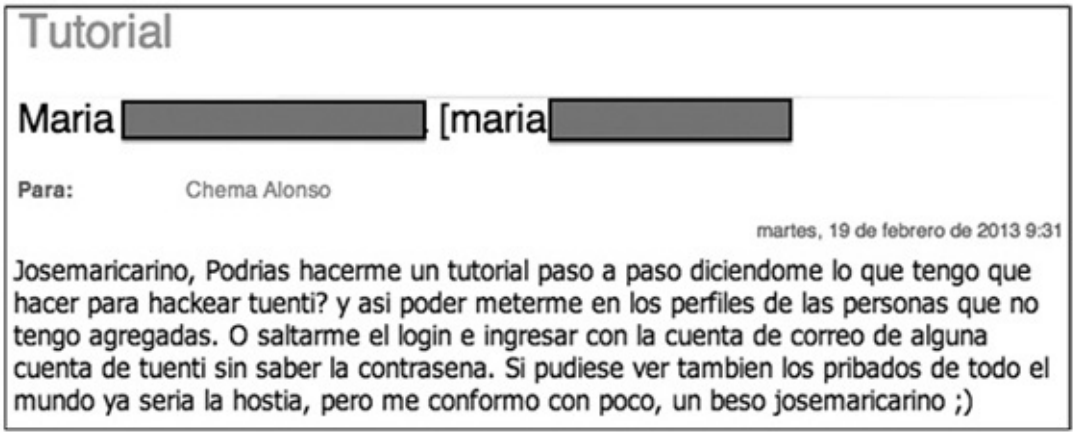
—Recibes miles de emails de personas que te piden las cosas más inverosímiles, casi todas delictivas. Supongo que eso refleja la imagen que tiene el público sobre vosotros, los hackers… ¿Cuáles han sido los más sorprendentes que has recibido? —le pregunto intentando tirarle de la lengua.

—Peticiones de todo tipo, desde chavales que quieren que les consiga monedas para un juego, gente que quiere que hackee el Facebook/Gmail/WhatsApp de una persona y hasta atacar a empresas de la competencia. Mucha gente quiere solucionar sus problemas haciendo este tipo de ilegalidades. Tengo cientos, si no miles, de estas peticiones. —Mientras me respondía, buscaba algún ejemplo con el navegador de su teléfono y al abrir su Twitter… ¡Sorpresa! Justo en ese instante acababa de entrarle una nueva solicitud—. Mira, según te contesto me ha llegado este tuit.

Me lo lee en alto: «Chema, una pregunta, necesito hackear un móvil por tema de infidelidad. ¿Cómo lo puedo hacer? ¿Me puedes ayudar?».

El Maligno ha dedicado muchos posts en su blog a este tipo de mensajes, explicando una y otra y otra vez que un hacker no comete delitos. Y espiar cuentas ajenas o alterar calificaciones, es un delito.[259]

Pero de todas, sin duda mi preferida es la del «escarmiento maligno» que dio a una señorita, una tal María, que pretendía acceder al Tuenti de una amiga para espiar sus mensajes privados…


Tutorial

Maria [redacted] [maria[redacted]

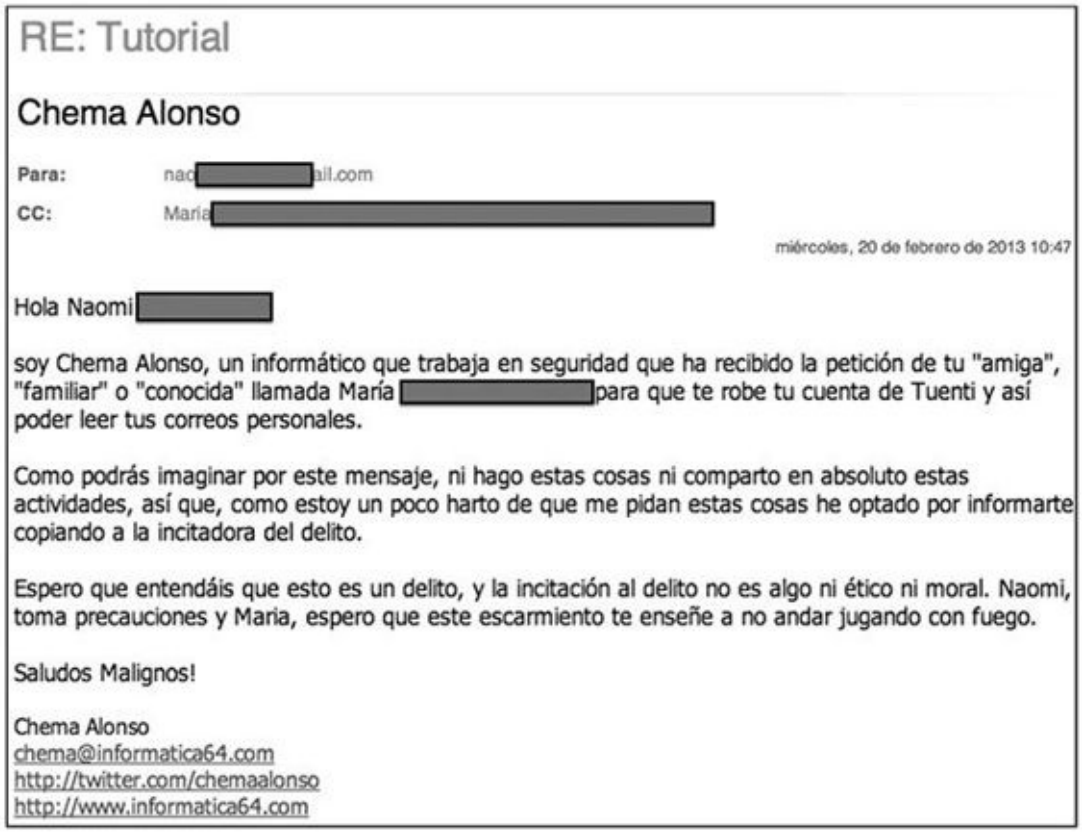
Para: Chema Alonso

martes, 19 de febrero de 2013 9:31

Josemaricarino, Podrias hacerme un tutorial paso a paso diciendome lo que tengo que hacer para hackear tuenti? y asi poder meterme en los perfiles de las personas que no tengo agregadas. O saltarme el login e ingresar con la cuenta de correo de alguna cuenta de tuenti sin saber la contrasena. Si pudiese ver tambien los pribados de todo el mundo ya seria la hostia, pero me conformo con poco, un beso josemaricarino ;)

Chema cruzó un email con esta chica para ver si el encargo iba a por «algún perfil en concreto» y la tal María coló como una inocente: le pasó el email de su amiga Naomi y hasta tuvo el cuajo de despedirse de Chema con un «Sé que no te dedicas a comercializar con estas cosas. Así que dejaré que me lo expliques gratis». Le esperaba un email maligno… Chema informó a la víctima, con copia a la inductora del delito, la cual no encajó con demasiada deportividad que el hacker (al que la tal María debía considerar un delincuente altruista que hackea «cosas» por amor al bit) hubiese traicionado su confianza informando a su amiga de sus tentativas de hackearle el Tuenti.[260]

Casos como el de María nos pueden parecer divertidos, pero basta echar un vistazo a la cantidad de solicitudes similares que recibe Chema Alonso, y otros muchos hackers, para darte cuenta de lo importante que es fortalecer tus contraseñas, y cambiarlas con regularidad. Porque seguro que tienes un@ amig@, novi@, familiar o compañer@ que en estos momentos está buscando el modo de acceder a tus emails, perfiles sociales o fotos, para cotillear un poco. Y si no puede hacerlo por sus medios, escribirá a personas como Chema Alonso para que le ayuden. Arriesgándose a recibir un escarmiento como el de María.



RE: Tutorial

Chema Alonso

Para: nac[redacted]il.com

CC: Maria[redacted]

miércoles, 20 de febrero de 2013 10:47

Hola Naomi[redacted]

soy Chema Alonso, un informático que trabaja en seguridad que ha recibido la petición de tu "amiga", "familiar" o "conocida" llamada María[redacted]para que te robe tu cuenta de Tuenti y así poder leer tus correos personales.

Como podrás imaginar por este mensaje, ni hago estas cosas ni comparto en absoluto estas actividades, así que, como estoy un poco harto de que me pidan estas cosas he optado por informarte copiando a la incitadora del delito.

Espero que entendáis que esto es un delito, y la incitación al delito no es algo ni ético ni moral. Naomi, toma precauciones y Maria, espero que este escarmiento te enseñe a no andar jugando con fuego.

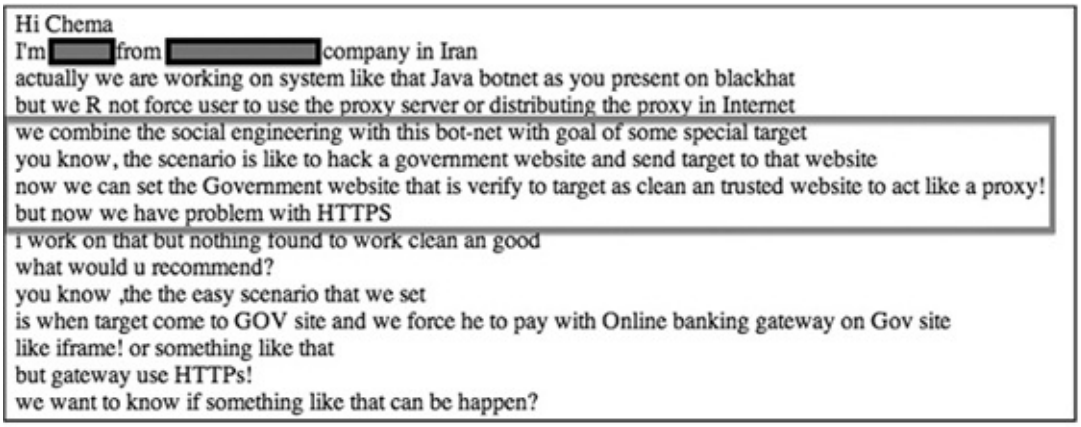
Saludos Malignos!

Chema Alonso
chema@informatica64.com
http://twitter.com/chemaalonso
http://www.informatica64.com

Sin embargo, este tipo de requerimientos no son los más inquietantes. El Maligno ha recibido proposiciones mucho más indecentes, para realizar maldades mucho más diabólicas…

—Como cosa excepcionalmente curiosa —me explica Chema—, después de dar la charla en Black Hat USA 2012 en Las Vegas titulada «Owning Bad Guys (and mafia) Using JavaScript Botnets», en la que contaba cómo montamos una *botnet* en JavaScript, con un servidor proxy anónimo fraudulento publicado en internet, me llegaron dos peticiones. Una de un Gobierno que quería que le ayudara a montar en Oriente Medio un sistema similar, y otra de un correo de Yahoo «raro, raro» que quería comprar todos los datos que hubiéramos recolectado con ese servidor proxy. Miedo me dio…[261]

Por supuesto la *botnet* que montaron Chema y sus amigos en TOR no tenía como objetivo delinquir, sino que formaba parte de una investigación fascinante sobre quién busca conectarse a través de un *proxy* anónimo en TOR, y para qué… Pero que un Gobierno centroafricano intentase contratar a un hacker español para desarrollar una red que monitorizase la actividad en internet de sus ciudadanos es un ejemplo excelente de que, más allá de paranoias sobre conspiraciones gubernamentales para espiar nuestra vida digital, esas cosas existen. Y a veces no solo son nuestros amigos, exnovios o compañeros, quienes quieren acceder ilegalmente a nuestro ordenador o a nuestro teléfono…


Hi Chema
I'm [redacted] from [redacted] company in Iran
actually we are working on system like that Java botnet as you present on blackhat
but we R not force user to use the proxy server or distributing the proxy in Internet
we combine the social engineering with this bot-net with goal of some special target
you know, the scenario is like to hack a government website and send target to that website
now we can set the Government website that is verify to target as clean an trusted website to act like a proxy!
but now we have problem with HTTPS
I work on that but nothing found to work clean an good
what would u recommend?
you know ,the the easy scenario that we set
is when target come to GOV site and we force he to pay with Online banking gateway on Gov site
like iframe! or something like that
but gateway use HTTPs!
we want to know if something like that can be happen?

Paradójicamente, y a pesar de que en pleno siglo XXI los periodistas deberíamos ser los primeros en estar familiarizados con lo que significa internet y los hackers, todavía tenemos pendiente esa asignatura. Yo mismo, un usuario muy activo de internet, estaba lleno de prejuicios al iniciar este viaje. Y sospecho que la mayoría de mis colegas no están mucho más duchos que yo en el tema. Quizá por eso se publican tantas inexactitudes a diario en los medios en torno a la palabra *hacker*.

—¿Y por qué un periodista con tanta cultura como Federico Jiménez Losantos arremetió contra ti tras tu encuentro con el rey Felipe VI? ¿Acaso en pleno siglo XXI los periodistas más influyentes del país siguen sin saber qué sois los hackers?

—Esta es una de las historias más curiosas de mi vida, y te juro que me han pasado muchas. Era el Mobile World Congress de 2015 y le habíamos preparado un juego al rey en el que tenía que falsificar la firma de César Alierta (como conseguí la firma de César para que la pudiéramos meter en el juego es otra aventura que cuento en la intimidad, porque casi se nos cae el experimento a veinticuatro horas vista).

»Cuando llegó el rey, yo le estaba esperando como soy yo. Con mi gorro y sin afeitar, que había sido un fin de semana duro. Llegó en comitiva con César Alierta, José María Álvarez-Pallete, el ministro Soria y Artur Mas a jugar y yo los atendí. Nos reímos, la demo funcionó y a Casa Real le gustó el momento, así que subió el vídeo a YouTube. El equipo de comunicación de Telefónica eligió esta foto —me dice Chema mientras utiliza el navegador de su teléfono para buscar la imagen y cedérmela amablemente para este libro— para pasarla a los medios de comunicación y en algún diario fue portada. Esto cayó en la redacción de Federico Jiménez Losantos que en antena dijo: "¿Qué hacker? Este es un quinqui ciberdelincuente del 15-M".[262]

»Te puedes imaginar, al rato me estaban enviando tuits, mensajes de correo y llamando para contarme la historia, así que contacté con el equipo de comunicación de Telefónica y les pedí el teléfono de la radio de Federico. Allí hablé con su subdirectora que me dijo: "Es que no te has quitado el gorro ante el rey". En ese momento aproveché para explicarle que no me lo quité, primero porque es mi imagen y si en el *badge* de Telefónica me dejan llevarlo y lo llevo siempre, no voy a quitármelo y, en segundo lugar, porque soy doctor por la Universidad y por ley, los doctores no estamos obligados a descubrirnos ante el rey. De ahí viene el birrete. Eso

fue muy divertido. Luego me dijeron que si tenía mirada agresiva, para lo que les pasé el vídeo de YouTube que había subido Casa Real. Al final, por WhatsApp me invitaron al programa, pero decliné la oferta. En la comunidad hacker tenemos un dicho *Don't feed the Troll.*

Es verdad. Doy fe. Chema buscó un instante en su teléfono y me mostró el WhatsApp de la subdirectora del programa. Aunque lo cierto es que no encontré las disculpas en ninguna parte del mensaje…

—Por favor, y no te robo más tiempo, aunque sea en una frase rápida… ¿Qué te sugieren estos nombres?: Edward Snowden.

—Yo creo que la historia le tratará como un héroe por haber abierto los ojos al mundo y le acabarán reconociendo.

—Julian Assange o Wikileaks.

—Me sugiere pena ver cómo el mundo haya dejado a un Gobierno arrestar a una persona sin juicio y que ningún país del primer mundo pelee por llevar su caso a un lugar neutral con garantías.

—Hervé Falciani.

—Creo que puso una pica contra algo que en mi opinión personal debe desaparecer. Los paraísos fiscales. El capitalismo podría funcionar cien veces mejor y estar al servicio de la sociedad si se acabaran los paraísos fiscales.

—CiberBerkut.

—No he seguido mucho este asunto, pero creo que el hacktivismo para desvelar cosas así siempre ayuda a madurar a las sociedades.

Chema comenzó a mirar de reojo su reloj de pulsera. Mala señal. Lo había sacado de su puesto de trabajo y está abusando de su generosidad robándole más tiempo del que podía darme. Sin embargo, en ningún momento hizo comentario alguno. Había tantas cosas que me gustaría preguntarle… pero decidí dejarlo ahí. Era nuestro primer encuentro personal a solas, después habría otros…

—Solo una más. Tú estás muy vinculado a los medios. Creo que todos mis compañeros de la prensa tienen solo tu número en la H de hacker en su agenda… Durante tres años has conseguido que «el Maligno» se manifestase desde los micrófonos de las mañanas de la COPE, con Javi Nieves, sin que lo exorcizaran. Así que estás al día de todo lo que pasa en la comunidad… ¿Hacia dónde va? ¿Cómo imaginas internet o nuestra vida digital en 2025?

—La verdad es que es una pregunta complicada. Los jóvenes cambian el paradigma y la dirección día tras día, generación tras generación. A mí, cosas como Tinder se me hubieran hecho impensables en mi generación, y ese tabú está roto hoy en día. Yo creo que las sociedades conectadas, el humano conectado, el coche conectado, el cerebro conectado a la realidad aumentada o la telepatía van a traernos escenarios apasionantes. Un paso más hacia Matrix o un paso más hacia un mundo en el que la Inteligencia Artificial nos domine un poco más. Yo decía en broma en la radio que estamos en la última generación de smartphones en los que nosotros

seamos quienes los gestionemos. En el futuro, ellos nos dirán qué hacer y cuándo.

JULIO DE 2015
MARKOS ES PEDRO

Göring has only got one ball
Hitler's [are] so very small
Himmler's so very similar
And Goebbels has noebbels at all!

Canción popular entre los ejércitos de la Commonwealth y de los Estados Unidos, tras la derrota del Reich en la Segunda Guerra Mundial

Cualquier periodista lo sabe. Recoges lo que hayas sembrado en tu carrera. Los compañeros que queman a sus fuentes por una primicia suelen tener una gran exclusiva, pero pierden para siempre a sus informadores. Sin embargo, si los respetan, tarde o temprano volverán a coincidir en el camino y podrán volver a contar con su ayuda. Arrieros somos…

Al final es cuestión de contactos. La «Teoría de los seis grados de separación», propuesta en 1930 por el escritor húngaro Frigyes Karinthy, sugiere que cualquier ser humano está relacionado con todos los habitantes de la tierra a través de una cadena que no tiene más de cinco intermediarios. Es decir, que el mundo es un pañuelo, con seis grados de separación entre todos nosotros.

Según Karinthy, cada persona conoce, entre amigos, familiares, vecinos y compañeros, una media de cien personas. Cada una de ellos relacionada con otras cien, lo que hacen 10.000. A su vez relacionadas con otro millón de personas… y así exponencialmente. Pero en 2015 Facebook pulverizó la teoría de Karinthy. Un estudio realizado por la Universidad de Milán asegura que la distancia entre dos personas ubicadas en cualquier parte del mudo se reduce a solo 4,74 pasos, y no a seis como sugería Frigyes. El estudio asegura que la tendencia es que, según aumentan los usuarios de Facebook, el número de pasos del proceso disminuye, y que si se limita a contactos de un mismo país, el proceso se puede completar con solo tres pasos (cuatro si se cuenta al usuario que inicia el proceso).

La Universidad de Milán ha investigado las relaciones de amistad de 721 millones de estos usuarios, un 10% de la población mundial, como muestra para demostrar la popular teoría de los seis grados de separación. Y para su sorpresa la distancia era menor: «Hemos encontrado que la teoría de los seis grados en realidad exagera el número de enlaces entre los usuarios. El 99,6% de las parejas de usuarios analizados están conectados por cinco grados y el 92% lo hace a través de cuatro grados», explicó Facebook en su blog oficial haciéndose eco del estudio italiano. Según la red social, ahora los

usuarios pueden conectarse con cuatro contactos, y todo gracias a las posibilidades que ha creado un servicio como Facebook.[263]

Aplicado a este caso, yo tenía que conocer necesariamente a alguien, que conociese a alguien, que tuviese acceso a la base de datos de la multinacional donde trabajaba MarkoSS88. Solo era cuestión de tiempo y de insistencia.

Pasaban los meses y todos continuábamos pendientes de que los seis (o 4,74) grados de separación fuesen algo más que una teoría. Y por fin, una luminosa mañana de verano, llegó la información. No por una fuente, sino por varias. Ronin lo tenía a dos grados de Linkedin. Es decir, no se conocían directamente, pero compartían contactos. Israel Córdoba lo tenía aún más cerca. Lo conocía en persona, aunque con quien se relacionaba normalmente era con su jefe en la empresa… Karinthy tenía razón. Y lo supimos cuando un amigo de un buen amigo resultó ser un empleado de la misma multinacional. El teléfono de Markos había sido derivado por la empresa a uno de sus ejecutivos: Pedro S. Ya lo teníamos.

Pedro se diplomó en Informática en la Universidad de Salamanca, con un máster en desarrollo web. Nació en 1969. Durante más de ocho años fue jefe de proyecto de una de las empresas más importantes de España, gestionando contratos de software y operadores, antes de ser fichado por la multinacional donde trabaja ahora.

—Está en comunicación —me explicó Israel—, o sea, que sabe perfectamente cómo borrar su rastro en internet.

Rafa tuvo razón desde el principio. Los conocimientos informáticos de MarkoSS88 no eran una casualidad…

Ronin, que había compilado todas nuestras pesquisas en un informe monumental de cincuenta páginas, nos echó una mano para rastrear la vida digital de Pedro. Pero resultó un hueso duro de roer.

Pedro se había ocupado de borrar todo rastro en la red, probablemente cuando decidió convertirse en MarkoSS88. Pero aunque era muy bueno, Ronin era mejor.

El ejecutivo no usaba Twitter, pero sí tenía Linkedin y un perfil en Facebook cerrado a sus poco más de setenta amigos. Pedro era más prudente que Jordi… Ronin tuvo que echar mano de todos sus conocimientos para rastrear en Bing, Yahoo o Ask, anuncios, boletines oficiales o publicaciones académicas. Y los encontró.

No es un consejo gratuito. Todo lo que sube a la red se queda en la red. Las advertencias de Israel Córdoba, Selva Orejón o Angelucho en las conferencias de X1Red+Segura no eran un farol. Si sabes cómo buscar, encuentras. Y un dato, por insignificante que sea, unido a otro, se convierte en una pista, y una pista en un indicio, y un indicio en una prueba.

Encontramos las referencias de reuniones profesionales de informáticos en las que había participado Pedro, reseñas de sus conferencias, denuncias por unos arañazos y robo en su coche, sus teléfonos fijos y móviles (como Markos, no usa WhatsApp), el perfil social de su esposa, que por cierto es técnico de Sistemas y Telecomunicaciones, y técnico en Marketing Digital y Redes Sociales en una empresa periodística, etcétera.

Los dos viven, con su hijo, en Moratalaz donde se concentraba la geolocalización de los tuits de MarkoSS88, y a un tiro de piedra del campus de Vicálvaro, donde comenzó esta pesadilla que ahora llegaba a su fin. En una especie de fortín blindado con portero físico las veinticuatro horas, plagado de cámaras de videovigilancia rodeando el perímetro, y con dos porteros electrónicos para acceder al edificio. Las ventanas de su piso dan al patio interior. Supongo que allí se siente protegido y a salvo. Y cree que puede salir al mundo a través de las redes, para manipular, asustar y mentir a sus víctimas. Pero mis amigos le han demostrado que se equivoca. Ni en ese búnker de Moratalaz ha podido esconderse.

MarkoSS88 es muchas cosas. Casi todas malas. Pero sobre todo es la prueba más evidente, el ejemplo más gráfico, de los peligros insospechados e inimaginables, que podemos toparnos en la red. Aunque no nos los busquemos adrede. Basta con que no nos protejamos…

Ahora llegaba la parte más desagradable. Informar a sus víctimas.

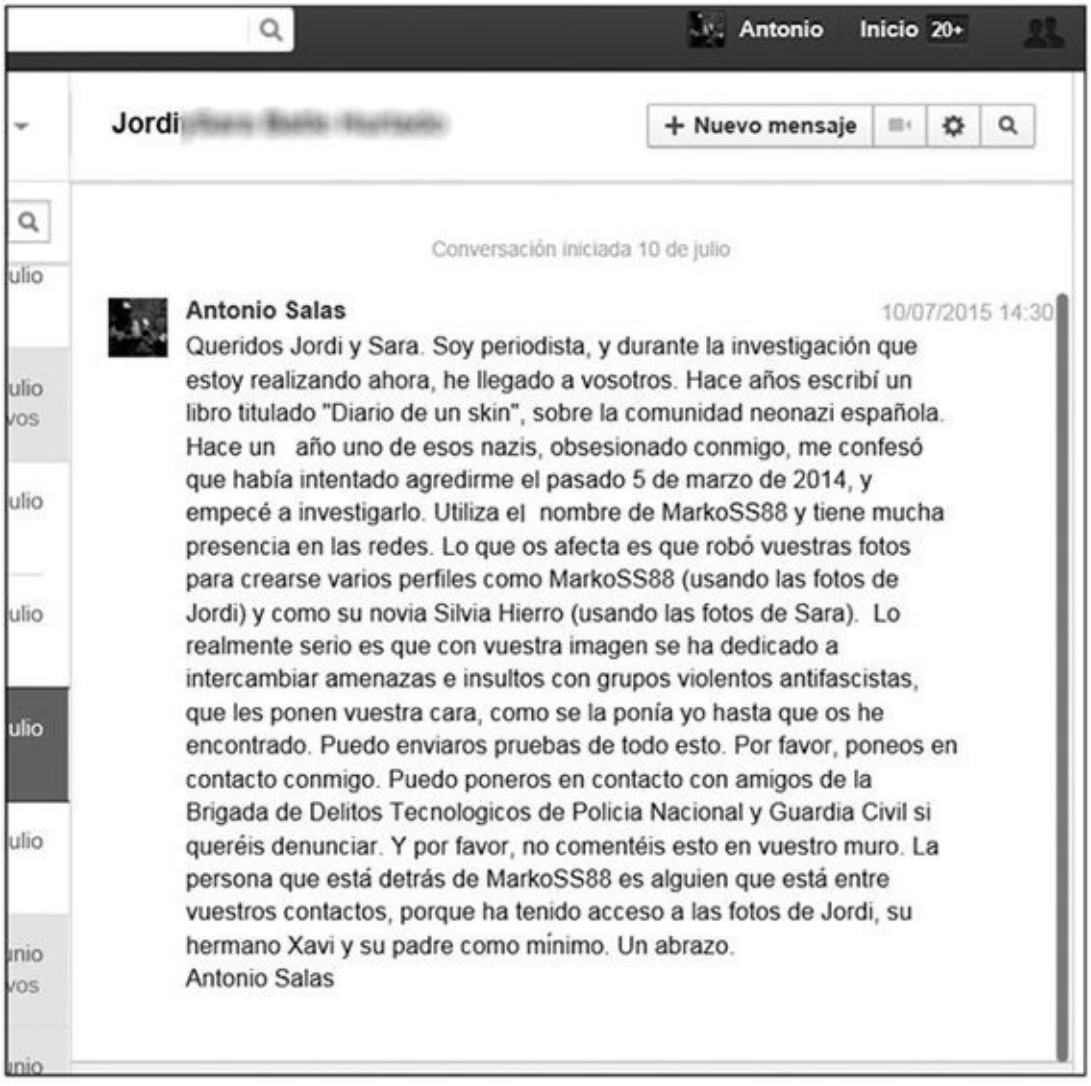
Marga y Soraya reaccionaron de forma radicalmente opuesta. La primera, con indignación. En cuanto vio el perfil de Jordi y Sara, y descubrió que su amigo del alma, aquel por el que había derramado tantas lágrimas, aquel que había buscado por tierra, mar y aire cuando desapareció, aquel con el que había compartido tantas noches de confidencias en la red era un fraude, se sintió estafada.

Soraya, sin embargo, enamorada hasta el tuétano de una cara que no se correspondía con los emails, sms y chats que le habían devuelto la ilusión, tras una relación anterior muy tormentosa, negaba la mayor. No podía ser. Era imposible. Jamás había visto en persona a Markos, ni siquiera habían hablado por teléfono hasta que nosotros lo descubrimos y comenzó a usar el Skype, modificando su voz para parecer más joven con un programa como el que uso yo en las entrevistas. Pero daba igual.

La historia era tan rocambolesca que cuando Markos nos aseguraba a todos que estaba muriéndose de hambre en una pensión de mala muerte en Mallorca, Soraya se cogió un avión sin avisarle, se plantó en Palma y alquiló un hotel para poder ver por fin a su amado en persona. Pero Markos no apareció. Inventó una nueva detención y una nueva paliza, y Soraya tuvo que regresar a la península sin haber visto ni escuchado a su novio virtual. Es lógico, en esos momentos Markos —es decir, Pedro— estaba en Madrid,

con su esposa e hijo y atendiendo sus responsabilidades como informático de una multinacional. Con Soraya solo quería tener cibersexo… supongo que al final este es el triste móvil de toda esta mascarada. Un perfil atractivo en internet para que un casi cincuentón pueda tener cibersexo con chicas que podían ser sus hijas… Ni siquiera es original. Antes que Soraya hubo otras. Y antes que Markos, otros miserables, como Roi, inventaron perfiles falsos para seducir a mujeres en la red.

En cuanto a Jordi y Sara, les escribí un email a través de Facebook, intentando explicarles lo que había ocurrido. Cómo un ladrón de vidas había hurtado sus fotos para construir una identidad ficticia. Una identidad conflictiva que no creo exagerar si afirmo que pudo haber puesto en peligro sus vidas.



La reacción de Markos no se hizo esperar. Yo no había vuelto a contestar sus correos desde que había descubierto el engaño. Pero cuando la verdad salió a la luz, retomó su identidad como MarkoSS88, el peligroso asesino convicto por homicidio para amenazarnos de muerte, tanto a Marga como a mí, creyendo que volvería a funcionarle. Solo que sus bravatas ya no me

asustaban. Le contesté, como siempre lo hice, de corazón. Fue la última vez que perdí mi tiempo con él:

No sé cómo decirte esto, pero vale ya… Se acabó. No tiene sentido seguir con todo esto. Yo no te mentí nunca, todo lo que te dije era cierto. Me preocupé por ti, igual que M. (Marga) que no se merece lo que estás haciendo. Como no se lo merece Soraya, ni Rocío, ni Pilar, ni Estefanía, etc.

Sé por qué haces lo que haces. No lo apruebo, pero lo entiendo. Eres un tío. Y si realmente hubieses leído los libros que te mandé, desinteresadamente, sabrías cómo pienso sobre nosotros.

Al principio me engañaste. Es verdad. Te creí. Quería creerte, porque estaba seguro de que si eras quien decías ser, podría convencerte para dejar el NS. Tú que jamás has sido nazi… Y todo lo que te dije en mis correos era verdad.

Cuando te envié mis libros, cuando te ofrecí dinero, cuando perdí mi tiempo preguntando a polis, médicos y enfermeras si sabían algo de ti, lo hice de corazón. Como Marga, como Soraya. Quizá por eso me tomaste por imbécil. Y eso no me molesta. No me preocupa que me tomen por gilipollas, porque eso solo delata la estupidez de quien lo hace. Lo que no perdono es que me hagan perder el tiempo.

Eres bueno, muy bueno. Meticuloso, constante, creativo… un buen informático. Pero yo soy mejor en lo mío. Y no paro. Puedo tomarme todo el tiempo del mundo. Y tu problema, tu gran problema, es que no has tenido suerte. Si me hubieses pillado en cualquier otra investigación, te habría salido bien. Pero llevo dos años metido en el mundo del hacking, la seguridad informática y el hacktivismo. Durante estos años mi vida ha sido Navaja Negra, No cON Name, CyberCamp, X1Red+Segura, etcétera. Mis colegas en estos años son César o Angelucho, del GDT de la UCO, Silvia y David, de la BIT del CNP, los peritos de INCIBE, el CCN o el CNI, y toda la comunidad hacker. Incluyendo a los hacktivistas de Anónymous, Wikileaks, The Jester…

Cuando hace unos meses te dije que tenía pendientes varios viajes a Moscú (Snowden), a Londres (Assange), a Italia (Falciani), etcétera, tampoco te mentía. Nunca lo he hecho. Pero tú no podías imaginarte que el objeto de mi nuevo trabajo era tu mundo. La ciberdelincuencia.

Antes de publicar tu entrevista en mi blog, intenté llamarte a los teléfonos que me diste, los dos derivados, tanto el de tu empresa como el de Parlem. Quería darte una oportunidad de explicarte de viva voz. Pero ahora entiendo por qué están derivados y para qué los usas realmente. Estuve en tu casa. La publicidad que pillaste en tu buzón hace unos meses la puse yo. Quería ver con quién vivías…

Es inútil que intentes borrar tu rastro. Tú mejor que nadie deberías saber que todo lo que sube a la red se queda en la red. Y todos tus perfiles están grabados. De hecho, yo usé en la entrevista, estúpido de mí, creyendo que te beneficiaba, muchas capturas de tus Facebook, Twitter, Telegram, y de los de «Silvia», protegiendo vuestras caras.

En el libro encontrarás toda tu historia. Serás uno más de los casos que relato…

Su reacción era previsible. Durante las siguientes semanas Markos intentó hacer desaparecer todas las huellas de sus delitos en la red. Dio de baja sus perfiles y los de su novia Silvia Hierro en las redes sociales, intentó hacer desaparecer todas las fotografías robadas a Jordi y su familia, asociadas a su identidad como MarkoSS88.

Consiguió que todos los emails que me había enviado desapareciesen de la carpeta de correo de mi buzón de email, de hecho creí que me había hackeado el correo, pero se limitó a acceder al servidor de Gmail para borrar los mensajes enviados, y consiguió que nadie pudiese ver la entrevista, ilustrada con las capturas de pantalla donde aparece con la cara de Jordi, porque «casualmente» alguien tiró mi página web, y también denunciaron mi

perfil *Diario de un skin* en Facebook, que desapareció misteriosamente de internet. Tuve que abrir una página nueva: www.antonio-salas.com y un nuevo blog: www.loshombresquesusurranalasmaquinas.blogspot.com.

Pero fue inútil. Todos sus emails estaban salvados, todos sus perfiles sociales grabados, y todas las evidencias de su comportamiento recogidas en los informes realizados por mis amigos, que inmediatamente facilité al ya comandante César Lorenzana para que los pusiese en conocimiento de la Fiscalía, con la esperanza de que esta actúe de oficio contra el ladrón de vidas. La historia del cibernazi MarkoSS88 había llegado a su fin.

Epílogo

> «Mi nombre es Avery Ryan. Fui víctima de un ciberdelito. Al igual que tú también publicaba en las redes sociales. Comprobaba mis cuentas corrientes por internet, e incluso guardaba los archivos confidenciales de mi consulta de psicología en mi ordenador. Pero entonces me hackearon… Mi investigación me llevó al FBI, donde me uní a un equipo de ciberexpertos en una guerra contra un nuevo tipo de criminales que se ocultan en la Deep Web. Que se infiltran en nuestras vidas diarias de formas inimaginables. Sin rostro, sin nombre. Al acecho en el interior de nuestros dispositivos. A una sola tecla de distancia. Te puede pasar a ti.»
>
> Cabecera de la serie *CSI: Cyber,* 2015

El lunes 24 de agosto de 2015 ocurrió algo mágico: uno de cada siete habitantes del planeta se conectó a Facebook en algún momento del día. Era la primera vez que ocurría. Mil millones de seres humanos compartiendo el mismo día la misma red social. Ese es el poder de internet.[264]

Por supuesto, eso no significa que, por primera vez, los seres humanos estemos unidos para corregir todos los errores de nuestros líderes políticos. Pero al menos ahora tenemos la oportunidad de hacerlo. Por primera vez en la historia existe una herramienta que nos permite comunicarnos con miles de millones de personas, en otros puntos de la tierra, sin mediación de los gobiernos. Que nos facilita el acceso a toda la información que podamos necesitar. Como si nos hubiésemos mudado a la sala central de la Biblioteca de Alejandría.

Internet nos ha dado un gran poder. Y, cómo no, eso incomoda a quienes consideran que los ciudadanos no están capacitados para ejercerlo. Por eso crean normas, leyes y reglas, que restrinjan en lo posible nuestro acceso a esa fuerza que es la red. Y por eso hacktivistas como Lord Epsylon escriben nuevos códigos y diseñan herramientas para burlar el control de los gobiernos en la red.

Argumentan, y tienen razón, que la red es peligrosa. Que la industria del cibercrimen ya mueve más dinero que el narcotráfico, la trata de blancas o el tráfico de armas. Y que mientras nuestra generación no concluya la inmigración a la cultura digital, estaremos desprotegidos. Pretenden que deleguemos en ellos nuestra seguridad digital, pero me temo que todavía no están cualificados para protegernos.

El cibercrimen avanza más deprisa que las leyes. Y de la misma forma en que un revólver de un policía municipal francés no puede competir contra los AK-47 automáticos de dos terroristas yihadistas en París, el presupuesto que manejan los ciberdelincuentes supera con mucho la tecnología de que disponen los ciberpolicías. Así que vamos a tener que poner algo de nuestra parte…

Yo sé que, en cuanto salgo del garaje y accedo a la carretera, asumo una serie de

riesgos. Algunos son de mi total responsabilidad. Si no me pongo el cinturón, si no paso la ITV, si excedo los límites de velocidad, es más fácil que sufra un accidente. Otros factores no dependen de mí: puedo cruzarme con un conductor ebrio, puedo encontrar aceite o gravilla en una curva, puedo ser víctima de las inclemencias meteorológicas. Pero en todo momento soy consciente de que incorporarse al tráfico implica estar atento a la conducción. Sin embargo, cuando encendemos el ordenador y entramos en la red suele embargarnos una temeraria sensación de invulnerabilidad, solo porque navegamos desde un lugar físico que nos resulta protector: nuestra casa, nuestra oficina, nuestro teléfono móvil… Nos mentimos a nosotros mismos.

Iniciativas como X1Red+Segura nos enseñan que por desgracia esa sensación de seguridad es totalmente ficticia. Que ahí dentro, en la red, acechan muchos peligros que no imaginamos. Y que las medidas de protección no existen… al menos en un 100%. Durante la terrible pandemia de 1918, que causó entre 50 y 100 millones de muertos en todo el mundo, la gente se protegía del contagio de la Gripe Española tapándose la nariz y la boca con un pañuelo, pero el virus era tan pequeñito que podía filtrarse por el trenzado de la tela llegando a las fosas nasales y a las mucosas y contagiando a una nueva víctima. Y los virus informáticos son aún menores. Por eso requieren medidas mucho más efectivas.

Aprendí hace mucho a no delegar mi seguridad en terceros. Ni en la red ni fuera de ella. No sabía nada de informática cuando me convertí en el webmaster de Carlos el Chacal, o cuando heredé la gestión de Hizbullah Venezuela en la red, así que me limité a usar el sentido común y no me fue mal. Pude haberme convertido en una muesca más en las estadísticas policiales, pero esa experiencia me convenció de que si eres prudente, un poco desconfiado y te lo piensas dos veces antes de pulsar el botón de Enter, puedes ahorrarte muchos disgustos. No hace falta ser un hacker para disfrutar de la red. Tan solo evitemos ser inconscientes al utilizarla, porque no siempre tendremos una segunda oportunidad para enmendar el fallo.

No podemos esperar compasión del banco si nos retrasamos en el pago de la hipoteca. Ni del Ministerio de Hacienda si erramos en la declaración fiscal. Ni del agente de la tráfico cuando excedemos el límite de velocidad o circulamos sin cinturón… Pues tampoco podemos esperar ninguna compasión de los ciberdelincuentes que ataquen nuestro ordenador personal, nuestro teléfono móvil o nuestras cuentas de correo o red social. Te sacarán todo lo que puedan sin el menor asomo de piedad. Créeme. Lo he visto. Y ni siquiera dudarán un ápice en poner tu propia vida en peligro, si con eso satisfacen sus objetivos. Como hizo MarkoSS88.

Cuando estés solo o sola en tu cuarto, ante el teclado del ordenador, la tablet o del teléfono, recuerda que nadie va a protegerte. Dependes de ti. Solo tú podrás decidir si aceptas a ese nuevo amigo en tu red social. Si abres ese correo prometedor. Si visitas tal o cual página. Si subes tal o cual foto, o se la envías a esa persona en la que hoy confías (a saber mañana). Nadie podrá pulsar el botón de Enviar, o de Suprimir en tu lugar. Así que decidas lo que decidas, medítalo un momento. Porque tu decisión es

irreversible. La red es una criatura de apetito feroz. Todo lo que entra en ella se queda en ella. Para siempre. El derecho al olvido es una definición legal, pero no una realidad. Todas las víctimas del Celebgate lo saben. Y ahora tú también.

Has salido a la carretera. Una autopista de millones de carriles, de senderos ocultos en una red escondida. Los compañeros de Angelucho, destinados en la Dirección General de Tráfico, saben que las autopistas son plurales. Por ellas circulan ambulancias y coches de bomberos, asistencia en carretera y patrullas de policía… Pero también las transitan narcotraficantes con los maleteros llenos de droga, sicarios buscando a su víctima, conductores suicidas o borrachos… Y a veces no depende de nosotros que nos crucemos en el camino de los primeros o de los segundos. Hoy ocurre lo mismo con las autopistas de la red. Las transita la información, el ocio, las relaciones. Pero también el cibercrimen, los espías y terroristas, y el *cyberbullying*, porque internet también es un altavoz de matones que gritan tras nombres ficticios.

¿Qué vas a hacer?

Sé que tu red social es importante para ti. Es tu tarjeta de visita ante el mundo. Donde enseñas lo mejor de ti. Pero no es real. Lo que ves en la pantalla solo es un código binario de 1 y 0 que no te representa. Los puñetazos duelen. Las patadas duelen. Pero los insultos y las burlas en Tuenti o en Twitter solo hacen daño si tú se lo permites. Yo recibo el odio de los skins, como MarkoSS88, y también de los puteros, terroristas o proxenetas casi a diario. Y al principio sentía miedo cada vez que leía sus amenazas, me incomodaban sus insultos. Hasta que decidí no leerlos. Y entonces el dolor desapareció. Sé que siguen ahí, gritando, maldiciéndome. Tratando de hacerme daño. Pero si alguien llama al telefonillo de tu portero automático para insultarte, y tú cuelgas, solo conseguirá quedarse afónico. Que trague su propia bilis, gritando a un micro apagado. No permitas que te afecte, como hicieron Aranzazu, Mónica o Carla. No hasta ese punto. No merece la pena. No lo vale.

Y ante la primera amenaza, no les des la oportunidad de que se crezcan. Porque si cedes una vez a su chantaje, creerán que cederás siempre. Por mucho que te avergüence el secreto que amenazan con divulgar, sabes que no puedes creer en sus promesas. Los miserables no tienen palabra. Pero personas que escogieron dedicar su vida a proteger y servir, y que además están cualificados para ello, están deseando ayudarte. Porque eso es lo que les hace sentirse útiles. Lo que da sentido a su trabajo. Y esas personas —como César Lorenzana, David Pérez, Angelucho, Esther Aren, Manuel Viota, Silvia Barrera y todos sus compañeros— se van a dejar la piel para ayudarte y tienen la capacidad, los recursos y la experiencia para que esa situación que ahora te atormenta se zanje antes de ir a peor. Y créeme: si no tomas medidas, irá a peor. A veces es preferible pasar por un momento incómodo, en una comisaría, un juzgado o una comandancia, que toda una vida con miedo. Te lo prometo. Lo sé por experiencia.

¿Y vosotros, padres? Existen muchos programas parentales para supervisar la navegación de los menores, pero la mayoría de los hackers que he conocido

coinciden en que las prohibiciones no suelen funcionar. Es decir, puedes capar el navegador de su ordenador o teléfono para que no entre en ciertas páginas peligrosas, pero cada día aparecen millones de nuevas webs, así que la tendencia actual no es crear listas negras, sino listas blancas. Páginas donde tu hijo pueda entrar sin riesgos. Todas las demás, no serán admitidas por el navegador.

Aun así, lamento la mala noticia: que tu hijo visite páginas no deseables es el menor de tus problemas. Cada vez que esté a solas, con su teléfono móvil, estará al alcance de infinidad de riesgos, así que tal vez tengas que hacerle firmar un contrato como el que Janell Burley Hofmann pactó con sus hijos. Antes o después, tendrás que prestar atención a la vida digital de tus pequeños, o atenerte a las consecuencias de lo que pueda ocurrirles. A veces es suficiente con enseñarles a usar con criterio sus dispositivos digitales. Pero si les enseñas a mirar antes de cruzar, enséñales a pensar, antes de clickar.

Cuando algo es gratis, el producto eres tú

De lo que no podrán protegerte, ni policías, ni amigos, ni familia, es de tu propia estupidez.

Ese mensaje amable en tu buzón de correo, remitido por la web en la que compras la ropa, diciéndote que te echan de menos. Esos anuncios televisivos, protagonizados por tus deportistas o actores favoritos, invitándote a hacerte rico en un casino *online*, y deseando que seas un ludópata. Esa campaña de «el banco que piensa en las personas» y se preocupa por tu bienestar ofreciéndote la hipoteca de tus sueños. Esos anuncios de tu canal de televisión amigo, que quiere informarte y entretenerte… Todo es mentira. Les importamos una mierda. Solo quieren una cosa de nosotros: dinero. El nuestro o el que puedan generar a través de nuestras compras, audiencia o domiciliación de la nómina. Nada más.

Todos esos anuncios conmovedores, entrañables, emotivos, con tiernos gatitos, familias sonrientes, caras conocidas y días luminosos están diseñados por empresas de marketing y agencias de publicidad, que han estudiado durante décadas las tendencias sociales, para que sus productos se vendan con más eficiencia. Así que no te dejes engañar. Ni los bancos, ni los refrescos, ni la televisión, ni las firmas de moda, ni la industria del automóvil, ni el juego *online.*.. absolutamente ninguna de las ofertas que entran en tu cerebro a través de la prensa, la radio o la televisión tienen el menor interés en tu bienestar. Solo quieren que consumamos. Cada vez más. Y sobre todo, que consumamos sus productos.

Cuando un folleto publicitario incluye la palabra *gratis,* lo que quiere decir es *cebo*. ¿Por qué crees que en internet iba a ser diferente?

Los expertos en seguridad informática utilizan una expresión desoladora: «cuando el producto es gratis, el producto eres tú». Si piensas que alguien se compra un ordenador de última generación, contrata servidores, paga abultadas facturas de la luz, teléfono y línea ADSL, y se tira dieciocho horas al día subiendo películas, libros y música a internet solo para que tú te los descargues gratis, es que eres una bellísima persona, que aún cree en el altruismo desinteresado… o un imbécil. Quienes suben los libros o las pelis piratas a internet cobran con tus datos. Las *cookies* que te infectan. El rastreo de tu navegación. Y algunos, como Kim Dotcom se hicieron millonarios así.

Es probable que no te preocupe que las *cookies* de tal o cual empresa graben tus movimientos en internet y radiografíen tu perfil de consumo para luego vendérselos a cualquier empresa de *tracking.* Es posible que no te importe que tu email se sature de correo spam. O permitir que cualquiera pueda entrar en tu perfil social, para ver, dejar o llevarse lo que quiera. Pero ten en cuenta que algún día podrías pagar un precio por ello. Como Jordi y Sara.

Quizá Román Ramírez tenga razón, y los próximos años sean muy oscuros. Todavía tardaremos una generación en aprender a gestionar correctamente nuestra

vida en la red. Y la única ayuda que tendremos será la de los hackers. Ellos son quienes descubrirán nuevos sistemas de cifrado para garantizar nuestra intimidad. Encontrarán la manera de simplificar las herramientas defensivas, para que hasta un pazguato digital como yo pueda protegerse mejor. Y si alguien tan torpe como quien esto escribe es capaz de comprenderlo, tú con más razón.

Los grandes gigantes de internet, como Google, Microsoft, Apple, Facebook o Yahoo continuarán llevándose nuestros mejores cerebros, a menos que la administración y las empresas nacionales reaccionen. Y utilizarán a genios, como Lucas, para aumentar sus protocolos de seguridad, para parchear sus vulnerabilidades y para ofrecernos un producto más fiable. No porque les importe un carajo nuestro bienestar, sino porque no quieren que nos pasemos a la competencia. Nuestros datos, nuestras fotos, nuestras vidas digitales valen dinero en la industria de la información y el Big Data, y lo quieren para ellos.

Por eso seguiremos siendo víctimas de su sutil chantaje. Una vez nos hemos acostumbrado a nuestro perfil social, cambian sin descanso las condiciones de uso, sin preguntarnos si estamos de acuerdo. «Si no te gusta, cierra tu perfil y a otra cosa.» Pero no temas hacerlo. Cuando tras descubrir la identidad de MarkoSS88 mi correo fue manipulado, y mi página web y mi Facebook desaparecieron de la red, no pasó nada. Yo sigo aquí. Trabajando en lo que creo. Sigo teniendo la misma familia, los mismos amigos y los mismos enemigos. Tu vida digital no es tan importante como tu vida real.

Continuaremos recibiendo documentos interminables, de ochenta páginas, con las condiciones de cada nueva aplicación que nos bajemos. Esos que nadie lee, limitándonos a aceptar, aceptar y aceptar, aunque para una app de una linterna le estemos dando acceso al responsable a nuestros contactos, datos personales, contraseñas, etcétera. Como los pueblos indígenas, que en otra época cambiaban el oro por cuentas de vidrio o pulseras.

La buena noticia es que no importa lo que firmes, ni Google, ni Facebook, ni Apple… Nadie puede anteponerse a tus derechos básicos, ni aunque pulses mil veces en la opción «aceptar» sin haberte leído las condiciones. Podrás reclamar cuando sea tarde, pero prepárate a un largo litigio en el que tendrás que leer algo más que ochenta páginas. Ganarás. Pero con solo utilizar un poco el sentido común, te habrías ahorrado todo ese proceso. También en este sentido deberemos confiar en que los investigadores informáticos, los hackers, encuentren alguna manera de minimizar nuestra vulnerabilidad frente a las abusivas condiciones que imponen las empresas de internet.

La industria del *malware* crece vertiginosamente. Los *blackhats* inventan nuevos virus para infectarnos, como los «cocineros de coca» inventan nuevas drogas químicas aún no tipificadas. Pero los *whitehacks* expertos en *malware,* como GriYo, o el doctor Ricardo J. Rodríguez, los estudian para buscarnos el «antídoto».

Al principio yo pensaba que los hackers eran piratas informáticos. Después creí

que los hackers eran buenos, y los malos eran los crackers. Pero algunos, más puristas, como Román Ramírez, opinan que crackers son los que practican cracking, y que los hackers pueden ser buenos o malos. Como los policías, los médicos o los periodistas. Los hay honrados, sinceros y que, siendo más o menos competentes, al menos no sienten vergüenza al mirarse al espejo. Pero también los hay corruptos.

Los hackers son como el portero o el sereno que vigila de madrugada que las puertas y ventanas de nuestra casa estén debidamente cerradas. Y si encuentra alguna cerradura debilitada por el uso, alguna claraboya entreabierta, algún portillo entornado, advierte a la inmobiliaria o al casero para que repare de inmediato esa deficiencia en nuestra seguridad. Gracias a ellos, y a su trabajo preventivo, los ladrones no entrarán a robar en nuestro hogar, y podremos descansar tranquilos.

Notificada la vulnerabilidad por el portero o el sereno, es responsabilidad del casero o la inmobiliaria actualizar su sistema. Y si no desatiende esa responsabilidad, te mandará una carta para que tú actualices las medidas de protección de tu casa: este es el nuevo número de tu caja fuerte; esta es la nueva llave del portal, el buzón y la cerradura; esta es la nueva combinación del portero automático… Pero si tú no actualizas esas nuevas medidas, se lo dejas más fácil a los ladrones, por mucho que el sereno (hacker) haya advertido a la inmobiliaria de por dónde pueden colarse en tu casa.

Por eso es tan importante que pongas algo de tu parte, actualizando tu ordenador, instalando un antivirus (gratuito o no, pero no uno pirata, que lleva el bicho incorporado), y cualquier otra medida que te haga sentir más seguro. Tienes mucho donde elegir.

Desde el instante en que activas la wifi, enciendes el ordenador y abres el navegador, eres vulnerable a través de todos y cada uno de esos pasos. Pero todos pueden reforzarse para que tu navegación sea lo más segura posible. A partir de ahí, solo es cuestión de sentido común. El mejor antivirus eres tú, pero también tu mayor vulnerabilidad. Todo depende de ti.

La verdad está ahí dentro… pero hay que saber buscarla

No sé tú, pero yo me siento totalmente desvalido. Dibujamos nuestro mapa del mundo en base a lo que nos cuentan los medios de comunicación, pero la mayoría están condicionados, cuando no radicalmente polarizados, por una u otra tendencia política. No nos cuentan cómo es el mundo, sino cómo quieren que creamos que es.

Internet, teóricamente, nos brinda la posibilidad de buscar la información por nuestra cuenta, al margen de los grandes medios, pero he descubierto que la red está tan llena de mentiras como los periódicos de derechas o de izquierdas. ¿Qué nos queda?

Prometo que me incomoda utilizar tanto la primera persona. Pero creo que, especialmente en esta ocasión, mi propia experiencia personal puede concretar, con ejemplos prácticos, situaciones que quizá difuminen su relevancia en un planteamiento teórico genérico. Y al haber perdido tanto tiempo y dinero intentando contrastar en el terreno informaciones que había leído en la red, me consta que abunda la desinformación.

Internet continuará siendo un altavoz de mentiras, como hemos visto una vez más ante la crisis de los refugiados sirios, en septiembre de 2015, convertida en el nuevo vector de ataque para el spam, el *phishing* y la propaganda contra la inmigración a base de noticias tan falsas como las bodas de niñas de diez años con terroristas islámicos en Gaza, Irán o Arabia Saudí. Y en los próximos años llegarán más.

Ante las afirmaciones vertidas en un libro, un canal de radio o televisión, o un medio impreso, hay representantes legales a los que exigir responsabilidades. Con lo que se publica en un blog, una red social o la Wikipedia, es más complicado. Pero las nuevas generaciones digitales se están acostumbrado a nutrirse cada vez más de la información que leen en la pantalla, y es responsabilidad de sus mayores que aprendan a discernir qué fuentes son fiables y cuáles no. De lo contrario, las generaciones futuras serán todavía más imbéciles que nosotros, y eso sería terrible.

Así que mantén tu capacidad crítica ante emails extraños, páginas web o las propias noticias de prensa. Cuestiónate qué intereses hay detrás de cada una de ellas. Navega por la red, disfrútala, pero siempre de un modo sensato y a las riendas: ella no te controla, tú la controlas a ella. Que internet no te cambie: no hay un mundo ficticio en la red y otro real fuera de ella: tú siempre serás tú, aunque te envuelvas en un nick. Y ese doble digital que te has creado, a lo mejor para huir de una rutina o para reírte un rato o para insultar a alguien porque, total, esto no es «real», no es «de verdad», continuará allí cuando ya no lo necesites. Internet es el mundo real, tu nick eres tú mismo. Lo siento: no dejas de ser tú cuando tecleas bajo otro nombre. Y todo lo que entra en la red, se queda en la red. ¿Cómo quieres recordarte? ¿Cómo quieres que te recuerden? ¿A quién quieres abrirle la puerta de tu vida? ¿Cómo vas a salir a

esas autopistas?

Puedes entrar en ellas un día de lluvia, con las ruedas gastadas, sin usar el cinturón, con un coche sin airbag y wasapeando mientras conduces, y lo más probable es que tarde o temprano tengas un accidente. Sin embargo, cuando te echas a la carretera con el coche o la moto en condiciones, el depósito lleno y sin prisas, ahí afuera tienes miles y miles de kilómetros de paisajes, de personas y de lugares que será maravilloso conocer. Como en la red.

Glosario *hacker* básico

A

agujeros: Ver *bug*.

AI: Artificial Intelligence. Inteligencia Artificial. Rama de la informática que estudia la simulación de inteligencia con ordenadores.

B

backdoor: Puerta trasera. Vulnerabilidad en un sistema informático que permite su acceso evitando el procedimiento de entrada legítimo. Puede tratarse de un bug o de un acceso creado por el fabricante (backdoor).

backup: Copia de seguridad del sistema o de los datos.

BBS: Bulletin Board System (Sistema de Boletines). Equipo informático donde los usuarios se reúnen, a través de la línea telefónica, para intercambiar software, libros, artículos o información.

bit: Unidad mínima de información digital. Solo puede tomar los valores 0 (cero) y 1 (uno).

blackhat: Hacker de sombrero negro. Ciberdelincuente.

botnet: Conjunto de ordenadores que un solo usuario ejecuta en remoto, para objetivos que requieren gran capacidad informática. Pueden ser utilizados con propósitos científicos (Proyecto SETI), o si se trata de ordenadores «zombificados» ilícitamente, para un uso criminal.

bouncer: Técnica de anonimización mediante una m**á**quina puente que recibe las órdenes de otro equipo, redireccionando hacia el sitio escogido. Se usa para mantener el anonimato, por ejemplo en el IRC.

boxes: Circuitos o elementos utilizados para hackear las líneas telefónicas: *phreaking*.

bug: También llamados agujeros o *holes*. Vulnerabilidades del software que permiten introducirse en sistemas informáticos ajenos.Ver *backdoor.*

byte: Unidad mínima de información en informática, compuesto por 8 bits. Puede adoptar 256 valores diferentes.

C

caballo de Troya: Ver *troyanos*.

captcha: Iniciales de *Completely Automated Public Turing test to tell Computers and*

Humans Apart («Prueba automática y pública de Turing para diferenciar computadoras de humanos»). Habitualmente se utiliza para validar que el usuario de un servicio es un humano y no un programa mediante una combinación de letras y/o números.

carding: Hacking de tarjetas de crédito, de sus números o de las identidades de sus propietarios.

código fuente: Conjunto de instrucciones escritas por el programador y que ejecuta el programa a través de un lenguaje de programación (Linux, Pitón, Basic, C, Cobol, Pascal, etcétera) que el ordenador traducirá a lenguaje binario.

cookies: Bloques de datos, enviados por la web visitada a nuestro ordenador, y que quedan almacenados en el disco duro. Permiten recordar contraseñas, preferencias, etcétera, pero recopilan información sobre el perfil de los usuarios.

copia de seguridad: Ver *backup*.

cortafuegos: Firewall, sistema de seguridad que permite proteger el sistema de incursiones ilícitas.

cracker: Del ingles *to crack,* «romper». Hackers que rompen los sistemas de seguridad para entrar ilícitamente en un sistema con diferentes objetivos. Con frecuencia se utiliza como sinónimo de ciberdelincuente para diferenciarlos de los hackers, pero no toda la comunidad acepta esa definición.

creepware: Software espía diseñado para activar de forma no autorizada el micrófono y la cámara de dispositivos móviles u ordenadores ajenos. Es una versión «privada» de los programas espía de la NSA, que se ha distribuido ilícitamente a través de páginas de descarga y aplicaciones para móviles. Se desconoce cuántos millones de equipos y teléfonos pueden estar infectados…

cypherpunk: Movimiento hacktivista que aboga por el uso de la criptografía como instrumento de cambio social y político nacido a finales de los ochenta en una lista de correo.T**í**tulo de uno de los libros de Julian Assange que puedes encontrar en la bibliografía.

D

DDoS: Los ataques DDoS o de denegación de servicio consisten en bombardear una web con miles de peticiones hasta colapsarla y hacerla caer de internet.

Deep Weeb: Solo el 4% del contenido total de internet aparece indexado en los buscadores como Google, Yahoo, Bing, etcétera. El 96% restante permanece oculto. En esa Deep Weeb, Hidden Web o web profunda, permanecen ocultos activistas y filtraciones, pero también pedófilos, traficantes de armas o drogas, y sicarios. A esas

páginas solo puede accederse a través de protocolos específicos, como TOR.

denegación de servicio: Ver *DDoS*.

doxing (doxeo): Técnica para obtener información de una persona a través de la tecnología. No se trata de hackearle la cuenta, sino de saber utilizar las herramientas que ya existen.

E

encriptar: Aplicación de sistemas matemáticos para convertir un mensaje legible en otro ininteligible, que requiera de unas contraseñas para volver a recuperar su estado natural.

exploit: Explotación de la vulnerabilidad de un sistema a través de un fragmento de software o datos, o una secuencia de comandos o acciones que permitan entrar ilícitamente en dicho sistema.

F

fake: Fraude, engaño, hoax.

firewall: Ver *cortafuegos*.

FTP: File Transfer Protocol. «Protocolo de Transferencia de Ficheros.» Protocolo de comunicaciones para intercambio de ficheros en internet más utilizado por los usuarios.

fuerza bruta, ataque por: Técnica de obtención de una contraseña o clave probando todas las combinaciones posibles. El ataque de diccionario, utilizando todas las palabras incluidas en un idioma y sus posibles combinaciones, a través de programas informáticos creados para ese fin, es un ataque de fuerza bruta.

G

geolocalización: Identificación automática de las coordenadas geográficas incluido por defecto en muchas aplicaciones informáticas: fotos, vídeos, tuits, etcétera.

greyhat: Hackers de sombrero gris, que no se identifican con los blackhat ni con los whitehat. Con frecuencia, sinónimo de hacktivistas.

grooming: Acoso de un adulto a un menor en internet, normalmente presentándose como otro menor, con objeto de abusar sexualmente de la víctima u obligarla a generar material audiovisual erótico o pornográfico.

gusano: Programa informático con la capacidad de reproducirse a sí mismo una y otra vez, saltando de un sistema a otro.

H

hacker: Investigador de las vulnerabilidades de un sistema y mucho más (si te has leído el libro, eso lo tendrás claro…).

hacking: Conjunto de técnicas y habilidades desarrolladas por los hackers.

hacking wifi: Acceso ilícito a la conexión inalámbrica de un sistema inalámbrico.

hacktivismo: Activismo social a través de la tecnología.

hardware: Elementos físicos de un sistema informático: memorias, microprocesadores, teclados, módems…

hoax: Bulo, fraude, engaño que circula por la red. Fake.

hole: Ver *bug*.

HTML: HyperText Markup Languaje. **«**Lenguaje de Marcas de Hipertexto.**»** Lenguaje más utilizado para la elaboración de páginas web.

HTTP: HyperText Tranfer Protocol. **«**Protocolo de Transferencia de Hipertexto.**»** Protocolo utilizado para la visualización de las páginas en la web.

I

ID: El identificador de usuario en los sistemas tipo UNIX.

ingeniería inversa: Reversing. Técnica de análisis de programas o componentes informáticos que avanza en dirección opuesta al proceso de elaboración o uso de dichos componentes o programas.

ingeniería social: Conjunto de técnicas y estrategias psicológicas que tienen por objeto la obtención de información útil sobre el objetivo y sus vulnerabilidades. También conocida como hacking humano.

Inteligencia Artificial: Ver *AI*.

internet de las cosas: Aplicación de la informática y la tecnología a los objetos, electrodomésticos y mobiliario de uso cotidiano. La implantación de programas informáticos y conexión en remoto de coches, frigoríficos, televisores, domótica, etcétera, forma parte del internet de las cosas.

intranet: Redes privadas de información, sin acceso desde el exterior, implantadas fundamentalmente en el ámbito empresarial.

IP Internet Protocol.Etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un ordenador dentro de una red que utilice el protocolo IP. La dirección IP puede variar muy a menudo por cambios en la red o porque el dispositivo encargado de asignar las direcciones IP decida asignar otra. A esta forma de asignación de dirección IP se denomina también

dirección IP dinámica. Los sitios de internet que por su naturaleza necesitan estar siempre conectados, por lo general tienen una dirección IP fija, que no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

L

lamer: Quienes utilizan las herramientas de hacking, sin ser hackers (los que hackean a partir de tutoriales en YouTube, por ejemplo).

Linux: Sistema operativo de software libre perteneciente a la familia UNIX y muy valorado entre los hackers.

M

MAC Adress o dirección MAC: Del inglés *media access control,* es un identificador de 48 bits (6 bloques hexadecimales) que corresponde a una tarjeta o dispositivo de red única para cada ordenador. También se conoce como la dirección física del ordenador.

malware: Software malicioso para infectar ordenadores y teléfonos móviles.

módem: Dispositivo de conexión del ordenador, con internet, a través de la línea telefónica principalmente. Adapta las señales digitales para su tránsito a través de la línea.

N

navegador: Programa o aplicación informática que permite el acceso a la red. Los más utilizados hoy día sonInternet Explorer, Mozilla, Google Chrome, Netscape… Cada uno con sus particularidades y vulnerabilidades específicas.

nick: Pseudónimo utilizado por los usuarios de internet, generalmente acompañado de un avatar o imagen con la que se identifican en canales de charla, foros, juegos *online* y demás.

P

password: Contraseña. Palabra o palabras, o combinación de palabras y números o símbolos, que autentifica al usuario para acceder a sus servicios en la red. Un password fuerte intarcala letras, números y símbolos, como me enseñó el comandante C**é**sar Lorenzana.

pentesting: Los test de penetración tienen por objeto evaluar la seguridad de un sistema informático poniendo a prueba sus debilidades, por ejemplo, a través de auditorías de seguridad.

PGP: Siglas de Pretty Good Privacy (Privacidad muy buena). Sistema de cifrado de

las comunicaciones muy utilizado por los hackers, que utiliza una combinación de claves públicas y privadas de hasta 2.048 bits.

phishing: O suplantación de identidad. Es uno de los fraudes más habituales en internet. Consiste en el envío de correos electrónicos manipulados para engañar al receptor, haciéndose pasar por su banco, el depositario de una herencia, un o una atractiv@ admirador@, un estamento oficial, etcétera. El objetivo es que el receptor entre en una página web que parece real, pero está preparada para robar sus contraseñas, entre otras cosas.

phreaking: Disciplina de hacking centrada en el hackeo de sistemas de cobro telefónico.

R

ramsonware: Tipo de malware o software malicioso, que bloquea el acceso al sistema o a sus archivos, al usuario legítimo, pidiendo un rescate por dicho acceso. Los ramsonwares «virus de la policía» o «virus de correos» imitaban las web de cuerpos policiales o del servicio de Correos, para engañar al usuario que ejecutaba el programa, y bloqueaba su ordenador, quedando a merced de los ciberdelincuentes.

reversing: Ver *ingeniería inversa.*

router: Equipo que forma parte de las redes de comunicaciones y tiene como misión encauzar el flujo de paquetes de información. Ver *módem*.

S

simulación de identidad: Usurpación del nick, avatar u otra forma de identificación del usuario para falsear una identidad en la red.

Sistema Operativo: SO. Programa o conjunto de programas que gestiona los recursos básicos y encendido de un sistema informático, y no el conjunto de programas y aplicaciones de dicho sistema.

spam: Correo basura. Con frecuencia el vehículo del malware enviado a nuestro equipo.

T

tracear: Seguimiento de un objetivo en internet, a través de diferentes técnicas de análisis, geolocalización, etcétera.

trol: Usuario que publica mensajes provocadores con la intención de molestar y despertar una respuesta emocional en otros usuarios. Su origen etimológico más probable evoca la idea de «morder el anzuelo» o «morder el anzuelo mucho más» (*trol* es un tipo de pesca en inglés). Trolear sería, por tanto, provocar una reacción en otros usuarios, hacerles «morder el anzuelo», a base de comentarios hirientes y

agresivos.

troyano: Software malicioso que ataca un sistema informático infiltrándose en el mismo, sin conocimiento del usuario legítimo, y dando el control a un operador remoto. El nombre está inspirado en la leyenda del Caballo de Troya.

U

URL: Uniform Resource Locator. «Localizador Uniforme de Recursos.» Dirección electrónica que debemos teclear en nuestro navegador para acceder a una web determinada.

V

virus: Se aplica este concepto genéricamente a todo tipo de malware o software malicioso, aunque existen distintas tipologías de virus en función de su programación, capacidad y diseño.

vulnerabilidad: Deficiencia en el sistema de seguridad de un programa, aplicación telefónica, servicio, software o hardware que puede ser explotado por usuarios no legítimos.

W

whitehat: Hackers de sombrero blanco. Investigadores de hacking, auditores informáticos, consultores de seguridad, etcétera.

WWW: World Wide Web.

Z

zombi, ordenador: Ordenador infectado por un malware que lo pone a disposición de un ciberdelincuente, dentro de una red o botnet que puede incluir a cientos de miles de zombis, sin que el usuario sea consciente de ello, y siendo utilizados para diferentes tipos de delitos: como ataques de denegación de servicios, posicionamiento en buscadores o aumento de seguidores en redes sociales, entre otros.

Bibliografía

Un libro centrado en internet como este tenía que beber directamente de las fuentes hechas a base de unos y ceros. Además de los viajes dentro y fuera de España, y las docenas de entrevistas, una parte de la documentación proviene de los blogs de los hackers más relevantes. También de las numerosas charlas y las jornadas de las distintas CON a las que he asistido en los últimos años. Ellos, los verdaderos expertos en este mundo digital, han sido mis maestros, mis fuentes de documentación, y a ellos me remito. Aun así, debo nombrar algunos libros específicos y blogs concretos, que me allanaron el camino:

- Alonso, C. y otros. *Hacking de dispositivos iOS: iPhone y iPad,* Informática 64, Madrid, 2013.
- Assange, J. y Dreyfus, S. *Underground,* Seix Barral, Barcelona, 2011.
- Assange, J. y otros. *Cypherpunks,* Deusto, Barcelona, 2013.
- Avilés, Á. P., «Angelucho». *X1red+segura* (descargable en pdf en la web de la GDT: www.gdt.guardiacivil.es/webgdt/x1red+segura.php)
- Barrera, S.«La lucha policial ante el horror de la pornografía infantil», tesina de fin de carrera.
- Erelle, A. *En la piel de una yihadista,* Debate, Barcelona, 2015.
- Falciani, H., *La caja fuerte de los evasores,* La Esfera de los Libros, Madrid, 2015.
- García Rambla, J. L. *Ataques en redes de datos IPv4 y IPv6,* Informática 64, Madrid, 2014.
- Garrido Caballero, J. *Análisis forense digital en entornos Windows,* Informática 64, Madrid, 2012.
- Gómez i Urgellés, J. *Matemáticos, espías y piratas informáticos,* RBA, Barcelona, 2010.
- Gómez López, J. *Hackers: Aprende a atacar y defenderte,* RA-MA, Madrid, 2009.
- Greenwald, G. *Snowden: Sin un lugar donde esconderse,* B de Books, Barcelona, 2014.
- Hadnagy, C. *Ingenieria social: el arte del hacking personal,* Anaya Multimedia, Madrid, 2011.
- Hermida, J. M. *La estrategia de la mentira,* Temas de Hoy, Madrid, 1993.
- Himanen, Pekka, *La ética del hacker y el espíritu de la era de la información,* Destino, Barcelona, 2001.
- Lobohem, F. *Así nos vigilan,* Ipunto, Madrid, 2010.
- McClure, S., Scambray, J. y Kurtz, G. *Hackers, secretos y soluciones para la seguridad de redes,* McGraw-Hill, Madrid, 2000.

- Molist, M., *Hackstory.es,* autor-editor, 2014.
- Molist, M. y Medina, M. *Cibercrimen,* Tibidabo, Barcelona, 2015.
- Monsoriu, M. *Diccionario web 2.0.* Creaciones Copyright, Madrid, 2010.
- — *Manual de redes sociales en internet.* Creaciones Copyright, Madrid, 2008.
- — *Técnicas de hacker para padres.* Creaciones Copyright, Madrid, 2007.
- Moreno, A. *Diccionario de informática y telecomunicaciones,* Ariel, Barcelona, 2001.
- Peirano, M. *El pequeño libro rojo del activista en red,* Roca Editorial, Barcelona, 2015.
- Ramos,A. y Yepes, R. *Hacker épico,* Informática 64, Madrid, 2014 (posteriormente convertida en cómic).
- Rando, E. y Alonso, C. *Hacking de aplicaciones web: SQL Injection,* Informática 64, Madrid, 2012.
- Stoll, C. *El huevo del cuco,* Planeta, Barcelona, 1990.
- Torres Soriano, M. *La dimensión propagandística del terrorismo yihadista global,* Editorial Universitaria de Granada, Granada, 2007.
- — *Al Andalus 2.0.: La ciber-yihad contra España,* autor-editor, 2013.
- Troncoso, R. y Ramírez, F. J., *Microhistorias: Anécdotas y curiosidades de la informática,* Informática 64, Madrid, 2012.
- Vidal, D. R. *Diario de un espía,* Cúpula, Barcelona, 2014.

Blogs sobre hacking y seguridad informática

- 48bits: www.48bits.com
- Adastra: thehackerway.com
- Aiuken: www.aiuken.com/media
- All Sources Inteligence: www.asint360.com
- Antonio Calles: www.flu-project.com
- CiberHades: www.cyberhades.com
- Ciberinvestigación: www.ciberinvestigacion.com
- Conexión Inversa: conexioninversa.blogspot.com.es
- Dragonjar: www.dragonjar.org
- El Blog de Angelucho: elblogdeangelucho.com
- El Foro del Hacker: foro.elhacker.net
- Eleven Paths: blog.elevenpaths.com
- Hacking Code School: www.hackingcodeschool.net
- HackPlayers: www.hackplayers.com
- Internet, Ciudad con Ley, de Silvia Barrera:

www.tecnoxplora.com/internet/ciudad-con-ley
- Jesús Cea Avión: www.jcea.es
- Juez Calatayud: www.granadablogs.com/juezcalatayud
- Lista de correo RootedCON: rootedcon@listas.rooted.es
- Mario Vilas: breakingcode.wordpress.com
- Mercè Molist: hackstory.net
- Scam & Seglog: blog.sit1.es
- S21Sec: blog.s21sec.com
- Security Art Work: www.securityartwork.com
- Security By Default: www.securitybydefault.com
- Seguridad Libre: www.seguridadlibre.com
- Seguridad Ofensiva: www.seguridadofensiva.com
- Silvia Barrera: www.silviabarrera.es
- Tarlogic: www.tarlogic.com/blog
- Un Informático en el Lado del Mal, de Chema Alonso «el Maligno»: www.elladodelmal.com

Webs oficiales

- GDT (Grupo de Delitos Telemáticos) Guardia Civil: www.gdt.guardiacivil.es
- BIT (Brigada de Investigación Tecnológica) Policía Nacional: www.policia.es/org_central/judicial/udef/bit_alertas.html
- INCIBE (Instituto Nacional de Ciberseguridad): www.incibe.es

Eventos y CON

- AlbahacaCon – Huesca: @AlbahacaCon, http://www.albahacacon.es
- Clickaseguro – Valdepeñas: @Clickaseguro, clickaseguro.es
- ConectaCon – Jaén: @ConectaCon, conectaconjaen.org
- GSICKMinds – A Coruña: @GSICKMINDS, gsickminds.net
- Hackr0n – Islas Canarias: @Hackr0n, hackron.com
- HoneySec – Guadalajara: @Honey_SEC, http://honeysec.info
- MorterueloCon – Cuenca: @morteruelocon, morteruelo.net
- Mundo Hacker – Madrid: @mundohackertv, mundohacker.es
- Navaja Negra – Albacete: @navajanegra_ab, navajanegra.com
- No cON Name – Barcelona: @noconname, noconname.org

- Qurtuba – Córdoba: @qurtubacon, qurtuba.es
- RootedCON – Madrid: @rootedcon, rootedcon.es
- Sec Admin – Sevilla: @secadm1n, secadmin.es
- Sh3llcon – Santander: @Sh3llCON, sh3llcon.es

Agradecimientos

A David Madrid, Rafa, Rubén, Pepe, Álex, Toni, Manu, Rado y todos los demás policías que invirtieron tantas horas de su tiempo en la investigación de MarkoSS88.

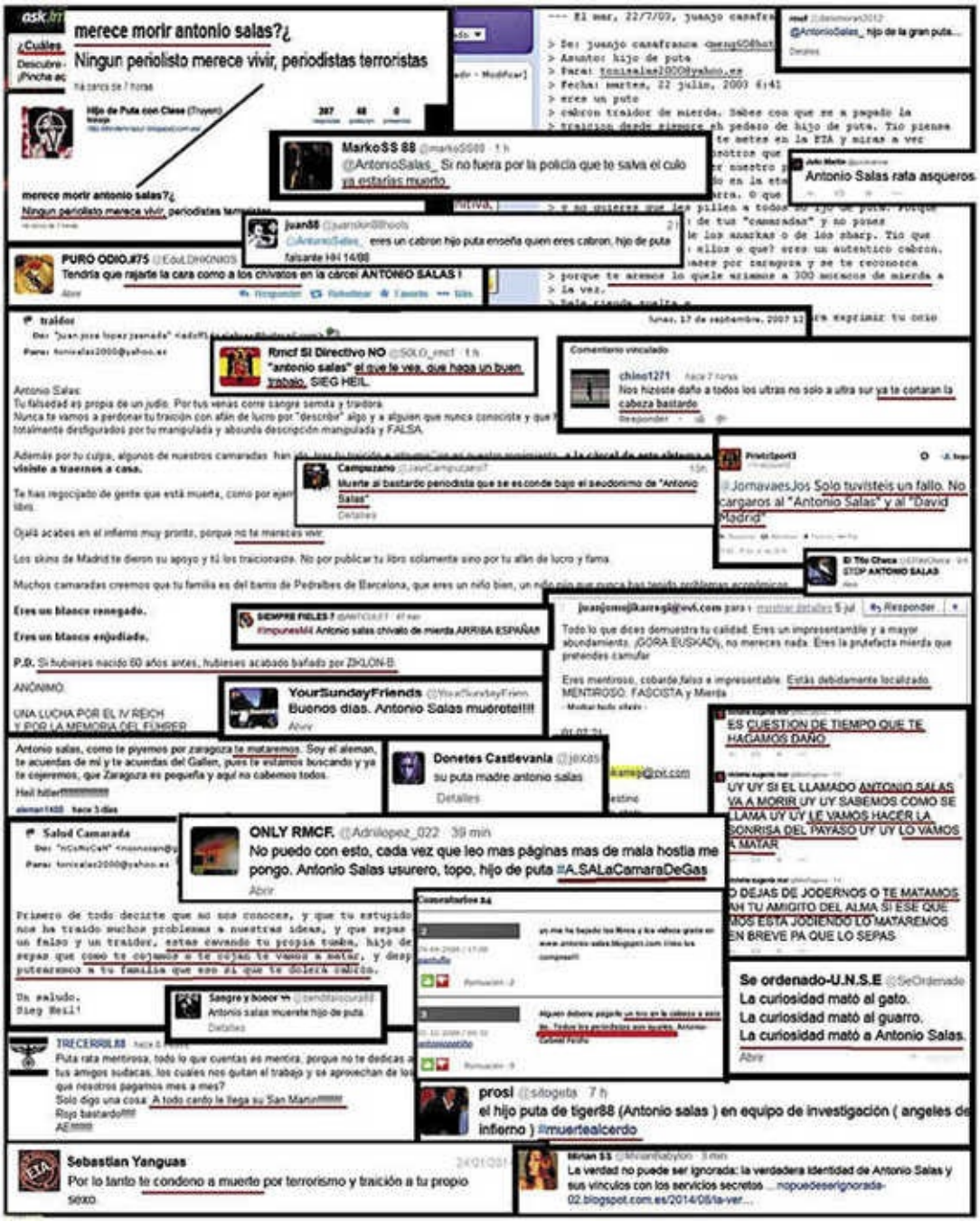
A Silvia Barrera, Selva Orejón, César Lorenzana, Israel Córdoba, David Pérez, Román Ramírez, Chema Alonso, Chus, Berto, Lord Epsylon, «Lucas», Pedro Candel… y todos los demás hackers, por abrirme las puertas de su fascinante mundo y por la paciencia que tuvieron conmigo.

El héroe Cálico Electrónico y el villano Gran Dimitri, por arrancarme tantas sonrisas.

A Maya, por su revisión crítica y todas sus aportaciones.

A la memoria de mi compañero José Couso, por dejarse la vida informándonos y para que su asesinato no se olvide, doce años después… ni nunca.

Encarte



Las amenazas de MarkoSS88 se diluían entre las recibidas a diario de parte de nazis, terroristas, puteros, proxenetas o traficantes… Hasta el 5 de marzo de 2014. (Foto A. Salas)

La sala de conferencias de la URJC se llenó el 5 de marzo durante la Jornada de Inteligencia y Servicios Secretos. Y MarkoSS88, que se matriculó con nombre y DNI falsos, se quedó en lista de espera. (Foto cortesía UEP)

Instalaciones del Grupo de Delitos Tecnológicos de la UCO. Sobre la columna, una máscara de Guy Fawkes, emblema de Anónymous. (Foto A. Salas)

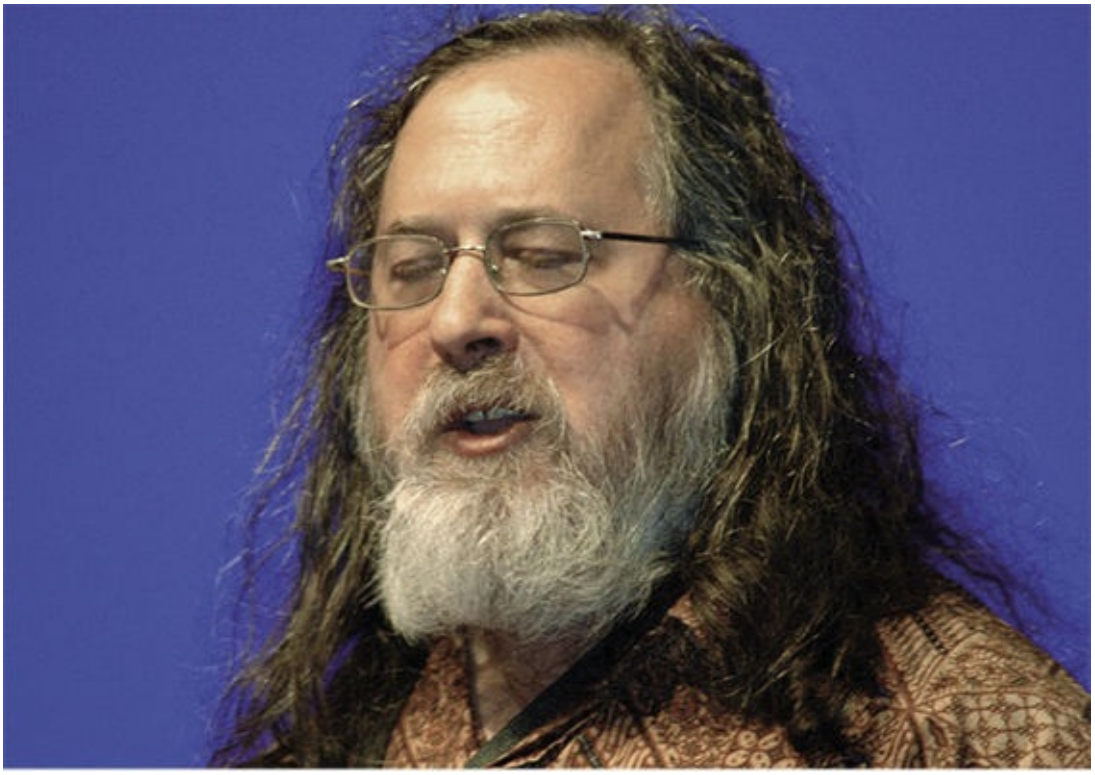
David R. Vidal, alias «el Agente Juan», durante 12 años espía del CNI, en su despacho. (Foto A. Salas)

Israel Córdoba, el business hacker, en su despacho de Aiuken Solutions: «Ya estamos en Matrix». (Foto A. S)

Ángel Pablo Avilés, «Angelucho», guardia civil del GDT y fundador de X1Red+Segura: «Tu mejor antivirus eres tú… pero tu mayor vulnerabilidad, también».

El mapa de los ciberataques que se producen en el mundo en tiempo real ilustra las dimensiones del problema. (Foto A. Salas)

David Pérez, hacker antes que policía: «…teníamos solo ocho días para detener al pedófilo, o seguiría violando a sus hijos durante todas las vacaciones…».



Richard Stallman, el más polémico impulsor del software libre: «Si ves a alguien ahogarse y sabes nadar, tienes el deber moral de salvarlo, a menos que sea Bush o Aznar». (Foto A. Salas)

El comandante César Lorenzana en su despacho de la UCO: «Si tapas la webcam de tu ordenador, ¿por qué no tapas la del móvil?». (Foto A. Salas)

Abubakar Shekau, miserable líder de Boko Haram, descubrió el poder de la Red con el secuestro de las niñas de Chibok.

El campamento de los refugiados sirios en Ceuta, en Ramadán de 2014. Mientras algunos ceutíes viajan a Siria para luchar con el ISIS, los sirios piden asilo en España para escapar de la guerra. (Foto A. Salas)

Selva Orejón durante uno de los cursos sobre reputación digital de OnBranding: «Todo lo que subes a la red puede usarse contra ti». (Foto A. Salas)

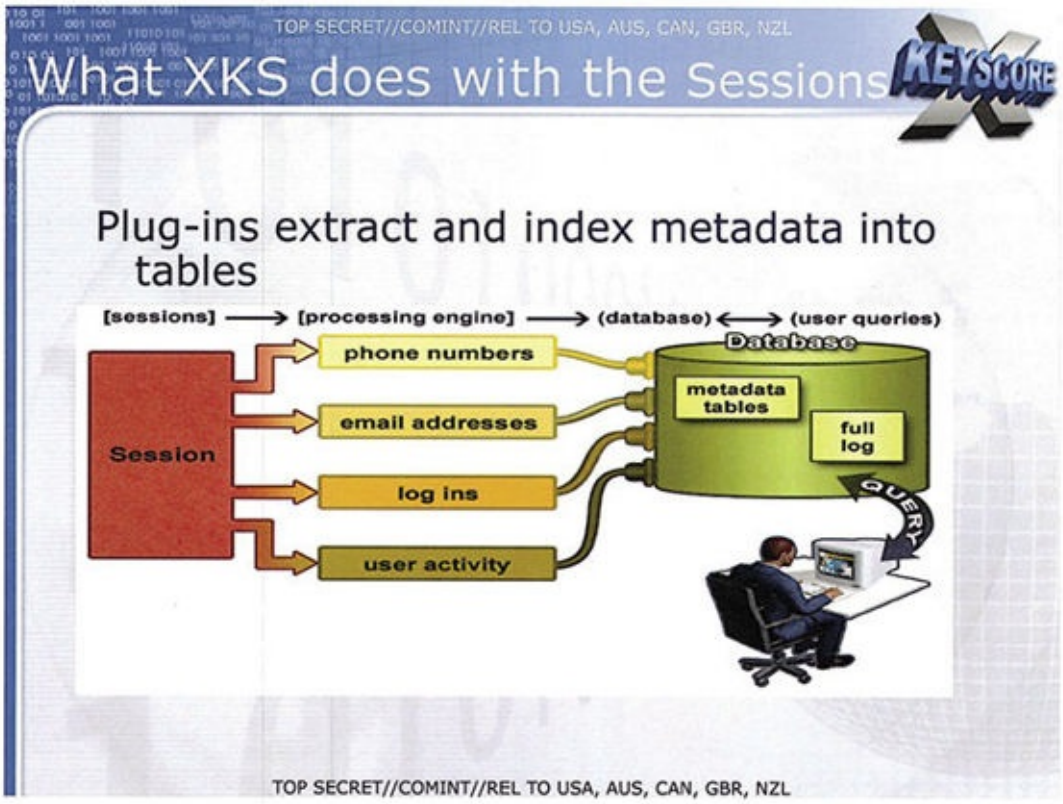
El terrorista católico Guy Fawkes, V de Vendetta y Anónymous, unidos por el merchandising hacker. (Foto cortesía Museo del Espía)

La inspectora Silvia Barrera, de la BIT. «El 72 % de las víctimas de pedofilia son niño/as de entre 0 y 10 años de edad. El 44 % de imágenes que representan son violaciones y torturas…». (Foto A. Salas)

Yago Hansen, el «hombre wifi», con uno de sus equipos de hacking wifi. «Es posible hackear tu ordenador desde 500 metros de distancia, infiltrándose en tu red inalámbrica». (Foto A. Salas)

El coronel Enrique Cubeiro, del MCCD, en el Museo del Espía: «En el ciberespacio se combate con ciberarmas. Y las ciberarmas son las mismas para el crimen organizado que para el hacktivismo o el espionaje». (Foto A. Salas)

Hervé Falciani, el informático que hackeó la banca suiza, con el autor: «Es fácil comprender por qué los políticos no hacen nada para combatir la evasión fiscal… al proteger a los bancos se protegen a sí mismos». (Foto A. Salas)



Edward Snowden desveló que programas como xKeyscore permiten a la NSA acceder a todas nuestras comunicaciones.

Epsylon fue el primer desalojado por la policía en la acampada de Sol de los Indignados: «Tus niveles de paranoia son directamente proporcionales a lo que sepas de las cosas». (Foto cortesía Epsylon)

Los 6 tatuajes en la cara interna de los brazos recuerdan al hacktivista y escritor de código Lord Epsylon quién es, y de dónde viene, a través de 6 símbolos hacker. (Foto A. Salas)

Lord Epsylon en el momento de hackear las comunicaciones de un satélite. (Foto A. Salas)

Antonio Salas en la sede de Charlie Hebdo en París. (Foto A. Salas)

La gran Mezquita de París, vigilada por la policía francesa desde el ataque a Charlie

Hebdo. (Foto A. Salas)

Amedy Coulibaly, uno de los terroristas de París, alertó a los servicios de información españoles al visitar Madrid días antes del ataque a Charlie Hebdo.

Ejemplares de Charlie Hebdo en la exposición Historia del Espionaje de Sarria. (Foto A. Salas)

Pepe, a la derecha, con sudadera verde y gris, durante la participación de David Madrid en la mesa redonda del congreso sobre espionaje en Sarria. (Foto A. Salas)

Los guardias civiles Berto y Chus detienen al «agente enemigo» ante Mauro y Fernando Rueda, en el Museo del Espía. (Foto cortesía D. Castillo)

Análisis forense de un disco duro en la Brigada de Investigación Tecnológica del CNP.
(Foto cortesía BIT)

La ilustradora Blanca Tulleuda resume cada sesión de X1Red+Segura con sus grabados. (Foto A. Salas)

El fiscal Jesús Bermúdez descubrió cómo hackear la Ley… «Si dejabas abierta la aplicación de gestión procesal y no apagabas el ordenador no avanzaba la fecha… así que, si se te pasaba la fecha de presentación de un recurso…». (Foto A. Salas)

Hugo Teso, con Román Ramírez, tras explicar cómo hackear un avión comercial con un teléfono móvil. (Foto cortesía RootedCON)

El doctor Ricardo J. Rodríguez, como GriYo, es experto en malware; ambos estudian los virus informáticos para encontrarnos la vacuna. (Foto A. Salas)

El polémico debate sobre quién puede dar el carnet de hacker, en la Rooted. De izquierda a derecha, R. Ramírez, A. Tarasco (Tarlogic), D. Solis (Blueliv), I. Córdoba, J. Davila (UPM), el fiscal J. Bérmúdez, C. Lorenzana, J. San José (EY). (Foto A. Salas)

Una imagen impensable hace pocos años: el comandante de la Cruz (UCO), de espaldas, escucha a los directores de las CON hacker españolas. De derecha a izquierda, Mavi Doñate, periodista de El País, con Román Ramírez (RootedCON), Carlos Díez (Sh3llcon), Igor Lukic (Hackron), M. García Peral (Clickaseguro), Jesús González (Mundo Hacker), Nico Castellano (NoConName), Álex Saiz (Navaja Negra), Jesús Marín (VillanetCon), Raúl Renales (Honey SEC), etc. (Foto A. Salas)

El hacker Chema Alonso durante su encuentro con S.M. el rey Felipe VI en el Mobile World Congress de 2015. (Foto cortesía Chema Alonso)

El vídeo hackeado por CiberBerkut a un senador de Estados Unidos pretende sembrar dudas sobre las decapitaciones del ISIS.

Notas

[1] http://www.elmundo.es/tecnologia/2014/11/20/546de362268e3ed7198b457f.html <<

[2] «Entrevista a mi asesino»: http://loshombresque-susurranalasmaquinas.blogspot.com.es/2015/09/entrevista-mi-asesino.html <<

[3] Temas de Hoy, 2013. <<

[4] El personaje de Álex Cardona, protagonista de *Operación Princesa*, está inspirado en la testigo protegido DPA123B: una joven universitaria latinoamericana que, con su denuncia, inició una imparable reacción en cadena que terminó con la imputación criminal de cientos de policías, políticos y empresarios gallegos. Las operaciones Carioca, Campeón, Pokemon, Manga, Bebé, Orquesta, etcétera, arrancaron gracias a la denuncia de esta joven. <<

[5] Editorial Cúpula, 2014. <<

[6] Temas de Hoy, 2004. <<

[7] www.intel.global. <<

[8] Temas de Hoy, 2010. <<

[9] Por ejemplo:

«Herramientas profesionales para desarrollo de bases de datos y aplicaciones web». http://www.pcworld.es/archive/4th-dimension-68

«Entornos paisajistas de 3D con animación y gran realismo». http://www.-pcworld.es/archive/corel-bryce-5

«Retoque fotográfico y edición de imágenes web». http://www.pcworld.es/archive/-picture-publisher-90 <<

[10] «Spain Spied on Moroccan Officials' Computers Between 2007-2014». http://www.marocpress.com/en/moroccoworldnews/article-34350.html/feed <<

[11] https://www.YouTube.com/watch?v=mEjxKtNq9T8

http://www.lasexta.com/programas/equipo-investigacion/noticias/antonio-salas-puedes-equivocar-vez-pero-hay-segundas-oportunidades_2013101800461.html <<

[12] http://www.rtve.es/alacarta/videos/personajes-en-el-archivo-de-rtve/entrevista-mercedes-mila-miguel-bose-1986/689820/ <<

[13] Temas de Hoy, 1993. <<

[14] El vídeo de la entrevista puede verse en: http://cnnespanol.cnn.com/2014/02/25/venezuela-angel-vivas-denuncia-injerencia-de-cuba-y-los-tupamaros-acusan-a-uribe-velez/ <<

[15] Documental *El Palestino: historia de un infiltrado.* https://www.YouTube.com/watch?v=21bjFzJ0F-w <<

[16] https://www.YouTube.com/watch?v=S7lDs4XzBJA <<

[17] https://www.YouTube.com/watch?v=DGFUeOVzI-Q <<

[18] http://colarebo.com/2010/10/25/la-oposicion-venezolana-roba-y-manipula-el-documental-el-palestino-de-antonio-salas/ <<

[19] La entrevista completa todavía está disponible en:

http://www.contrapunto.com.sv/latinoamerica/habra-plomo-si-no-respetan-triunfo-de-chavez <<

[20] El vídeo del que se tomó la imagen falsa de Chávez es: https://www.YouTube.com/watch?v=DB4bIH0GsYU<<

[21]
http://internacional.elpais.com/internacional/2013/01/24/actualidad/1359002703_817(
<<

[22]
http://internacional.elpais.com/internacional/2013/01/26/actualidad/1359234203_8756
<<

[23] http://www.diariolaprimeraperu.com/online/mundo/al-qaeda-se-infiltra_116287.html <<

[24] http://www.abc.es/hemeroteca/historico-17-08-2007/abc/Tecnologia/la-cia-y-el-vaticano-manipulan-los-articulos-de-la-wikipedia_164412456251.html <<

[25] http://www.welivesecurity.com/la-es/2015/09/01/wikipedia-bloquea-usuarios-titeres/ <<

[26] «Diez mentiras sobre el terrorismo internacional»: http://www.antoniosalas.org/blog/diez-mentiras-sobre-el-terrorismo-internacional <<

[27] http://www.noticiassin.com/2015/07/irak-podria-ser-el-primer-pais-en-legalizar-el-matrimonio-con-ninas/ o http://www.abc.es/internacional/20140319/abci-irak-matrimonio-ninnas-201403181723.html <<

[28] http://mentirassobreelislam.blogspot.com.es <<

[29] http://mentirassobreelislam.blogspot.com.es/2009/12/la-verdad-sobre-las-bodas-de-hamas.html, http://mentirassobreelislam.blogspot.com.es/2010/09/sakineh-la-falsa-victima.html, http://mentirassobreelislam.blogspot.com.es/2009/12/manipulacion-de-imagenes-falsa-nina.html, http://mentirassobreelislam.blogspot.com.es/2013/04/amina-y-la-falsa-fatua.html, http://mentirassobreelislam.blogspot.com.es/2009/12/otra-mentira-mas-el-supuesto-castigo-un.html… <<

[30] *Microhistorias: Anécdotas y curiosidades de la informática.* Informática 64, 2013. <<

[31] *Microhistorias: Anécdotas y curiosidades de la informática*, pág. 66. <<

[32] http://www.20minutos.es/fotos/actualidad/policias-de-calendario-en-sanse-3526

<<

[33] «Víctor Marquès y Miguel Ángel Campos en la Universitat de Barcelona; José Miguel Femenia y Rogelio Montañana en la Universitat de València; Miquel Àngel Lagunas y Manel Marín en la Universitat Politècnica de Catalunya; Jordi Adell y Toni Bellver en la Universitat de Castelló; José Antonio Mañas en la Universidad del País Vasco y después, la Politécnica de Madrid; José Ramón Martínez Benito y Josu Aramberri en la Universidad del País Vasco; Iñaki Martínez y Miguel Ángel Sanz en RedIRIS…», enumera Mercè Molist. <<

[34] Acrónimo de Bulletin Board System o Sistema de Tablón de Anuncios. Fueron el primer lugar de encuentro de los apasionados por la informática, y un software que permite la conexión a través de internet (antes a través de la línea telefónica), utilizando un programa terminal para descargar programas, interactuar con otros usuarios, jugar *online,* acceder a publicaciones especializadas, etcétera. Fueron las precursoras de los actuales foros. <<

[35]
http://www.infolibre.es/noticias/politica/2015/08/26/ahora_madrid_acusa_utilizar_dec
<<

[36] http://www.networkworld.es/seguridad/el-impacto-economico-del-cibercrimen-se-eleva-a-445000-millones-de-dolares <<

[37] http://www.loshombresquesusurranalasmaquinas.blogspot.com.es/2015/10/cazar-policias.html <<

[38] http://antivirus.es/la-muerte-de-amy-winehouse-elevo-el-phishing-3616 <<

[39] http://www.elmundo.es/blogs/elmundo/enredados/2013/12/22/despedida-de-su-empresa-por-un.html <<

[40] http://www.lacapital.com.ar/informacion-gral/Publico-un-comentario-en-Facebook-y-fue-despedida-antes-de-empezar-a-trabajar-20150430-0004.html <<

[41] http://www.huffingtonpost.com/2012/11/20/lindsey-stone-facebook-photo-arlington-national-cemetery-unpaid-leave_n_2166842.html <<

[42] http://www.huffingtonpost.com/2013/11/03/boston-marathon-victim-costume_n_4208720.html <<

[43] http://elblogdeangelucho.com/elblogdeangelucho/blog/2012/09/30/seguridad-basica-en-la-red-iii-diez-mandamientos-para-una-navegacion-segura/ <<

[44] http://larebeliondelvaron03.blogspot.com.es/2015/01/quienes-son-los-verdaderos-enemigos-de.html <<

[45]
http://internacional.elpais.com/internacional/2014/05/17/actualidad/1400343233_222
<<

[46] Solo tres semanas antes, el 26 de abril de 2014, Miller, el heraldo y autoproclamado portavoz del Dios blanco y cristiano de la Biblia, había vuelto a los titulares internacionales por una circunstancia muy poco «cristiana». Tras ser acusado del asesinato de tres judíos en Kansas (EE.UU.), el líder racista era localizado y detenido por la policía de Raleigh mientras mantenía relaciones sexuales en el asiento trasero de un coche con un travesti de raza negra. Que un adulto decida mantener relaciones con un travesti, con otro hombre, o con otra mujer, de la raza que sea, no es noticiable. Pero que pillen a un profeta del KKK comiéndole la verga a un travesti negro no parece muy coherente con la ideología proclamada por los racistas autodenominados cristianos. Según el fiscal federal J. Douglas McCullough, Miller fue detenido «haciendo cosas que para un fiscal no es cómodo decir en voz alta». Aunque Miller aseguró, en su «defensa», que había concertado los servicios del travesti para luego agredirle… Imagino que en el momento de su detención, y mientras le practicaba una felación, solo intentaba ganarse su confianza. <<

[47] *Mujahidin* (مجاهدين) plural de *mujahid* (مجاهد), participio activo del verbo árabe ŷā*hada*, que significa «hacer la yihad», y ŷ*ihā*d, a su vez, significa «esfuerzo orientado a la consecución de una finalidad». En la práctica, y puesto que el concepto de yihad aparece muchas veces ligado al combate militar, *muyahid* tiene un sentido de «combatiente musulmán» o «combatiente por el islam». <<

[48] http://templohindu.blogspot.com.es <<

[49]
http://www.loshombresquesusurranalasmaquinas.blogspot.com.es/2015/10/cronica-del-juicio-abu-sufian-acusado.html y http://www.loshombresquesusurranalasmaquinas.blogspot.com.es/2015/10/abu-sufian-el-terrorista-inocente.html <<

[50] *La dimensión propagandística del terrorismo yihadista global*, pág. 17. <<

[51] Idem, pág. 33. <<

[52] Idem, págs. 63-66. <<

[53] Idem, pág. 87. <<

[54] Idem, pág. 227. <<

[55] http://www.europapress.es/chance/gente/noticia-pilar-rubio-denuncia-policia-harta-fakes-falsificaciones-twitter-20131122085940.html <<

[56] http://articulos.softonic.com/reconocer-perfil-falso-facebook?ex=SWH-1566.0 o http://es.wikihow.com/detectar-una-cuenta-de-Facebook-falsa <<

[57] https://www.gdt.guardiacivil.es/webgdt/home_alerta.php <<

[58] https://twitter.com/gdtguardiacivil y https://www.facebook.com/GrupoDelitosTelematicos?fref=ts <<

[59] https://www.youtube.com/watch?v=mj0bjoNEaYk <<

[60] http://www.elmundo.es/navegante/98/noviembre/06/entremoral.html <<

[61] Ver *El año que trafiqué con mujeres,* Temas de Hoy, 2004. <<

[62] http://www.elmundo.es/navegante/2006/02/07/seguridad/1139328838.html <<

[63] http://www.elmundo.es/elmundo/2010/03/02/navegante/1267545550.html <<

[64] http://www.diariofemenino.com/actualidad/famosos/articulos/david-bisbal-navidad-extorsion-2008/ <<

[65] https://www.europol.europa.eu/content/more-200-children-identified-and-rescued-worldwide-police-operation

http://www.lavanguardia.com/sucesos/20110316/54129349174/desarticulada-la-mayor-red-pedofila-del-mundo-con-70-000-usuarios.html<<

[66] http://www.europapress.es/portaltic/software/noticia-detenidos-tres-gerentes-empresa-comercializaba-software-bombas-logicas-20100622121036.html <<

[67] http://www.20minutos.es/noticia/764755/0/hackers/salvame/pp/#xtor=AD-15&xts=467263 <<

[68] https://www.guardiacivil.es/ga/prensa/noticias/4045.html <<

[69] https://www.gdt.guardiacivil.es/webgdt/popup_noticia.php?id=1228 <<

[70] https://www.gdt.guardiacivil.es/webgdt/popup_noticia.php?id=1237 <<

[71] http://www.boe.es/buscar/act.php?id=BOE-A-1995-25444&p=20150428&tn=1#ci-8 <<

[72] El cibercriminal puede contralar su red zombi o *botnet*, por ejemplo a través de canales de chat. El descubrimiento de un zombi no implica la identificación del atacante o demás zombis. El servicio de chats del IRC por ejemplo, mantiene el anonimato. Un servidor de IRC puede albergar un canal en cualquier parte del mundo. Por eso la investigación en un canal de IRC se enfrenta a muchos problemas técnicos. <<

[73] http://www.elladodelmal.com/2013/12/creepware-fiarse-del-led-de-la-webcam.html <<

[74] https://www.gdt.guardiacivil.es/webgdt/cusuarios.php <<

[75] Estas máscaras, popularizadas por la película *V de Vendetta*, las adoptó posteriormente como seña de identidad el grupo hacktivista Anónymous. <<

[76] Editorial Círculo Rojo, 2015. <<

[77] infoceidiv@gmail.com <<

[78] http://www.dw.com/en/sick-hackers-attack-concentration-camp-website-with-child-pornography/a-18439993 o http://www.bbc.com/news/world-europe-32652394 <<

[79] http://www.europapress.es/nacional/noticia-concejal-socialista-cantabria-interpone-denuncia-amenazas-reiteradas-twitter-20130829184711.html <<

[80] http://www.cuartopoder.es/wp-content/uploads/2012/09/RAXEN-Especial-2011-Completo.pdf <<

[81] https://www.change.org/p/markos-libertad-injusticia-silenciada-pero-no-nos-har%C3%A1n-callar-markoslibertad <<

[82] https://twitter.com/hashtag/MarkosLibertad?src=hash <<

[83] «Markossestamoscontigo»: https://twitter.com/hashtag/markossestamoscontigo?f=realtime&src=hash (iniciada el 16 de enero de 2013 por @FranMAD1902).

«TodossomosMarkoss»: https://twitter.com/hashtag/todossomossmarkoss?f=realtime&src=hash (iniciada el 15 de enero de 2013 por @TheSpecialRubia).

«Markospudrete»: https://twitter.com/hashtag/markospudrete?f=realtime&src=hash (iniciada el 27 de enero de 2013). <<

[84] Ver *Operación Princesa*, Temas de Hoy, 2013. <<

[85] http://www.20minutos.es/noticia/146651/0/cracker/chantaje/menor/ <<

[86] http://www.forocomunista.com/t29421-alerta-antifascista-nazis-buscan-a-alfon-y-tienen-su-direccion <<

[87] http://www.eltiempo.com/archivo/documento/MAM-693503 <<

[88] http://www.abc.es/tecnologia/redes/20130505/abci-adoptauntio-mujeres-clientas-201305031557.html <<

[89] http://antonio-salas.blogspot.com.es/2005/11/mucho-cuidado-con-los-falsos-antonio.html, http://www.nuevorden.net/main.html, entre otras. <<

[90] Una pena inusualmente corta por un delito de homicidio, incluso en defensa propia, que él justifica con una triquiñuela legal de su abogado. <<

[91] http://www.elmundo.es/cronica/2013/12/08/52a326060ab74083768b456c.html <<

[92] Desde su página web oficial www.incibe.es se ofrecen numerosos servicios gratuitos a los internautas. Tanto a nivel empresarial como de usuario. <<

[93] http://www.elmundo.es/elmundo/2011/06/06/leon/1307378971.html <<

[94] Escrita en coautoría con Rodrigo Yepes y publicada en 2014 por Informática 64, y posteriormente convertida en cómic. <<

[95] Insisto en que es imposible reseñarlos todos. Marc «Van Hauser» Heuse, Lorenzo Martínez, Marion Marschalek, Vicente Aguilera, Robert Stroud, Josep Albors, Daniela Kominsky, David Meléndez, Pablo González, Consuelo Martínez, Jaime Álvarez, Dani García y por supuesto el entrañable Pedro Candel, entre otros muchos, nos obsequiaron con conferencias magistrales. <<

[96] http://www.welivesecurity.com/la-es/2014/05/27/protege-router-5-rapidos-consejos/ <<

[97] http://articulos.softonic.com/wifi-consejos-seguridad?ex=SWH-1566.0 <<

[98] http://nypost.com/2015/03/01/terrorists-using-ebay-and-reddit-to-send-coded-messages-mossad/ <<

[99] La extensa entrevista a MarkoSS88 puede leerse íntegramente en: http://www.loshombresquesusurranalasmaquinas.blogspot.com.es/2015/09/entrevista-mi-asesino.html <<

[100] navajanegra.com <<

[101] https://www.jcea.es/ <<

[102] http://podcast.jcea.es/podcast1984 <<

[103] http://www.20minutos.es/noticia/2553811/0/facebook/trucos-secretos/quien-accede-tu-cuenta/

http://elcomercio.pe/redes-sociales/facebook/facebook-como-saber-quien-entro-tu-cuenta-y-cinco-consejos-mas-noticia-1840164 <<

[104] http://www.abc.es/tecnologia/20150908/abci-porno-fotos-secretas-201509082220.html <<

[105] XKeyscore es un sistema de búsqueda de datos en internet utilizado por la Agencia de Seguridad Nacional (NSA) conjuntamente con otros organismos internacionales como la Oficina de Seguridad de Comunicaciones neozelandesa o la Dirección de Señales de Defensa australiana. El programa es capaz de identificar la nacionalidad del usuario, mediante análisis lingüísticos del lenguaje que emplea en los correos interceptados por el buscador, además de procesar los metadatos contenidos en dichos documentos: historial de navegación, nombres, números de teléfono… El fin de toda intimidad en la red. <<

[106] Vigipirate (contracción de «vigilancia» y «pirata») es el sistema nacional de alerta en Francia, desde 1978. Dividido en cinco niveles de amenaza representados por los colores blanco, amarillo, naranja, rojo y escarlata, el atentado contra *Charlie Hebdo* implicó un despliegue total de policías y militares en las calles, el rastreo de las comunicaciones, el incremento de las detenciones… <<

[107] *Diario de un espía*, pág. 51 y ss. <<

[108] Tras el tiroteo en la Rue Toullier, la policía descubrió varios «arsenales» de Ilich, que utilizaba a sus amantes para que le guardasen armas y explosivos. En la casa de una de ellas, en el número 11bis de la Rue Amélie, se encontraron varias granadas M26 pertenecientes al mismo *stock* usado en el atentado de la Publicis Drugstore.Tras su captura, los homicidios de la Rue Toullier le valieron a Ilich su primera condena a cadena perpetua, dictada en 1997. <<

[109] https://www.youtube.com/watch?v=1AzOwK5HZZg <<

[110] http://www.elmundo.es/elmundo/2011/11/12/internacional/1321077669.html <<

[111] https://www.youtube.com/watch?v=TF4DlcUohFk <<

[112] En el IRC: irc.anonops.com puerto: 6667 Puerto SSL: 6697, canales #francophone #OpCharlieHebdo; también en https://webchat.anonops.com. Y en Twitter bajo los *hastahg* #OpCharlieHebdo y #JeSuisCharlie. <<

[113] http://www.musulmanesandaluces.org/hemeroteca/120/Atentado%20Paris%20-%20pruebas%20montaje.htm <<

[114] Le dediqué un capítulo en *El Palestino:* «La crisis de las caricaturas del Profeta», pag. 63 y ss. <<

[115] Durante un viaje a Filipinas, poco después de los atentados, un periodista le preguntó al papa su opinión al respecto. Su respuesta dejó estupefactos a los reporteros, que esperaban una condena incondicional de la matanza. El papa condenó, sí, pero con matices: «No se puede provocar, no se puede insultar la fe de los demás. No puede burlarse de la fe. No se puede. Creo que los dos son derechos humanos fundamentales, tanto la libertad religiosa, como la libertad de expresión. Tenemos la obligación de hablar abiertamente, de tener esta libertad, pero sin ofender. Cada religión tiene dignidad, cualquier religión que respeta la vida y la persona, y yo no puedo burlarme. Y este es un límite. No se puede ofender, o hacer la guerra, o asesinar en nombre de la propia religión o en nombre de Dios. Es verdad que no se puede reaccionar violentamente, pero si Gasbarri [uno de sus colaboradores, que se encontraba a su lado en el avión papal], gran amigo, dice una mala palabra de mi mamá, puede esperarse un puñetazo. ¡Es normal!». <<

[116] El ISIS había reivindicado el atentado de Coulibaly, aunque no el de los hermanos Kouachi, que fue reivindicado por Al Qaeda. <<

[117] Obviamente, y aunque algunos energúmenos simpatizantes de ETA como Sebastián Yanguas así lo creyesen, yo no tuve nada que ver con que Velasco pidiese la extradición de Cubillas. El juzgado número 6 de la Audiencia Nacional llevaba mucho tiempo detrás de la conexión Venezuela-Francia-España de ETA, y ya en febrero de ese año había pedido a Interpol la busca y captura de Cubillas. Aunque me resulta incomprensible que si yo —un periodista *freelance* sin recursos ni apoyos— pude llegar hasta él, los servicios de Información y Inteligencia no lo hayan detenido todavía… <<

[118] *En la piel de una yihadista*, Debate, 2015. <<

[119] *Memorias de un ultra*, de Juanma Crespo (Temas de Hoy, 2005), cuarto título de la Serie Confidencial que yo dirijo, recoge el testimonio en primera persona y escrito desde prisión de Juan Manuel Crespo, miembro de los Guerrilleros de Cristo Rey. <<

[120] Acrónimo de Bondage-Dominación-Sado-Masoquismo, el juego de rol sexual en el que se busca el placer a través del dolor o la sumisión. <<

[121] http://www.owk.cz/ <<

[122] http://xanfarin.com/2007/12/06/doppelganger-analisis-del-parasitismo/ y http://www.incoherencia.com/pasado/this-is-war/doppelganger-iii/ <<

[123] http://www.elladodelmal.com/2011/04/creepy-data.html <<

[124] http://losescepticosvayatimo.blogspot.com.es/2009/06/antonio-salas-victima-de-la-envida-de.html. <<

[125] El temible pirata Roberts es un personaje de la novela *La princesa prometida* de William Goldman, llevada al cine en 1987, que oculta su identidad tras un antifaz, y que esconde un secreto. No se trata de un solo individuo, sino que su traje negro y su antifaz pasan de generación en generación, manteniendo la idea de que el pirata Roberts es inmortal. El nick en Silk Road probablemente no fue escogido al azar. <<

[126] www.museodelespia.com <<

[127] http://museodelespia.com/news-and-events/exito-abrumador-de-la-ia-jornada-de-inteligencia-de-el-mde/ <<

[128] Toma su nombre de una tropa que estuvo en funcionamiento durante la Segunda Guerra Mundial, pionera en la utilización de técnicas de guerra no convencionales y en operaciones psicológicas. http://www.europapress.es/portaltic/internet/noticia-armada-britanica-prepara-batallon-cibersoldados-20150202111858.html <<

[129] http://www.europapress.es/ceuta-y-melilla/noticia-borran-pintadas-aparecidas-barrio-melilla-favor-daesh-estado-islamico-20150413144608.html <<

[130] http://vozpopuli.com/actualidad/56053-investigan-una-pintada-en-lepe-con-el-mensaje-lo-de-charlie-hebdo-fue-poco-lo-peor-esta-por-llegar <<

[131] http://www.antifeixistes.org/8614_atacs-islamofobs-a-lestat-espanyol-lextrema-dreta-tracta-de-teure-profit-de-la-massacre.htm

http://politica.elpais.com/politica/2015/09/06/actualidad/1441569646_315615.html
<<

[132] http://www.amazon.es/Al-Andalus-2-0-ciber-yihad-contra/dp/8461679911 <<

[133]
http://www.elmundo.es/internacional/2015/08/26/55de1fb846163f94028b45a7.html
<<

[134] Ver *Operación Princesa.* <<

[135] http://www.dcclothesline.com/2015/05/18/french-mayor-we-must-ban-the-muslim-faith-in-france/ <<

[136] Temas de Hoy, 2005. <<

[137] www.fpdeseo.org <<

[138] http://www.museodelespia.com/news-and-events/mauro-el-pequeno-espia/ <<

[139] http://www.emad.mde.es/CIBERDEFENSA <<

[140] http://elpais.com/diario/2010/01/24/domingo/1264308753_850215.html <<

[141] http://www.viruslist.com/sp/hackers/news?id=208275460 <<

[142] Por ejemplo, en http://map.norsecorp.com <<

[143] Sus atribuciones están recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. <<

[144] https://www.ccn-cert.cni.es/ y @CCNCERT <<

[145] https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html <<

[146] www.cnpic.es <<

[147] *Securitecnia,* núm. 409, junio de 2014, pág. 36 y ss. <<

[148] Eric Filiol y Thibaut Scherrer, «Securing Cities with CCTV? Not so Sure. A Urban Guerilla Perspective», 2013. <<

[149] http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html <<

[150] http://www.tecnoxplora.com/internet/ciudad-con-ley/ <<

[151] http://marketingnize.com/no-concibo-un-futuro-sin-ciberdelincuencia-y-por-lo-tanto-un-futuro-con-una-identidad-virtual-legitima-que-destierre-al-anonimato-retoblog/ <<

[152] En 2008 la Policía Municipal de Coslada (Madrid) protagonizó un escándalo al denunciarse una trama de corrupción, extorsión, cohecho, tenencia ilícita de armas, blanqueo de capitales, etcétera, encabezada por su jefe de Policía, Ginés Jiménez. <<

[153] Ver «El Celebgate». <<

[154] En un reportaje del programa *Crónica* de TVE titulado «Acoso en la sombra» se desarrolla perfectamente este caso y otras investigaciones de la Brigada de Investigación Tecnológica del CNP. <<

[155] http://www.elmundo.es/ciencia/2014/06/09/539589ee268e3e096c8b4584.html
<<

[156] http://www.mediapart.fr/journal/international/171213/espana-2013-el-resurgir-del-movimiento-neonazi o https://larmurerie.wordpress.com/2013/12/23/les-neonazis-gagnent-du-terrain-en-espagne/ <<

[157]
http://onemagazine.doopaper.net/publicacion/onemagazine/onemagazine12/FEBRERO 2015-La-revista-para-las-personas-influyentes-En-Portada-Agentes-secretos--servicios-de-inteligencia--contraespionaje--Ent.html <<

[158] https://www.youtube.com/watch?v=jEqTd5WD0U8 <<

[159] En el ámbito del hacking se denomina «Judas» a una fuente que revela información clasificada o sustraída de un sistema informático, por tener acceso directo a ella. El empleado recién despedido de una empresa, el exmarido que divulga fotos comprometidas de su pareja, etcétera. <<

[160] También me resultaron fascinantes las conferencias de Pablo Fernández Burgueño, a quien debemos la histórica sentencia del derecho al olvido en Google; Valentín Martín, que nos enseñó a manejar racionalmente los navegadores; Deepak Daswani, que nos alertó sobre las conexiones wifi; Jesús María González, afrontando el incómodo tema de las agresiones a menores en la red; Pablo San Emeterio y Jaime Sánchez, que nos advirtieron sobre los peligros ocultos en las apps del móvil; Juan Luis G. Rambla, que explicó a los padres para qué vale el control parental; los siempre divertidos Lorenzo Martínez y Juan Garrido, o el académico Víctor A. Villagra, entre otros. Todos ellos magistralmente presentados por Mónica Valle, la copresentadora del imprescindible programa *Mundo Hacker.* <<

[161] *La caja fuerte de los evasores*, La Esfera de los Libros, pág. 113. <<

[162] En agosto de 2013, el sargento Bradley Manning (ahora Chelsea Elizabeth Manning), analista de Inteligencia destinado en Bagdad durante la ocupación, fue condenado por un tribunal militar a una pena de treinta y cinco años de cárcel como responsable de haber filtrado a Wikileaks los miles de documentos publicados por los hacktivistas. <<

[163] Idem, pág. 92. <<

[164] Idem, pág. 161. <<

[165] Idem, pág. 107. <<

[166] Idem, pág. 181. <<

[167] Ángel Suárez, alias «Casper», lideró durante años una de las bandas del crimen organizado más activas de España. Condenado a noventa años de cárcel en abril de 2015, su banda sumó una pena de 261 años de prisión, incluyendo a su contable, que terminó coincidiendo con Falciani en prisión. <<

[168] Idem, pág. 173. <<

[169] Idem, pág. 152. <<

[170] Debate realizado por INCIBE, con la presencia de altos mandos militares, el Gobierno y varias empresas del IBEX35: http://www.7enise.webcastlive.es/webcast7.htm <<

[171] Por desgracia para Epsylon, antes de que acabase el año se publicaría la noticia de que esa conexión había dejado de ser segura. Un par de hackers habían presentado las vulnerabilidades de los Iridium en una CON, con el consiguiente parcheado de los responsables. Al enviarme el enlace a la noticia, añadió un comentario irónico: «Tendré que buscar otra manera de entrar en la red…». http://securityaffairs.co/wordpress/39510/hacking/hacking-iridium-network2Ehtml
<<

[172] http://www.publico.es/ciencias/tecnologia/hackers-espanoles-preguntan-bill-gates.html <<

[173] http://www.rtve.es/noticias/20101007/redsos-impulsores-del-manifiesto-contra-ciberataque-sgae-cultura-tapar-boca-alguien-no-manera-protestar/359803.shtml <<

[174] http://www.securitybydefault.com/2010/10/como-se-defendio-la-sgae-de-anonymous.html <<

[175] https://www.youtube.com/watch?v=iychhMO3hZQ <<

[176] http://www.nodo50.org/briega/node/669 <<

[177] https://www.youtube.com/watch?v=CdaAbVKHxGw (en el minuto 1:35 aparece un famoso futbolista español, que jugaba en la época en Ámsterdam, dando su apoyo personal a la manifestación). <<

[178] http://hacksol.tomalaplaza.net/cronologia-de-las-redes-el-movimiento-15m/ <<

[179] Por ejemplo el prestigioso diario británico *The Guardian:* http://www.theguardian.com/technology/2010/jan/05/mr-bean-hacker-zapatero <<

[180] Mucho antes de que todo esto ocurriese, Lord Epsylon ya impartía conferencias analizando los ataques de denegación de servicio en el ámbito del hacktivismo. Algunas todavía se pueden localizar en la red: http://giss.tv/dmmdb//contents/ddos_small-dl.ogg o http://www.sindominio.net/hackmeeting/wiki/2006/nodos/netstrike. Incluso su participación en la RootedCON 2012, donde presentó una nueva herramienta: https://vimeo.com/42466699 <<

[181] http://seclists.org/fulldisclosure/2009/Jul/279 <<

[182] http://colarebo.com/2010/10/25/la-oposicion-venezolana-roba-y-manipula-el-documental-el-palestino-de-antonio-salas/ <<

[183] http://hipertextual.com/2012/08/anonymous-detiene-a-hacker-espanol <<

[184] http://www.20minutos.es/noticia/1078201/0/policia/cupula/anonymous/ <<

[185] http://www.elconfidencial.com/tecnologia/2013-07-09/el-pp-denuncia-a-anonymous-por-revelacion-de-secretos-al-filtrar-su-contabilidad_766379/ <<

[186] http://www.periodistadigital.com/politica/partidos-politicos/2013/07/08/hacker-contabilidad-pp-1990-2011-barcenas.shtml <<

[187] http://www.elconfidencial.com/tecnologia/2013-07-08/anonymous-publica-la-contabilidad-del-pp-desde-1990-hasta-2011_766387/ <<

[188] http://www.elmundo.es/elmundo/2011/06/12/espana/1307832007.html <<

[189] http://focusecuador.net/2015/09/02/the-guardian-se-hace-eco-de-exclusiva-de-focus-assange-es-investigado-por-inteligencia-de-ecuador/ <<

[190] http://03c8.net/dkdf.html <<

[191] El artículo original, en inglés, puede consultarse en: https://bitcoin.org/bitcoin.pdf <<

[192] Desde su irrupción en la red, periodistas de todo el mundo han intentado descubrir la verdadera identidad del genial Satoshi, y muchos nombres han tratado de poner cara al padre del Bitcoin: Vili Lehdonvirta, Shinichi Mochizuki, Gavin Andresen, Jed McCaleb, Ross William Ulbrich, Michael Claro, Neal Rey, Vladimir Oksman, Charles Bry, Nick Szabo, Dorian Nakamoto, Hal Finney… Pero todos negaron ser Satoshi. <<

[193] Las conchas a las que se refiere Epsylon son los caurí. Se cree que la palabra *cauri* deriva del término hindú *kauri*. Son conchas de gasterópodos de la familia Cypreidas, muy codiciadas por los coleccionistas. La especie que se utilizó como moneda es conocida como *Monetaria Moneta* y procede exclusivamente de las islas Maldivas, en el océano Índico. Hay muchas referencias históricas ya escritas sobre el tema. Por ejemplo: http://www.taringa.net/posts/apuntes-y-monografias/13259506/Cauri-una-moneda-singular.html <<

[194] https://github.com/epsylon - http://03c8.net/ <<

[195] https://nlnet.nl/project/xsser/ <<

[196] Taller Orbitando Satélites: LABoral Gijón 2011: https://www.youtube.com/watch?v=-OleYS6Poj0 <<

[197] Epsylon junto con sus colegas hacktivistas nos muestra cómo es posible escuchar a la Estación Espacial Internacional desde una antena construida con tubos y alambres: https://www.youtube.com/watch?v=0l3gPf5BDjA <<

[198] De hecho, existen ya varios precedentes:

http://www.taringa.net/posts/ciencia-educacion/16714822/Unico-Hackeo-de-Senal-de-TV-abierta-en-1987-Exitoso-EUA.html

http://www.abc.es/medios-redes/20130212/abci-television-informa-ataque-zombie-201302121024.html

Documental: Hackers del espacio: https://www.youtube.com/watch?v=6Y1iEIUYMdw

Incluso el Ejército Islamico hackeó en 2015 la señal del canal de TV francés TV5Monde: http://www.elpais.com.uy/mundo/islamico-hackea-canal-tv-frances.html <<

[199] La Asamblea General de la ONU proclamó la DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS como «ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos, tanto entre los pueblos de los Estados Miembros como entre los de los territorios colocados bajo su jurisdicción». Y por si alguien lo ha olvidado: http://www.un.org/es/documents/udhr/ <<

[200] Ver capítulo 8, «Los hackers de ETA». <<

[201]
http://www.criptored.upm.es/descarga/ConferenciaRomanRamirezTASSI2013.pdf <<

[202] http://actualidad.rt.com/ultima_hora/view/117808-facebook-premio-vulnerabilidades <<

[203]
http://www.wsj.com/articles/SB10001424052748703467304575383203092034876
<<

[204] http://www.cnet.com/news/report-of-fbi-back-door-roils-openbsd-community/ <<

[205] En realidad, poco antes Chema Alonso ya le había dedicado una entrada a este tema en su blog: http://www.elladodelmal.com/2014/07/tor-confirma-que-el-anonimato-se-rompio.html <<

[206] http://securityinside.info/hacking-team-pwned/ <<

[207] Blackwater, fundada en 1997 por Al Clark y Erik Prince para proporcionar apoyo a la formación de organizaciones militares y policiales. Prince comparaba lo que Blackwater quería hacer por el Ejército norteamericano con lo que FedEx hizo por su servicio postal. Después de dar formación a los SEAL y SWAT, grupos de operaciones especiales del Ejército y la Policía, Blackwater recibió su primer contrato oficial con el Gobierno en 2000, tras el atentado yihadista contra el USS Cole en Yemen. Durante la guerra de Irak, efectivos de Blackwater participaron en la ocupación. En 2007, el Gobierno de Irak presentó cargos contra muchos de esos efectivos, por las atrocidades que habían realizado con la población civil durante la ocupación. Varios ya han sido condenados. <<

[208] www.noconname.org <<

[209] Tinfoleak es un producto de Internet Security Auditors, la empresa liderada por Fernández Bleda y Aguilera. <<

[210] El libro original de Ondargáin está disponible *online* en: http://ondargain3.tripod.com/id12.html <<

[211] http://milagrosdeallah.blogspot.com.es/

http://muhammadabdallah.blogspot.com.es/ <<

[212] http://muyseguridad.net/2015/05/23/adult-friend-finder-hack/ <<

[213] http://www.publico.es/sociedad/clientes-ashley-madison-suicidan-filtracion.html <<

[214] http://elpais.com/elpais/2015/08/20/media/1440085688_610035.html <<

[215] *Interviú,* núm. 2.054, septiembre de 2015. <<

[216] Arturo Pérez Reverte expresó toda la rabia que sintió la sociedad con las acosadoras de Carla, con un artículo titulado «Esas jóvenes hijas de puta». http://www.perezreverte.com/articulo/patentes-corso/971/esas-jovenes-hijas-de-puta/ <<

[217] http://www.taringa.net/posts/noticias/17275353/Responsabilizan-a-Ask-fm-por-suicidio-de-4-menores.html <<

[218] Su página en español es: itgetsbetter.es. <<

[219] http://www.abc.net.au/news/2014-02-23/charlotte-dawson-death-puts-focus-on-cyber-bullying/5277904 <<

[220] http://noticiasymasnoticia.blogspot.com.es/2013/11/nuevo-caso-de-chica-que-anuncia-su.html,

http://www.larazon.es/historico/9292-anuncia-su-suicidio-en-facebook-y-no-lo-evita-ninguno-de-sus-1-082-amigos-HLLA_RAZON_351648#.Ttt1GTJkdqgAF49,

http://noticias.terra.com/mundo/latinoamerica/joven-mexicano-anuncio-en-facebook-su-intencion-de-suicidio,ae0d8ce716a79fecc0dad2a792ea6bd3tcjvRCRD.html <<

[221] http://www.que.es/ultimas-noticias/espana/201304061016-fotos-porno-whatsapp-desarticulan-grupo-cont.html <<

[222] http://www.granadablogs.com/juezcalatayud <<

[223] «Llevo como juez de menores desde 1988 y nunca he condenado a un gitano por maltratar a sus padres. Y si lo normal en los casos que llevo de menores es un porcentaje de 25% niñas, frente al 75% niños, en el maltrato a los padres es un 40 o 45% niñas frente a un 55 o 60% niños. Las niñas ya casi maltratan tanto a sus padres como los chicos…» <<

[224] http://www.abc.es/familia-padres-hijos/20140110/abci-contrato-madre-iphone-201401091035.html <<

[225] http://uesonoliva.blogspot.com.es/p/plantilla-2010-11.html <<

[226] Ignacio Santiago lo explica perfectamente en su blog: http://ignaciosantiago.com/blog/todo-lo-que-tienes-que-saber-sobre-las-estafas-en-internet/ <<

[227] http://www.elladodelmal.com/2010/10/enterprise-spoofing-para-captar-mulas.html y http://elblogdeangelucho.com/elblogdeangelucho/blog/2012/08/27/quieres-ser-mi-mula-pago-bien/, respectivamente <<

[228] http://www.abc.es/20120521/espana/abci-ofertas-falsas-trabajo-internet-201205201300.html <<

[229] https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf <<

[230] https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3440.pdf <<

[231] http://www.securitybydefault.com/2011/01/steampunk-el-siglo-xix-acude-al-rescate.html <<

[232] Ver capítulos 12 y 14. <<

[233] http://perseuslegal.com/ <<

[234] http://www.eldiario.es/turing/Hacker-presunto-culpable_0_140336061.html <<

[235] *La caja fuerte de los evasores*, La Esfera de los Libros, 2015, pág. 240. <<

[236] http://www.larazon.es/espana/colau-prepara-su-propio-servicio-de-inteligencia-GH10249708#.Ttt1fX9JihmRqtZ <<

[237] http://dvidal.intel.press/ <<

[238] https://wikileaks.org/plusd/cables/06DAMASCUS5399_a.html <<

[239] https://wikileaks.org/hackingteam/emails/ <<

[240] cyber-berkut.org/en <<

[241] http://www.welt.de/politik/deutschland/article136114277/Cyber-Angriff-auf-Kanzleramt-und-Bundestag.html <<

[242] http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316 <<

[243] http://en.interfax.com.ua/news/general/197607.html <<

[244] http://sputniknews.com/voiceofrussia/news/2014_05_23/CyberBerkut-announces-destruction-of-electronic-system-of-Ukraines-Central-Election-Commission-5809/ <<

[245] http://actualidad.rt.com/actualidad/179860-hackers-rodaje-ejecucion-estado-islamico-mccain <<

[246] http://www.periodistadigital.com/america/legislacion-y-documentos/2015/07/13/el-vídeo-de-unos-hackers-que-pretende-demostrar-que-las-ejecuciones-del-ei-son-montajes-grabados-en-un-estudio-de-cine.shtml <<

[247] http://www.elmundo.es/blogs/elmundo/orilla-sur/2014/11/28/el-discreto-apoyo-de-espana-a-marruecos.html <<

[248] http://www.arso.org/ColemanPaper.htm. <<

[249] http://blogs.periodistadigital.com/desdeelatlantico.php/2014/10/10/wilikeaks-del-majzen-graves-secretos-del http://www.elmundo.es/blogs/elmundo/orilla-sur/2014/10/22/wikileaks-en-marruecos-un-culebron-con.html <<

[250] http://www.moroccoworldnews.com/2014/12/147162/moroccan-hacker-group-reveals-identity-of-chris-coleman/ <<

[251] Ya en 2010, y tras una encuesta entre sus lectores, el blog Hack Players lo eligió como el hacker más famoso de España. Chema agradeció el premio con una entrada en su blog, recordando además a otros muchos compañeros que, en su opinión, merecían también ese reconocimiento: http://www.elladodelmal.com/2010/01/el-hacker-mas-famoso-de-espana.html <<

[252] De Carlos Álvarez Martín, Pablo González Pérez, Juan Miguel Aguayo Sánchez, Pablo González, David Puente, Rames Sarwat, Miguel Ángel Gastesi Urroz, Daniel López Creus, Daniel, Enrique Rando, Juan Garrido García Rambla, Juan Luis Alonso Cebrián o el mismo Chema Alonso, entre otros. <<

[253] https://www.youtube.com/user/Chemai64 <<

[254] http://elpais.com/diario/2006/07/27/ciberpais/1153965749_850215.html <<

[255] *Cibercrimen*, pág. 205. <<

[256] http://www.bolsamania.com/noticias/tecnologia/la-nevera-de-samsung-que-utilizan-los-hackers-para-robar-tus-datos-gmail--842199.html <<

[257] En realidad, el 30 de abril de 2014 ya se había emitido un capítulo piloto insertado en la temporada 14 de *CSI: Las Vegas* titulado «CSI-Cyber» para sondear la aceptación entre el público. <<

[258] Cálico Electrónico es una serie cómica de animación *flash* distribuida gratuitamente a través de internet. Su primer capítulo se estrenó el 1 de junio de 2004 y se emitió el último a través de su canal de YouTube el 1 de mayo de 2015. Ambientada en una metrópolis llamada Electronic City, el protagonista es un superhéroe de figura contraria a la clásica (bajito, gordinflón y sin superpoderes) y de nacionalidad española, que una y otra vez arriesga su vida para salvar a la ciudad. Asimismo, en todos los capítulos adquiere diversos artilugios en la tienda ElectronicaWeb. Cada capítulo incluye las tomas falsas del «rodaje». Su creador es Niko, y con su equipo Nikodemo Animation hace diferentes animaciones de *flash* de todo tipo, generalmente del género de la comedia. Debido a la falta de fondos, el propio Niko comunicó el «cierre» del equipo (después de más de cinco años), poniendo fin a la serie de Cálico y todos los derivados de la serie hasta que alguien pueda continuar y mantenerla. Recientemente, Cálico ha vuelto gracias a que la empresa Informática 64 recuperó los derechos.

El Gran Dimitri es un personaje del programa *Mundo Hacker* que parodia la figura del ciberdelincuente al que todo le sale mal. Tuvo tal éxito en su primera aparición en el programa, rescatado de un vídeo de YouTube, que terminaron adoptándolo como un personaje fijo interpretado por Yanko Vasilev. <<

[259]. http://www.elladodelmal.com/2015/07/los-10-hits-de-peticiones-ilegales-del.html

http://www.elladodelmal.com/2014/07/en-julio-tampoco-voy-hacer-estas-cosas.html
http://www.elladodelmal.com/2012/07/buscas-criminales-no-hackers.html <<

[260] http://www.elladodelmal.com/2013/02/un-escarmiento-maligno-para-una.html
<<

[261] http://www.elladodelmal.com/2013/05/ola-k-ase-me-montas-un-gobierno-in.html <<

[262] https://pbs.twimg.com/media/B_Mx2ehU0AEn5RC.jpg <<

[263] http://www.abc.es/20111122/medios-redes/abci-facebook-seis-grados-201111221734.html <<

[264] http://www.lanacion.com.ar/1822778-facebook-llego-a-1000-millones-de-usuarios-conectados-en-un-solo-dia <<