

FANCY BEAR SE VA DE *PHISHING*

LA OSCURA HISTORIA DE LA ERA
DE LA INFORMACIÓN EN CINCO
HACKEOS EXTRAORDINARIOS

SCOTT J. SHAPIRO



UNA NOTA SOBRE EL AUTOR

Scott J. Shapiro es el profesor «Charles F. Southmayd» de Derecho y profesor de Filosofía en la Facultad de Derecho de Yale y director del Centro Yale de Derecho y Filosofía y el Laboratorio de Ciberseguridad de Yale. También es el autor de *Legalidad* y coautor, junto a Oona A. Hathaway, de *The Internationalists: How a Radical Plan to Outlaw War Remade the World*.

CONTENIDO

Agradecimientos	6
Una nota sobre el autor	8
Introducción: El proyecto brillante	13
Crecer en Nueva Jersey	16
1. El gran gusano	35
La historia antigua de la ciberseguridad	37
De Multics a UNIX	41
<i>Juegos de guerra</i>	44
Bob Morris	49
Diseción del gusano	51
«Idiota»	57
¿Qué es Internet?	58
La lección del gusano	64
2. Cómo la tortuga hackeó a Aquiles	71
Aquiles y la tortuga	73
Código y datos	76
<i>Upcode</i> delictivo	78
El jurado como un ordenador	81
La ambigüedad del código y los datos	84
¡Desbordamiento!	88
Código oculto en datos	92
«Se la cargó a las primeras de cambio»	94
Robert sube al estrado	96
La sentencia	99
3. La fábrica de virus búlgara	103
Ordenador para ti	105
Vienna	108
La fábrica	110

El malware es asqueroso	116
¿Qué son los virus?	117
¿Qué es un gusano?	120
Dark Avenger	123
4. El padre de dragones	127
Johnny von Neumann	130
El misterio de la autorreplicación	133
El constructor universal	135
Contener tu propio código	139
Entra en escena Sarah Gordon	142
Motor de mutación	144
El Silicon Valley del Este	148
Psicología moral del creador del virus	152
Madurar	155
Dark Avenger y Sarah Gordon	157
¿Quién es Dark Avenger?	160
5. El ganador se lo lleva todo	163
Sistemas operativos	166
El ganador se lo lleva todo	169
«No estaban en Silicon Valley»	172
Jardines cercados	176
El maremoto de Internet	180
Supercontagiadores	183
Melissa, ILOVEYOU	185
El <i>upcode</i> del <i>downcode</i>	189
El 11 de septiembre y la vigilancia masiva	194
Informática de Confianza	199
Dualidad moral	201
«Esto es mío»	205
6. Snoop Dogg hace la colada	209
Inyección SQL	211
El código invisible	214
Cameron LaCroix	217
Tiene fotos desnuda	220
Autenticación	222
En sincronía	222
«Paris, lo siento»	227

7. Cómo utilizar un <i>mudge</i>	233
Linda, la cajera feminista	235
Correos representativos	238
Disponibilidad y afectividad	241
Aversión a la pérdida	245
Typosquatting	248
Carácter físico revisado	251
Sistemas 1 y 2	255
8. <i>Kill Chain</i>	259
Fancy Bear	261
Vigilancia e intrusión	263
Proxies	269
Cozy Bear	272
El <i>upcode</i> del espionaje	276
Los Guccifers	281
22 de julio	284
La identidad falsa	286
¿A qué juegan?	292
9. Las guerras de Minecraft	299
21 de octubre	303
Ataque al registro de la universidad	306
Integración vertical	308
Minecraft	311
MalWar	314
El crimen como servicio	316
Poodle Corp	322
Mirai Nikki	325
El último que queda en pie	326
10. El ataque de las tostadoras asesinas	329
Las <i>botnets</i> de agosto	331
Anatomía de una <i>botnet</i>	333
Activar la tostadora	336
Mirai contra Google	337
El <i>Kill Chain</i> del FBI	340
Farsantes en el ciberespacio	343
Reyes del ciberespacio	344
Divulgación irresponsable	348
Los siguientes pasos de Mirai	350
Atacar a un perro con filete	352
El <i>downcode</i> nunca es suficiente	355

Conclusión: la muerte del solucionismo	359
Soluciones de <i>upcode</i>	361
A. Ciberdelincuencia	363
B. Ciberespionaje	383
C. Guerra cibernética	396
Epílogo	413
Índice alfabético	419

INTRODUCCIÓN: EL PROYECTO BRILLANTE

«Creo que la he jodido de verdad». Paul sabía que Robert estaba en problemas serios. El silencioso estudiante de posgrado de veintidós años con gafas nunca decía tacos. Más tarde, Paul testificaría en el juicio de Robert que su amigo era «bastante puritano en la forma de hablar. Por eso pensé que tenía que haber salido mal algo muy importante».¹

Y algo muy importante había salido mal. El amigo de Paul se había cargado Internet. La llamada se produjo a las once de la noche del 2 de noviembre² de 1988. Robert Morris Jr., un estudiante de doctorado de informática en Cornell, describió el desastre que estaba teniendo lugar a Paul Graham, un estudiante de posgrado de Harvard.

Más temprano esa misma noche, sobre las ocho de la tarde, Robert se sentó frente a un terminal en la Sala 4160 de Upson Hall, entonces sede del departamento de informática de Cornell en Ithaca, Nueva York,³ e inició sesión de manera remota en `prep.ai.mit.edu`, un ordenador VAX 11/750 en el laboratorio de Inteligencia Artificial del MIT, en Cambridge, Massachusetts.

Transfirió y ejecutó tres archivos, lanzando así lo que él y Paul habían denominado «el proyecto brillante», un programa con autorreplicación..., un «gusano» informático.⁴

1. Testimonio de Paul Graham, transcripción de *EE. UU. contra Robert Tappan Morris*, p. 986.
2. Todas las horas están en EST (hora estándar oriental).
3. Testimonio de Dawson Dean, transcripción de *Morris*, p. 574. La sede actual está en Bill & Melinda Gates Hall.
4. Donn Seeley dice que son las seis de la tarde, PST (hora estándar del Pacífico), que son las nueve de la noche EST. Indica: «11/21: 18:00 (aprox.): Esta fecha y esta hora se vieron en archivos del gusano encontrados en `prep.ai.mit.edu`... Los archivos se eliminaron más tarde y se perdió la hora exacta. El registro del sistema en preparación llevaba dos semanas estropeado. El sistema no lleva una contabilidad y los discos no tienen copia de seguridad en cinta: un objetivo perfecto». Donn Seeley, «A Tour of the Worm», 1988, <http://www.cs.unc.edu/~jeffay/courses/nids05/attacks/seeley-RTMworm-89.html>. En el juicio, Robert Morris Jr. testificó: «Lo liberé, creo, sobre las ocho de esa noche». Transcripción de *Morris*, p. 1097. Dawson Dean informó de que había visto a Robert en un terminal de Sun «a última hora de la tarde, así que serían sobre las ocho». Transcripción de *Morris*, p. 874.

El gusano estaba programado para infectar ordenadores en la entonces naciente Internet. Después de que se infiltrase en un ordenador, ese ordenador serviría como base desde la que infectar otros. Con cada nuevo objetivo, el gusano se copiaría a sí mismo y enviaría a su clon a un nuevo hogar. Trabajando en tándem, el gusano y sus clones seguirían multiplicándose hasta que hubiesen completado su misión y colonizado Internet al completo.

La motivación de Robert era puramente científica; quería crear un programa que pudiese explorar el ciberespacio. Estaba intentando infectar tantos ordenadores como pudiese solo para ver cuántos podía infectar, no para causar estragos estropeándolos. Pero, cuando Robert volvió de la cena para comprobar el progreso de su experimento, se dio cuenta de que la red iba muy lenta.

Había un retraso evidente entre el momento en que se tecleaban los caracteres y el momento en que aparecían en la pantalla y entre la orden y la ejecución. El gusano estaba propagándose con demasiada rapidez y consumía demasiados recursos. Había pasado como un búmeran de Cambridge de vuelta a Ithaca en menos de tres horas y estaba apoderándose de la red de su departamento. Y eso fue solo el principio.

El gusano de Robert no solo inutilizó la red de Cornell; estaba arrasando Internet, aplastando todo lo que encontraba a su paso. Solo unos minutos después de su lanzamiento en el MIT, la primera impresión conocida del gusano se produjo en la universidad de Pittsburgh.⁵ Desde Pittsburgh, el gusano atravesó el país a toda velocidad y llegó a rand.org, la red de RAND Corporation en Santa Mónica, California, a las 8:24 de la tarde. En menos de una hora, los directores informáticos de RAND se dieron cuenta que su red estaba ralentizándose; varios nodos estaban paralizados. A las 9:00 de la noche, se detectó al gusano recorriendo el Instituto de Investigación de Stanford. Para las 9:30 de la noche, estaba en la universidad de Minnesota. A las 10:04, se infiltró en la máquina con la puerta de enlace de Berkeley, el ordenador que servía como portal a Internet de la universidad. Casi de inmediato, los administradores informáticos se dieron cuenta de que había una carga inusualmente grande en la máquina y una acumulación de procesos pendientes en su sistema. A medianoche, los administradores del MIT volvieron de tomarse un helado y descubrieron que su red también estaba fallando. A la 1:05 de la madrugada, el gusano penetró en el Laboratorio Nacional Lawrence Livermore, una instalación responsable de la seguridad del arsenal nuclear del país. Pronto el gusano se había metido en el

5. Eugene Spafford, «The Internet Worm Program: An Analysis», Purdue Technical Report CSD-TR-823, 29 de noviembre, 1988, 2, <https://spaf.cerias.purdue.edu/tech-reps/823.pdf>.

Laboratorio Nacional de Los Álamos, en Nuevo México, el hogar del Proyecto Manhattan y de las primeras bombas atómicas del mundo. El proyecto brillante de Robert ya no parecía tan brillante.

La situación en la universidad de Utah era típica. El primer ataque a cs.utah.edu se produjo justo después de medianoche, a través del sistema de correo electrónico, a las 12:09. En menos de once minutos, la carga de la red (la cantidad de datos transportados por la red) llegó a 5. En una noche normal, la carga estaba entre 0,5 y 2. Un 5 significaba una ralentización; un 20 sería un colapso. A las 12:41 de la noche, la carga en Utah había subido a 7. Veinte minutos más tarde, a 16. Cinco minutos más tarde, se cayó toda la red. Jeff Forys, el administrador de Utah, derrotó a los invasores uno por uno hasta que desaparecieron todos, solo para volver con fuerza menos de una hora después. La carga llegó a 27. A la 1:49 de la noche, Forys desconectó la red, lo cual mató a unos cuantos intrusos. Pero, cuando volvió a conectarla, atacó otro grupo. La carga se disparó hasta 37 y Forys era incapaz de reducirla. Contener a los gusanos a mano⁶ ya no funcionaba.

El teléfono despertó a Dean Krafft, jefe de las instalaciones informáticas en Upson Hall, donde Robert Morris había lanzado su funesto experimento. «A la una y media de la noche, recibí una llamada de un estudiante de postgrado sénior del departamento diciendo que parecía que había un problema de seguridad y que varias máquinas estaban fallando»,⁷ testificó Krafft más tarde. El veinte por ciento de los ordenadores del departamento de Cornell estaban paralizados. Cuando las máquinas se apagaban y se reiniciaban, funcionaban durante un breve periodo de tiempo y volvían a congelarse. Krafft dijo al alumno que desconectase los ordenadores del departamento⁸ de la red principal del campus. (Cornell tuvo suerte. En Carnegie Mellon, se vieron afectados ochenta de cien ordenadores; en la universidad de Wisconsin, doscientos de trescientos. Bell Labs,⁹ la rama de investigación y desarrollo del gigante de la telefonía AT&T, no se vio afectada).

A las 2:38 de la mañana, Peter Yee del Centro de Investigación Ames de la NASA compartió la primera advertencia pública en la lista de correo TCP-IP, el principal tablón de anuncios público para noticias relacionadas con Internet.

6. Para ver una cronología, consulta Seeley, «A Tour of the Worm», p. 2.

7. Testimonio de Dean Krafft, transcripción de *Morris*, p. 132.

8. Krafft, transcripción de *Morris*, p. 134.

9. John Markoff, «How a Need for Challenge Seduced Computer Expert», *The New York Times*, 6 de noviembre, 1988.

3. LA FÁBRICA DE VIRUS BÚLGARA

Vesselin Bontchev¹ no sabía leer alemán. Era investigador júnior en el Instituto de Robótica y Cibernética Industrial de la Academia de Ciencias de Bulgaria en Sofía, la capital del país. Durante unas largas vacaciones en Múnich en 1989, se topó con un libro escrito por el profesor Klaus Brunnstein, de la universidad de Hamburgo, llamado *Computer-Viren-Report: Gefahren, Wirkung, Aufbau, Früherkennung, Vorsorge*² (*Informe sobre virus informáticos: peligros, efectos, estructura, detección temprana y prevención*). Vesselin estaba fascinado por los virus informáticos, así que lo compró.

Debido a la barrera lingüística, solo podía leer el apéndice técnico al final del libro, escrito en inglés. Sin embargo, Vesselin pudo ver en las explicaciones que el profesor Brunnstein había cometido numerosos errores. Así pues, Vesselin escribió una carta larga en inglés al profesor Brunnstein en la que detallaba los errores. Era valiente, incluso ingenuo, que un investigador júnior hiciese algo así.

Pocas semanas después, un alumno del profesor Brunnstein, Morton Swimmer, escribió a Vesselin con una invitación a la universidad de Hamburgo. Vesselin la rechazó. Volar a Hamburgo desde Múnich era demasiado caro. El ferrocarril era demasiado lento. Haría falta un día entero para cruzar Alemania en tren y Vesselin iba a regresar a Sofía cuatro días después.

Si Vesselin no iba a Hamburgo, Hamburgo iría a Vesselin. Brunnstein envió a Swimmer a Múnich para que se reuniera con Vesselin. Swimmer estaba impresionado. Aquel investigador júnior de Bulgaria sabía de lo que hablaba.

-
1. Material de las dos siguientes secciones extraído de entrevistas realizadas por Zoom a Vesselin Bontchev, 6, 7 y 9 de octubre, 2020 (de aquí en adelante «Entrevista VB»).
 2. Klaus Brunnstein, *Computer-Viren-Report: Gefahren, Wirkung, Aufbau, Früherkennung, Vorsorge* (Múnich: Wirtschaft, Recht und Steuern, 1989).

Varias semanas después de haber vuelto al instituto en Sofía, Vesselin recibió una llamada telefónica de Blagovest Sendov,³ el presidente de la Academia de Ciencias de Bulgaria. Fue una llamada inesperada: Vesselin nunca había conocido al presidente de la academia ni había hablado con él antes. Se quedó todavía más sorprendido por la furiosa acusación del presidente Sendov: «¿Por qué está usted creando virus informáticos?».

Vesselin no creaba virus informáticos. Para él, no haber escrito nunca uno era motivo de orgullo. Lo que hacía era recopilar virus creados por otras personas, la mayoría de los cuales encontraba en ordenadores infectados. Estudiaba esos programas maliciosos para mejorar su software antivirus, que distribuía de manera gratuita. Vesselin incluso publicó la dirección de su casa en la revista informática más importante de Bulgaria; quienes le enviasen un disquete en blanco y un sobre sellado recibirían una copia de su software. Que lo acusasen de escribir virus no solo era falso; era irritante. Vesselin gritó también a Sendov, un funcionario de alto nivel con rango de ministro y el jefe del jefe de su jefe, por la acusación infundada.

Cuando la conversación se calmó, surgió la verdadera historia. Sendov había vuelto de una conferencia sobre ciberseguridad en Jerusalén, donde había conocido al profesor Brunnstein. Brunnstein le había preguntado a Sendov por el experto en virus informáticos de su academia. Sendov no tenía ni idea de quién era y decidió averiguarlo. Cuando contactó con Vesselin por teléfono, su «furiosa acusación» era una broma. No creía que ninguno de los investigadores de la Academia estuviese de verdad creando virus.

Dada la experiencia de Vesselin, Sendov ofreció crear un nuevo laboratorio en la academia especializado en virología informática. A lo largo del año anterior, Bulgaria había experimentado una epidemia repentina de virus informáticos. No solo estaban infectados los ordenadores de la academia; era difícil encontrar un solo ordenador en toda Bulgaria que no lo estuviese. Puesto que los virus informáticos eran patógenos nuevos, muy pocos sabían cómo detenerlos. Sendov esperaba que Vesselin pudiese ayudar.

Ofreció al investigador de veintinueve años ser el nuevo director del laboratorio. Vesselin, sin embargo, no quería dirigir el laboratorio. El trabajo administrativo le resultaba tedioso. La gente le resultaba tediosa. Le gustaba tratar con ordenadores. Son predecibles; los humanos, no.

No obstante, era una oportunidad que no podía dejar pasar. Permitiría a Vesselin trabajar en la materia que amaba. Y no había un lugar mejor que Bulgaria para los amantes de los virus. El país socialista, asediado por la

3. https://en.wikipedia.org/wiki/Blagovest_Sendov.

hiperinflación, las infraestructuras en mal estado, el racionamiento de alimentos y combustible, apagones diarios y jaurías de perros salvajes por las calles, se había convertido en una de las zonas de alta tecnología más activas del planeta. Legiones de jóvenes programadores búlgaros estaban enredando con sus Pravetz-16, clones pirateados de PC de IBM, bombeando virus informáticos que lograban llegar hasta el próspero y brillante Occidente.

Vesselin Bontchev sería el general a cargo de las ciberdefensas de Bulgaria. El presidente Sendov había elegido al hombre adecuado.

Ordenador para ti

Si eras búlgaro y te interesaban los ordenadores a finales de los ochenta, leías religiosamente una revista: *Komputar za vas*⁴ (*Ordenador para ti*). El gobierno búlgaro había lanzado la revista en 1985 para incentivar el interés en los ordenadores personales. Vesselin no solo leía todos los números, sino que también se había convertido en colaborador de la revista.

En 1988, Vesselin tenía veintiocho años y vivía con su madre en un piso de tres habitaciones en Sofía. Nacido en la turística ciudad de Varna, en el Mar Negro, Vesselin era bajo y delgado, con un lunar carnoso en el lado derecho de la boca. Sus padres eran ingenieros; su madre trabajaba en la Academia de Ciencias de Bulgaria como especialista en ingeniería estructural. Vesselin se graduó en la Universidad Técnica de Sofía en 1985 con un título de máster en informática, tras lo cual se unió al Instituto de Robótica y Cibernética Industrial en la Academia de Ciencias de Bulgaria.

En 1988, *Komputar za vas* publicó su primer artículo⁵ sobre virus informáticos. Escrito originalmente en alemán para la revista *Chip*, el artículo predecía una epidemia de virus destructivos que arrollaría a la industria informática.

Chip ilustraba su historia con virus de aspecto alienígena que caían desde el cielo, atacando a disquetes de colores brillantes y derritiéndolos hasta convertirlos en una sustancia viscosa de colores brillantes. *Komputar za vas* contrató a un traductor profesional, pero el traductor no tenía experiencia con ordenadores y produjo una traducción extraña. Por ejemplo, el término alemán para «disco duro» (*festplatte*), se tradujo en búlgaro como «plato duro».⁶ Por suerte, Vesselin corrigió estos errores antes de la publicación.

4. *Komputar za vas* 1-2 (1989): pp. 5-6.

5. «Viruses in Memory», *Komputar za vas* 4-5 (1988): pp. 12-13.

6. «Dr. Vesselin Bontchev: Non-Replicating Malware Has Taken over the Computer Virus», Sensors Tech Forum, 14 de noviembre, 2016, <https://sensorsstechforum.com/dr-vesselin-bontchev-non-replicating-malware-taken-computer-virus/>.

Komputar za vas publicó la traducción búlgara mejorada con la misma ilustración que en Alemania, aunque, al más puro estilo socialista, la imagen se imprimió en un apagado blanco y negro.

Aunque corrigió la traducción, a Vesselin le pareció que el artículo original se equivocaba. Sus advertencias apocalípticas eran extremas. Pero el artículo era acorde al tratamiento que hacían los medios de los virus informáticos, que era sensacionalista e inexacto. Cuando el gusano Morris hizo fallar Internet en noviembre de 1988, los telediarios búlgaros informaron con entusiasmo de que el gusano era capaz de infectar todos los ordenadores del mundo. Vesselin sabía que esa afirmación⁷ era completamente falsa. Como hemos visto, solo se habían infectado dos tipos de ordenadores: VAX y Sun. Todos los demás ordenadores eran inmunes.

Para frenar la histeria, Vesselin escribió un artículo, «The Truth About Computer Viruses», publicado en el número de enero-febrero de 1989 de *Komputar za vas*. El miedo a los virus informáticos estaba convirtiéndose en una «psicosis colectiva, similar al SIDA». Vesselin afirmaba que cualquier programador competente podía saber cuándo un archivo estaba corrompido por un virus. Los archivos infectados son más grandes que los archivos sin infectar. Se ejecutan más despacio. Hacen cosas raras, como reproducir canciones, dibujar árboles de Navidad en la pantalla y reiniciar ordenadores. ¡Era difícil pasar por alto un virus! La prevención mediante la higiene cibernética era tan simple como la detección. «No permita que otras personas utilicen su ordenador; no use productos de software sospechosos; no utilice productos de software adquiridos de manera ilegal».

Más tarde, Vesselin se arrepentiría de aquel artículo.⁸ No se había dado cuenta de que quizá lo que era un virus evidente para él podría no ser tan obvio para una persona en una secretaría que usase un ordenador como máquina de escribir. Además, la mayoría de los usuarios de Bulgaria no tenían su propio ordenador personal; lo compartían. La higiene cibernética era difícil cuando los ordenadores eran de todo menos personales.

Cuando Vesselin escribió este artículo despectivo, todavía no había visto un virus. Todo lo que sabía sobre virus lo había aprendido en artículos académicos. Un año antes, Vesselin estaba en una conferencia sobre ordenadores en Polonia. Preguntó a los participantes si alguna vez habían detectado un virus. Había oído hablar de ellos, pero nunca había observado uno en realidad. Por eso, Vesselin se quedó sorprendido cuando dos hombres entraron en la oficina de *Komputar za vas*, donde él solía pasar el rato, y afirmaron tener un virus. Habían leído los

7. En aquel momento, Vesselin no sabía que el gusano Morris solo podía infectar los Sun y Vax.

8. «Interview with Vesselin Bontchev», *Alive* 1, n.º 1 (abril-julio de 1994).

artículos sobre esas extrañas criaturas nuevas en la revista y querían enseñar a Vesselin el virus que habían descubierto en su pequeña empresa de software. Es probable que Vesselin se quedase igual de sorprendido de que hubiese empresas de software en Bulgaria. En 1989, Bulgaria todavía estaba en plena transición tras el comunismo y las empresas privadas eran poco frecuentes. La gran mayoría del software de Bulgaria era pirata.

Los hombres no solo informaron de que tenían un virus; también afirmaban que habían escrito un programa antivirus que eliminaba el virus. Estaban tan orgullosos que habían llevado su portátil. El portátil tenía un virus. Cuando ejecutaron su programa antivirus, el virus desapareció.

Vesselin estaba al mismo tiempo fascinado y horrorizado: fascinado porque nunca había visto un virus antes (ni un portátil, ya que estamos), y horrorizado porque esos hombres acababan de matarlo. El horror se transformó en pánico cuando los hombres le dijeron que también habían purgado el virus de los ordenadores de su empresa. Vesselin corrió a sus oficinas buscando cualquier resto. Encontró una impresión del código del virus en la basura. Se lo llevó a casa y lo introdujo, byte a byte, en su ordenador. Puesto que el virus tenía una longitud de 648 bytes, tuvo que introducir 1.296 caracteres (cada carácter tiene 4 bits, dos caracteres son 8 bits o 1 byte) más 324 espacios, uno entre cada dos bytes. Para no cometer errores,⁹ introdujo estos caracteres dos veces. Al final, Vesselin se dio cuenta¹⁰ de que había resucitado al virus comúnmente conocido como Vienna.

9. Vesselin no se dio cuenta de que el código fuente que reconstruyó de forma tan meticulosa había sido publicado el año anterior por Ralf Burger, un investigador de seguridad alemán, en la segunda edición de su libro *Computer Viruses: A High Tech Disease* (Londres: Abacus, 1988). Burger hizo el virus menos infeccioso, pero no era difícil averiguar cómo hacerlo más infeccioso. También cambió la carga útil. Mientras que Vienna sobrescribía los cinco primeros bytes de un archivo con instrucciones de reinicio, la versión de Burger escribía cinco espacios en blanco. Pero, como señaló Alan Solomon, «A Brief History of PC Viruses (1986-1993)», http://users.uoa.gr/~nektar/science/technology/a_brief_history_of_viruses.htm. La editorial añadió un prólogo en el libro de Burger explicando la decisión de publicar esta información: «Quizá algunos lectores sientan que los ejemplos de virus del libro deberían omitirse. Debería aclararse que hemos imprimido los ejemplos para ilustrar lo fácil que es escribir un virus. Está claro que cualquiera que esté decidido a provocar la destrucción sabrá cómo crear virus mucho más sofisticados y dañinos».

10. «Según el investigador de antivirus soviético Bezrukov, el primer virus apareció allí casi al mismo tiempo que en Bulgaria y, por cierto, era el mismo virus (Vienna)»: Vesselin Bontchev, «The Bulgarian and Soviet Virus Factories», actas de la 1.ª Conferencia Internacional de Virus Bulletin, 1991, pp. 11-25, <https://bontchev.nlc.v.bas.bg/papers/factory.html>.

CONCLUSIÓN: LA MUERTE DEL SOLUCIONISMO

El crítico Evgeny Morozov¹ ha llamado a la idea de que la tecnología puede resolver, y lo hará, nuestros problemas sociales «solucionismo». La respuesta solucionista a las hambrunas son los sistemas de irrigación. Al calentamiento global, reestructurar el medio ambiente, por ejemplo, sembrando los océanos de algas que absorban el CO₂. ¿Desastres nucleares? Construir drones controlados a distancia para mantener los reactores y eliminar cualquier precipitación radiactiva accidental. ¿Ineficiencias en el mercado laboral? Sitios web que permitan a los trabajadores temporales gestionar sus propios horarios. Un ejemplo clásico de solucionismo es el artículo publicado por *Wired* en 2012: «Africa? There's an App for That».² ¡Buenas noticias! Podemos revertir siglos de imperialismo, revolución y pobreza con nuestros teléfonos móviles. El solucionismo es ubicuo en la ciberseguridad.³

1. Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (Washington, DC: PublicAffairs, 2013). (Traducción al español: *La locura del solucionismo tecnológico*, Katz, 2015).
2. «Africa? There's an App for That», *Wired*, 7 de agosto, 2012, <https://web.archive.org/web/20120807145838/https://www.wired.co.uk/news/archive/2012-08/07/africa-app-store-apple>.
3. El solucionismo también está generalizado en la investigación académica, en gran parte porque la ciberseguridad suele estudiarse y enseñarse en departamentos de informática. Pero no todas las investigaciones en esta área son solucionistas. Consulta, por ejemplo, Josephine Wolff, *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches* (Cambridge, MA: MIT Press, 2018). Recientes trabajos antropológicos sobre *hackers* se centran en el *upcode* social, las normas y reglas de la comunidad *hacker/ciberseguridad*. Consulta, por ejemplo, Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London: Verso, 2014). (Traducción al español: *Las mil caras de Anonymous. Hackers, activistas, espías y bromistas.*, Barcelona: Arpa Editores, 2016). Análisis económico: Consulta, por ejemplo, Ross Anderson, «Why Information Security Is Hard—An Economic Perspective», actas de la 17.^a Conferencia Anual sobre Aplicaciones de Seguridad Informática, 2001, <https://www.acsac.org/2001/papers/110.pdf>. Sociología: Jonathan Lusthaus, *The Industry of Anonymity* (Cambridge, MA: Harvard University Press, 2018), pp. 10-17. Derecho: Consulta, por ejemplo, Daniel J. Solove y Woodrow Hartzog, *Breached!: Why Data Security Law Fails and How to Improve It* (Oxford: Oxford University Press, 2022). Cabría señalar que existe un campo académico entero conocido como «Ciencia, Tecnología y Sociedad» o STS por sus siglas en inglés, que estudia cómo la tecnología se ve afectada por el *upcode* social y cómo lo afecta a él.

Todas las empresas de ciberseguridad prometen que su tecnología mantendrá nuestros datos a salvo. Paséate por cualquier feria y verás kilómetros de vendedores dando bombo a una solución milagrosa diferente. En sus discursos de ventas mencionan cualquier cosa «de nueva generación»: cortafuegos, software antimalware, servicios de detección de intrusos, utilidades de información de seguridad y gestión de eventos, analizadores de tráfico de red, herramientas de etiquetado de documentos, visualizadores de registros y cuadros de instrumentos unificados para la gestión de amenazas. Si pides a los vendedores que digan en qué se distinguen sus productos de sus competidores, dirán lo mismo: «El "ingrediente secreto" es nuestra IA. Es la mejor del mercado».

Los políticos también hablan de la ciberseguridad en términos solucionistas. Asumen que la respuesta adecuada a nuestra inseguridad cibernética es invertir cantidades más grandes de tiempo y dinero en tecnología. Los políticos hablan de un Proyecto Manhattan cibernético o un Moonshot cibernético como si esos esfuerzos tecnológicos masivos fuesen la solución definitiva.

Para ver los límites del solucionismo, vamos a pensar en una breve analogía: las hambrunas. Durante siglos, la gente ha asumido que las hambrunas estaban causadas por la carencia de alimentos. Se creía que esa falta de comida era el resultado de acontecimientos naturales, como la sequía, las inundaciones, los tifones y la peste, o por desastres causados por el hombre, como las guerras, los genocidios y las deficiencias en las labores agrícolas. No obstante, el economista ganador del premio Nobel, Amartya Sen, desafía esta narrativa familiar con datos sólidos. En su libro rompedor *Poverty and Famines*⁴ (1981), Sen argumentaba que la carencia de alimentos no es la principal causa del hambre. Las hambrunas surgen pese a la disponibilidad de comida. En 1943, por ejemplo, Bengala sufrió una crisis devastadora en la que murieron casi 3 millones de personas, incluso aunque había un 13 por ciento para comer más que en 1941, cuando no había hambruna.⁵ Del mismo modo, Etiopía experimentó una hambruna en 1973 incluso aunque las existencias de comida no eran diferentes a cómo habían sido en años anteriores.

Sen aducía que eran los fracasos políticos, y no los agrícolas, los que causaban las hambrunas. En el caso de Bengala, había comida de sobra, pero los trabajadores no podían permitírsela. La Segunda Guerra Mundial elevó los precios de los alimentos un 300 por ciento, pero los salarios de los trabajadores solo subieron un 30 por ciento. El gobierno británico en la India podría haber abordado el problema ajustando los mercados laborales o permitiendo que

4. Amartya Sen, *Poverty and Famines: An Essay on Entitlement and Deprivation* (Oxford: Oxford University Press, 1981).

5. Sen, *Poverty and Famines*, p. 55.

las importaciones compensasen el déficit inflacionario.⁶ Pero no lo hizo. La hambruna de 1973 en Etiopía fue el resultado de las malas condiciones del transporte entre regiones. De nuevo, el país tenía comida de sobra, pero no formas suficientes⁷ de hacer llegar la comida a quienes la necesitaban.

La explicación de Sen para las causas de la hambruna apuntaba a una solución alternativa. Si las hambrunas se deben a fracasos políticos, entonces la solución también debería ser política. Ni siquiera la tecnología agrícola más avanzada puede compensar una política corta de miras.

Lo que es cierto para las hambrunas también lo es para la ciberseguridad. La ciberseguridad no es principalmente un problema tecnológico que requiere sobre todo una solución de ingeniería. Es un problema humano que requiere un entendimiento del comportamiento humano. Necesitamos prestar atención a nuestro *upcode*, determinar dónde se encuentran las vulnerabilidades y arreglar esas reglas de manera que produzcamos un *downcode* mejor.

Soluciones de *upcode*

Una de las principales conclusiones de este libro es que el *upcode* da forma a la producción del *downcode*. Los desarrolladores escriben *downcode* porque responden a un *upcode* existente. Por tanto, el *upcode* se sitúa causalmente más arriba en el proceso que el *downcode*. Si cambiamos el *upcode*, cambiaremos el tipo de *downcode* producido.

Esta relación entre *upcode* y *downcode* abre una nueva posibilidad: en vez de poner parches en el *downcode* inseguro, parcheamos el *upcode* que es responsable del *downcode* inseguro. Resolver problemas en la pila del *upcode* puede corregir desastres técnicos situados más abajo en el proceso.

Veamos un ejemplo simple de una solución de *upcode*. El malware de Mirai creó sus *botnets* al explotar dispositivos con contraseñas predeterminadas entre los dispositivos IoT. En 2018, el gobernador Jerry Brown firmó la propuesta de ley sobre la seguridad de dispositivos conectados,⁸ que requería que los dispositivos conectados a Internet vendidos u ofrecidos para la venta en California tuviesen «características de seguridad razonables». Una característica de seguridad razonable es aquella que, bien es única para cada dispositivo, bien requiere que el usuario elija una nueva contraseña antes del primer uso. California es un mercado enorme, y la ley sobre la seguridad de dispositivos conectados obligaba a los fabricantes de dispositivos IoT que quisiesen vender

6. Sen, *Poverty and Famines*, p. 148.

7. Sen, *Poverty and Famines*, pp. 93-94.

8. Código Civil de California, sección 1798.91.04 (2018).

allí sus productos a sustituir las contraseñas predeterminadas por características de seguridad razonables. Ahora, la vulnerabilidad explotada por Mirai se ha parcheado para todos los dispositivos IoT nuevo. El código que queda más abajo en el proceso se ha arreglado debido a un cambio en el código que queda más arriba.

Pensemos en otro ejemplo. La Comisión de Seguridad e Intercambio de Estados Unidos (SEC, por sus siglas en inglés) ha propuesto recientemente regulaciones diseñadas para incitar a las empresas a tomar mejores decisiones de seguridad.⁹ Requiere que los consejos de administración de las empresas informen de manera periódica de sus políticas para identificar y gestionar riesgos para la ciberseguridad. Las empresas deben revelar cómo están supervisando los directores ese riesgo y cómo la gerencia está evaluándolo e implementando procedimiento de ciberseguridad. Al requerir estos informes del *upcode*, la SEC obligaba a que las consideraciones sobre seguridad se integrasen en la toma de decisiones corporativa al más alto nivel. Los riesgos de ciberseguridad se convirtieron en preocupaciones «cruciales para la misión» que los directores y la gerencia no podían ignorar y debían revelar a los inversores.

A diferencia de la ley orientada a IoT de California, la regulación del SEC es un cambio sistémico en el *upcode*. No está diseñada para parchear una vulnerabilidad en particular. Cambia los incentivos que rigen la toma de decisiones corporativa. Arreglar el *upcode* a este nivel no se limita a arreglar una vulnerabilidad en el *downcode*, sino que tiene como objetivo producir mejores prácticas de seguridad en una amplia variedad de aplicaciones y servicios.

No existe tal cosa como «resolver» el «problema» de la ciberseguridad. Solo hay compensaciones entre diferentes aspectos de nuestra seguridad de la información y entre nuestra información y las seguridades físicas. Tenemos que equilibrar los costes y beneficios antes de decidir si parcheamos el *upcode* y cómo lo hacemos. Para cada movimiento defensivo que se hace, se producirá un cambio en las tácticas ofensivas. Incluso a nivel del *upcode*, el juego del gato y el ratón nunca termina. Nuestro objetivo es cambiar el juego de manera que el gato gane la mayoría de las veces.

Estos juegos toman tres formas relevantes: delincuencia, espionaje y guerra. El gusano Morris, el virusano Melissa, el hackeo a Paris Hilton y la *botnet* Mirai eran delitos. Lo que hizo Cozy Bear fue espionaje. Fancy Bear podría haber participado en un acto de guerra. Cada juego requiere sus propias medidas.

9. «SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies», nota de prensa, SEC, 9 de marzo, 2022, <https://www.sec.gov/news/press-releases/2022-39>.

A. Ciberdelincuencia

A principios de los noventa, los informes de Uniform Crime, las estadísticas oficiales del FBI sobre actividades delictivas en Estados Unidos, mostraron un descenso pronunciado en todas las categorías, tanto en delitos contra la propiedad (robo, allanamiento, fraude) como en los delitos violentos (agresión, violación, asesinato). Parecía como si la delincuencia estuviese bajando en todo el país. Los políticos y los cuerpos de seguridad anunciaban a bombo y platillo el éxito milagroso de sus políticas y liderazgo.

Ese milagro resultó ser, al menos en parte, ilusorio.¹⁰ Cuando los criminólogos analizaron los informes sobre victimización (encuestas a gran escala preguntando a los ciudadanos si han sido víctima de un delito el año anterior), descubrieron que los delitos contra la propiedad no habían disminuido; habían pasado a cometerse *online*. El descenso estadístico era producto de una elaboración de informes incompleta sobre ciberdelincuencia. Ahora, los investigadores creen que al menos la mitad de los delitos contra la propiedad se comenten en Internet. En Reino Unido, más de la mitad de los delitos contra la propiedad se comete *online*.

Por tanto, pedir que se detenga la ciberdelincuencia no es diferente a pedir que se detenga la delincuencia. No se puede hacer. La delincuencia es parte de la vida. Aunque no existe una varita mágica que erradique la delincuencia, en Internet o fuera de ella, es posible reducirlo de manera humana y rentable.

Hasta la fecha, la única solución de *upcode* tratada con seriedad ha sido la de los cuerpos de seguridad. Hay una demanda constante de que se produzcan mayores esfuerzos por parte de los fiscales y se invierta mayor presupuesto por parte de los políticos: más agentes cibernéticos, una formación más intensiva de los fiscales y una mayor inversión en tecnología para hacer un seguimiento de la ciberdelincuencia.

Estos proponentes son conscientes de las dificultades a la hora de perseguir la ciberdelincuencia. Un fraude con tarjeta de crédito podría perpetrarse desde Rusia utilizando un servidor C2 rumano contra un banco francés al reclutar a una cámara de seguridad en Nueva York que sea parte de una *botnet* que distribuya malware escrito en Ucrania a un ordenador en Brasil perteneciente a una empresa china. A diferencia de los métodos de los carteristas, donde delincuente y víctima están en el mismo lugar, los ciberdelincuentes no necesitan estar en

10. M. Tcherni *et al.*, «The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?», *Justice Quarterly* 33, n.º 5 (2016): pp. 890-911; Ross Anderson *et al.*, «Measuring the Changing Cost of Cybercrime», 18.º Taller Anual sobre la Economía de la Seguridad de la Información, 2019.

el mismo país ni en el mismo lado del mundo que la víctima. Para perseguir una actividad tan transnacional, los estados suelen necesitar la cooperación de otros estados. Los servidores rumanos y los registros de los ISP rusos pueden contener pruebas esenciales para procesar a los estafadores.

Sin embargo, según el derecho internacional,¹¹ ningún estado tiene la obligación legal de ayudar a otro a enjuiciar delitos. El *upcode* global, con su sistema de estados soberanos, trata la aplicación de la ley como una cuestión interior. Rumanía no tienen ninguna obligación legal de dar al FBI acceso a servidores en su territorio y Rusia no está obligada a entregar a un sospechoso de un delito de su país.

Hay varios arreglos legales disponibles. Muchos países firman tratados de extradición. De acuerdo con estos tratados, los estados tienen el deber de entregar a sospechosos a los socios de su tratado si estos lo solicitan. Los tratados de extradición son simples dispositivos de interconexión de redes; permiten que sistemas legales diferentes soliciten la cooperación del otro en cuestiones de interés transnacional.

Si eres un ciberdelincuente que vive en un país como la Federación Rusa, que no tiene acuerdos de extradición ni con Estados Unidos ni con ningún otro país, deberías tener cuidado de no viajar a un país que sí los tenga. Saber qué estados tienen estos tratados es *upcode* crucial para los ciberdelinquentes viajeros. Sorprendentemente, no todos lo tienen en cuenta.

Vladislav Klyushin, de 42 años, dirigía M13, una empresa de ciberseguridad que servía a lo más alto de la sociedad y el gobierno de Rusia. El sitio web de M13, por ejemplo, afirma que proporciona seguridad a la presidencia rusa. En 2020, concedió la Medalla de la Libertad a Klyushin. Sin embargo, el FBI sospechaba que Klyushin tenía un negocio paralelo que generaba decenas de millones de dólares con la compraventa de acciones a partir de información hackeada sobre los beneficios de las empresas.¹²

11. Con frecuencia, los estados firman acuerdos de asistencia legal mutua que los obligan a ayudarse entre sí en procesos penales. Consulta la Convención sobre la Ciberdelincuencia del Consejo de Europa (Convención de Budapest), que se diseñó para aumentar la cooperación, pero aún no ha tenido un impacto significativo. Christopher D'Urso, *Nowhere to Hide: Investigating the Use of Unilateral Alternatives to Extradition in U.S. Prosecutions of Transnational Cybercrime* (tesis doctoral, Oxford University, 2021).

12. Henry Meyer, Irina Reznik y Hugo Miller, «U.S. Catches Kremlin Insider Who May Have Secrets of 2016 Hack», Reuters, 3 de enero, 2022, <https://www.bloomberg.com/news/articles/2022-01-03/kremlin-insider-klyushin-is-said-to-have-2016-hack-details>. Consulta también Departamento de Justicia, Oficina del Fiscal de Estados Unidos, Distrito de Massachusetts, «Russian National Extradited for Role in Hacking and Illegal Trading Scheme», 20 de diciembre, 2021.

En la primavera de 2021, agentes federales descubrieron que Klyushin iba a viajar a Suiza. El 21 de marzo, un avión privado procedente de Moscú aterrizó en el aeropuerto de Sion, en el suroeste de Suiza. Poco después de bajar del avión, con un helicóptero esperando para llevarlo a una estación de esquí en Zermatt, Klyushin fue detenido por la policía suiza y trasladado a una prisión cercana. Su esposa, sus cinco hijos y el socio que viajaban con él continuaron hasta Zermatt y se alojaron en un chalet de lujo durante casi diez días antes de regresar a Moscú. Tanto Rusia como Estados Unidos pidieron a los tribunales suizos que extraditasen a Klyushin a sus respectivos países. Mientras tanto, el Departamento de Justicia aseguró las imputaciones de Klyushin e Ivan Yermakov.

Yermakov, como tal vez recuerdes, se ocupaba de las tareas de exploración y algo de *phishing* para Fancy Bear en 2016. Desde entonces, había dejado el GRU y se había unido a M13. Los cargos por compraventa de acciones con información privilegiada eran la segunda imputación de Yermakov, ya que había sido acusado de espionaje en 2018 por los hackeos al Comité Nacional Demócrata. Las acusaciones contra Klyushin y Yermakov alegaban que habían hackeado los servidores de dos agencias utilizadas por empresas estadounidenses que cotizaban en bolsa para presentar sus informes trimestrales y los habían obtenido poco antes de su publicación. Con esta información robada, estos hombres tomaban decisiones sobre inversiones en empresas como IBM, Snap, Tesla y Microsoft, obteniendo unos beneficios de 82,5 millones de dólares.

Estados Unidos tenía un interés añadido en Klyushin. Como proporcionaba servicios de ciberseguridad para la presidencia de Rusia, era probable que tuviese documentación acerca de cómo había hackeado el GRU al Comité Nacional Demócrata en 2016. Evidentemente, Rusia estaba ansiosa por mantener a Klyushin fuera del alcance de los estadounidenses, pero los tribunales suizos se pusieron de parte de Estados Unidos. Ahora, una persona de alto nivel del Kremlin con información privilegiada se encuentra en una prisión federal en Boston a la espera de juicio por los cargos de compraventa de acciones utilizando información privilegiada.

Además de buscar la extradición, los estados han formado alianzas de uso compartido de inteligencia y recursos para causas penales. Piensa en el reciente desmantelamiento de la *botnet* masiva Emotet que comenzó en 2014 como troyano bancario, malware que roba información financiera de aplicaciones de banca.¹³

13. Una vez que infecta un ordenador, por lo general a través de archivos adjuntos en correos, Emotet rebusca entre las bandejas de entrada. Envía mensajes de correo antiguos a los destinatarios con enlaces malicioso o documentos de Word contaminados con copias de Emotet. Si el receptor hace clic o abre el documento y habilita las macros, su ordenador se infecta.

«Shapiro es divertido y está fascinado por este tema, y consigue atraer incluso a los no especialistas con descripciones técnicas de programación... Un solo párrafo pasa con agilidad de Putin a Descartes y a *Matrix*... [Los lectores] verán que sus expectativas se han subvertido (de forma entretenida)».

—JENNIFER SZALAI, *The New York Times Book Review*

Es una paradoja de nuestros tiempos que vivamos en la sociedad de la información, pero no entendamos cómo funciona. ¿Qué pasaría si supiésemos más? En *Fancy Bear se va de phishing*, Scott J. Shapiro recurre a su popular clase en la universidad de Yale sobre hackeo para mostrar que el cibercrimen tiene menos que ver con la programación defectuosa que con el cableado imperfecto de nuestra psique y nuestra cultura. Cuenta la historia de perpetradores ilustres, como Robert Morris Jr., el estudiante de postgrado que se cargó Internet de forma accidental en los ochenta, y el búlgaro «Dark Avenger», quien inventó el primer motor de virus informáticos mutantes. También conocemos al adolescente de dieciséis años del sur de Boston que se hizo con el control del móvil de Paris Hilton, los agentes de inteligencia rusos que trataron de controlar unas elecciones en EE. UU., y otros.

Al relatar sus historias, Shapiro expone los kits de herramientas para *hackers* y revela que los cibercriminales no solo hacen un mal uso del código informático, sino que también explotan los principios filosóficos de la informática: las mismas características que hacen posibles los ordenadores también hacen posible el hackeo. Explica cómo funciona en realidad nuestra sociedad de la información, la manera en que nuestros datos se almacenan y se manipulan y por qué son tan vulnerables a la explotación. Mezcla de jugueteo intelectual y narrativa dramática de crímenes reales, *Fancy Bear se va de phishing* expone los secretos de la era digital. Aquí hay hackeo, espionaje, guerra y cibercrimen como nunca habías leído antes.

«[Shapiro] fusiona con maestría la consideración de dos tipos de código, software y legal... Su narrativa se mueve entre explicaciones técnicas, razonamientos legales y las ideas de pensadores entre los que se incluyen René Descartes y Alan Turing... [Shapiro] logra hacer que [el hackeo] sea inteligible para no especialistas».

—THE ECONOMIST

«Fascinante... *Fancy Bear se va de phishing* ofrece sugerencias equilibradas, argumentando que necesitamos ir más allá de una obsesión por las soluciones técnicas y centrarnos en el *upcode* obsoleto y vulnerable que da forma al *downcode* de mala calidad con el que vivimos ahora».

—RICHARD LEA, *The Wall Street Journal*

ANAYA
MULTIMEDIA

www.anayamultimedia.es

2315287
ISBN: 978-84-415-5279-1

