Tesis de maestría
FLACSO – Facultad Latinoamericana de Ciencias Sociales

El ciberterrorismo: ¿una amenaza real para la paz mundial?

Autor: Sebastián Masana
Tutor: Carlos Escudé
Maestría: Relaciones Internacionales

INDICE

• Grupos extremistas islámicos
    -Hizbollah
    -Hamas

Capítulo V: Introducción a la problemática del ciberterrorismo

• Antecedentes. Juegos de guerra
• Bill Clinton, el primer presidente de la era de Internet
    -La Comisión Presidencial para la Protección de la Infraestructura Crítica
    -Creación del Centro Nacional de Protección de Infraestructura (NIPC)
    -La Dirección Directiva Presidencial 63
    -La falla del milenio
    -El plan *Cyber Corps*

Capítulo VI: Principales hipótesis y predicciones sobre el ciberterrorismo

• Las hipótesis de Barry Collin
• Hacia un análisis cauteloso
    -¿Un Pearl Harbor electrónico?
    -Mitos y realidades sobre los virus informáticos

Capítulo VII: La amenaza del ciberterrorismo: ¿Una excusa para la invasión gubernamental de la privacidad?

• Introducción
• El *chip clipper*
• Phil Zimmerman y el PGP
• La privacidad en la era de Internet
    -El proyecto FIDNET
    -El Carnivore
    -Echelon
    -La privacidad después de los atentados del 11 de septiembre

Capítulo VIII: La prevención del ciberterrorismo, un negocio millonario

• Un contrato de 5000 millones de dólares

Conclusiones

Introducción e hipótesis

La proliferación de computadoras conectadas a módems telefónicos que se inició a principios de los años 80 aumentó la vulnerabilidad de los sistemas informáticos y permitió el nacimiento de los hackers, individuos capaces de ingresar ilegalmente en las redes computacionales e incluso de alterar su contenido.

Esa vulnerabilidad hizo que los organismos de inteligencia de Estados Unidos comenzaran especular con la posibilidad de que algún grupo terrorista pueda cometer atentados o actos de sabotaje de gran envergadura empleando medios telemáticos, sin necesidad siquiera de que el agresor se encuentre dentro del territorio estadounidense. Para designar a esa eventual categoría de actos terroristas, se acuñó el término ciberterrorismo (*cyberterrorism*).

El temor ante hipotéticos ataques ciberterroristas se acentuó durante los años ´90 debido a varios factores, como ser:

a) El surgimiento de Internet y su masiva penetración en la sociedad. Eso multiplicó la cantidad de módems existentes; aumentó la vulnerabilidad de muchas redes privadas (ya que las mismas pasaron a estar conectadas a Internet, que es una red de acceso público) y fomentó la proliferación de hackers, debido a que penetrar una red ilegalmente o fabricar virus capaces de infectar miles de computadoras, pasó a ser cada vez más sencillo, como se describe en el capítulo II de esta tesis.

b) La sensación de vulnerabilidad generada por la proximidad del *millenium bug* (*la falla del milenio*), también conocido como Y2K. La incapacidad de muchas computadoras para registrar fechas posteriores a 1999 hizo temer un “apocalipsis informático” en la transición al 2000, que finalmente no se produjo gracias a la masiva inversión en prevención y adecuación de los sistemas computacionales a nivel oficial y privado.

Al analizar los artículos de la prensa estadounidense publicados en los años inmediatamente anteriores al 2000, se evidencia el temor existente entre los organismos de inteligencia de que entre los técnicos contratados para las tareas de reconversión informática, se infiltraran terroristas con el objeto de colocar virus, robar contraseñas o alterar los sistemas computacionales de tal forma de dejarles una “puerta trasera” que posteriormente les permitiera ingresar en forma ilegal para cometer un atentado.

c) La proliferación masiva de noticias sobre el accionar de los hackers, cuyas capacidades aparecen en muchos casos exageradas. Estos factores hicieron que durante la administración de Bill Clinton se adoptaran una serie de medidas preventivas en relación al ciberterrorismo.

Mientras los políticos y congresistas repetían constantemente expresiones como “Pearl Harbor electrónico”, los medios de comunicación difundían hipótesis catastróficas, tales como ciudades enteras sin luz eléctrica, o aeropuertos cuyas torres de control eran hackeadas por ciberterroristas con el objeto de ocasionar la colisión premeditada de aviones.

En la presente tesis se desarrollarán los temas recién mencionados, y se aportarán datos a favor de las siguientes hipótesis:

a) Los escenarios hipotéticos de atentados ciberterroristas que ocasionan víctimas fatales resultan fantasiosos y exagerados por la simple razón de que en las distintas áreas de la infraestructura civil estadounidense (agua, energía, transporte y comunicaciones) la in-

tervención humana en forma directa cumple todavía un rol fundamental. No es posible provocar apagones, incendios, explosiones, escapes radioactivos o choques de aviones empleando simplemente una computadora y un módem.

b) Gran parte de los especialistas que fomentan el miedo el ciberterrorismo a través de los medios de comunicación trabajan en compañías tecnológicas —muchas de ellas contratistas del gobierno estadounidense— que en los últimos años se vieron enormemente beneficiadas con el incremento del gasto estatal en seguridad informática destinado a prevenir ataques cibernéticos**.**

c) Las predicciones apocalípticas en relación al ciberterrorismo realizadas por las agencias de seguridad estadounidenses se inscriben dentro de una campaña que tiene como objetivo limitar la privacidad de los ciudadanos estadounidenses y ampliar los poderes de dichos organismos para espiar e intervenir las comunicaciones de personas consideradas sospechosas.

Capítulo I: Definiciones operativas

Antes de analizar el concepto de ciberterrorismo, es necesario explicitar las definiciones de terrorismo, cibernética y ciberespacio.

Terrorismo

Paul Wilkinson describe al terrorismo como "el uso de la intimidación coercitiva por los movimientos revolucionarios, regímenes o individuos, por motivos políticos".[1] Esta definición, si bien contiene algunas de las características que distinguen a la acción terrorista, resulta insuficiente para dar cuenta de dicho fenómeno. Walter Laqueur propone un concepto más amplio, y entiende al terrorismo como "el empleo o amenaza de violencia, un método de combate o una estrategia para lograr ciertos objetivos, con el propósito de inducir un estado de temor en la víctima que no se ajusta a las normas humanitarias y en cuya estrategia es fundamental la publicidad".[2]

Según la definición oficial del FBI, "el terrorismo es el uso ilegal de la fuerza o la violencia contra personas o propiedades a fin de intimidar o cohersionar al gobierno, la población civil o cualquier otro segmento, persiguiendo objetivos sociales o políticos".

A su vez, el Departamento de Estado norteamericano presenta la siguiente definición: "El término terrorismo implica actos de violencia premeditada y políticamente motivada perpetrados contra objetivos no combatientes por grupos subnacionales o agentes clandestinos".[3]

Lo cierto es que no existe todavía una definición de terrorismo aceptada universalmente. Una de las principales dificultades con que se tropieza para alcanzar un consenso ha

---

[1] Wilkinson, Paul: *Political Terrorism*. Macmillan, Londres, 1974, pp. 11-12. Citado en Gillespie, Richard: *Soldados de Perón*, Ediciones Grijalbo, Argentina, 1987, p. 109.

[2] Citado por Bartolomé, Mariano César, en *El terrorismo como amenaza transnacional*. Conferencia dictada en el Primer Seminario sobre Seguridad Pública, auspiciado por el Gobierno de la Provincia de Tucumán, noviembre de 1997. Ver texto completo en http://www.ba.ucsa.edu.ar/isco/doc/Tr4.htm

[3] Las definiciones del FBI y el Departamento de Estado pueden consultarse en el sitio www.terrorism.com.

sido la continua controversia acerca de las guerras de liberación nacional y los motivos aducidos para justificar la violencia.

La dificultad de establecer los límites entre lo que es legítimo y lo que no lo es, entre una forma correcta de lucha y una forma incorrecta ha incorporado difíciles consideraciones políticas a la labor de definición. Como se suele decir, "el que para uno es un terrorista para otro es un luchador de la libertad".

Diferencia entre terrorismo y guerrilla

No es la intención del presente trabajo ahondar en el debate acerca de la noción de terrorismo. Sin embargo, cabe señalar la diferencia entre terrorismo y guerrilla.
Para Richard Gillespie,[4] los terroristas, contrarios al Estado se proponen intimidar al pueblo y demostrar que el Estado es incapaz de garantizar la seguridad y el orden público. Cuanto más indiscriminada e imprevisible es su violencia, mayores son las posibilidades de que logren sus objetivos.

Pero quienes practican la guerrilla —"una forma no convencional de combatir en las zonas urbanas y suburbanas con fines políticos"[5]— buscan la conquista del poder del Estado mediante una estrategia político–militar que requiere considerable apoyo y colaboración pública. Por ello su violencia tiende a ser discriminada y previsible, aún cuando a menudo provoca una reacción menos discriminada.

Mientras que los terroristas pueden considerar a los inocentes civiles como objetivos legítimos, los guerrilleros urbanos limitan generalmente sus ataques a los agentes del Estado (especialmente personal militar y policíaco) y a enemigos políticos claramente definidos (con frecuencia relacionados de algún modo con el Estado).

De cualquier manera, la guerra de guerrillas urbana y el terrorismo político no son siempre fenómenos mutuamente exclusivos. El terrorismo puede ser empleado por los guerrilleros urbanos como un "arma auxiliar".[6]

Cibernética

La enciclopedia Encarta de Microsoft —fuente poco confiable para otras cuestiones pero que en este caso nos resulta útil— define a la cibernética como la "ciencia interdisciplinaria que trata de los sistemas de comunicación y control en los organismos vivos, las máquinas y las organizaciones".[7]

Cibernética proviene del griego *kyberneees* ('timonel' o 'gobernador'). El concepto fue aplicado por primera vez en 1948 por el matemático Norbert Wiener a la teoría de los mecanismos de control. Esta ciencia surgió de los problemas planteados durante la Segunda Guerra Mundial a la hora de desarrollar los denominados cerebros electrónicos y los mecanismos de control automático para los equipos militares, como los visores de bombardeo. La cibernética contempla de igual forma los sistemas de comunicación y control de los or-

[4] Gillespie, Richard: *Soldados de Perón*, Ediciones Grijalbo, Argentina, 1987, p. 109.

[5] Wilkinson, Paul. *Terrorism and the Liberal State*. Macmillan, Londres, 1977, p. 60. Citado en Gillespie, Op. Cit. Pg 109.

[6] Ibid, p 38.

[7] "Cibernética", Enciclopedia Microsoft Encarta 97 © 1993-1996 Microsoft Corporation.

ganismos vivos que los de las máquinas. Para obtener la respuesta deseada en un organismo humano o en un dispositivo mecánico, habrá que proporcionarle la información necesaria. En el cuerpo humano, el cerebro y el sistema nervioso coordinan dicha información, que sirve para determinar una futura línea de conducta; los mecanismos de control y de autocorrección en las máquinas sirven para lo mismo.

La cibernética también se aplica al estudio de la psicología, la inteligencia artificial, los servomecanismos, la economía, la neurofisiología, la ingeniería de sistemas y los sistemas sociales. La palabra cibernética ha dejado de identificar un área independiente de estudio y la mayor parte de la actividad investigadora se centra ahora en el estudio y diseño de redes neuronales artificiales.

Si bien esas aclaraciones son necesarias, es importante considerar, más allá de la definición académica del término cibernética, el sentido que se le da popularmente a esa palabra. La ciencia ficción (expresada a través del cine, la televisión, la literatura y los *comics*) fue la encargada de difundir a nivel masivo este concepto. La cibernética hace alusión, en la mayoría de las obras de ciencia–ficción, a la unión de un organismo viviente con componentes electrónicos o electromecánicos.

En los años 70, la serie televisiva *El hombre nuclear* (*The Six Million Dollar Man*) dio el perfecto ejemplo de lo que se entiende a nivel masivo por cibernética.[8] Tras haber sufrido un accidente en el cual perdió ambas piernas, un ojo y un brazo, el astronauta Steve Austin (protagonizado por Lee Majors) recibió implantes electrónicos que resultaban inadvertidos visualmente, pero que le permitían correr a más de 100 kilómetros por hora, ver con la precisión de una mira telescópica y levantar objetos de varias toneladas.

La serie estaba basada en el libro *Cyborg*, de Martin Caidin. El término *cyborg (Cybernetic Organism*, organismo cibernético) se usa para designar a un ser viviente (generalmente un hombre) que tiene una parte humana y otra electrónica. En los años 80 ese concepto de *cyborg* fue reforzado por el filme Terminator, de James Cameron (1984), que dio origen a una secuela y sirvió de inspiración a decenas de otros filmes.

Ciberespacio

En 1984, el escritor de ciencia ficción William Gibson acuñó el término ciberespacio (*cyberspace*) en su novela *Neuromante*. En *Neuromante*, ciberespacio se refiere a una vasta matriz de datos controlada por poderosas compañías. La matriz de Gibson tiene una interfaz visual y tridimensional, que permite a los usuarios navegar luego de "enchufarse" (*jacking in*) o conectarse a través de equipos especiales.

En cuanto al origen del término, Gibson previamente había pensado en las expresiones *dataspace* e *infospace*, hasta que se decidió por *cyberspace*. "Desde el momento en que gran parte de nuestra actividad se desarrolla digitalmente (desde las transacciones bancarias hasta la compra y venta de acciones en las bolsas) es útil tener una expresión que permita a todo eso formar parte de un territorio", expresó el mismo Gibson.[9] En ese senti-

[8] Cada capítulo de la serie comenzaba con una voz en off que decía: "Steve Austin. Astrounauta. Su vida está en peligro. Usaremos la más avanzada tecnología para convertirlo en un organismo cibernético, poderoso, superdotado...". *The Six Million Dollar Man* constó de 103 episodios emitidos entre 1973 y 1978.

[9] Entrevista televisiva realizada en Suecia para el programa televisivo Rapport, noviembre 3, 1994. El audio de la entrevista completa (en inglés) se puede escuchar en: http://www.josefsson.net/gibson/

do, el ciberespacio es un espacio virtual de *bits* y *bytes*, en oposición al espacio físico de átomos y moléculas.

Bruce Sterling, el segundo escritor más importante del género *ciberpunk* después de Gibson, señala que si bien el término ciberespacio fue acuñado en 1984, "el territorio en cuestión, la frontera electrónica, tiene unos ciento treinta años. El ciberespacio es el *lugar* en el que una conversación telefónica parece tener lugar. No en el interior de tu teléfono. No en el interior del teléfono de la otra persona, en otra ciudad. Es *el lugar entre* los teléfonos".[10]

El advenimiento de Internet llevó a los cultores de la ciencia–ficción a asociar a la "red de redes" con la matriz de Gibson y por ende, con el ciberespacio.

El autor de esta tesis considera que identificar al ciberespacio con Internet es erróneo. La forma en que se accede a Internet carece del componente cibernético necesario para justificar el prefijo *ciber*. En el mundo virtual de Case —protagonista de Neuromancer— la mente consciente y el cuerpo están separados. "(...) la mente alcanza una libertad sin precedentes. (...) La realidad de Case es representada en una red de datos tridimensionales. Esa representación evita cualquier sentido de desorientación (...) porque el *imput* sensorial visual, auditivo y kinestésico es análogo al del mundo real (...) Case se siente tan cómodo en el mundo virtual como cuando camina en el mundo real, o tal vez más..."[11]

En el juego de rol *Cyberpunk* —en cuya creación intervino Gibson— para acceder a la Matriz los personajes imaginarios cuentan con un *ciberimplante* en el cráneo, en el cual se coloca un enchufe. Es decir, la conexión se produce directamente a través del sistema nervioso. Eso hace que si en la Matriz alguien es atacado y muere, la persona muere también en la realidad (se le "fríe" el cerebro). Lo mismo ocurre con el juego de rol *Shadowrun*, imitación de *Cyberpunk*, que posteriormente dio origen a una larga serie de novelas.[12]

Ese mismo mecanismo es representado en el filme *Matrix*,[13] en el cual para ingresar al mundo virtual es necesario contar con un implante craneal, y si el protagonista muere dentro del mundo imaginario, muere también en la realidad. Pero al mismo tiempo, esa conexión directa a través del sistema nervioso hace que cuando los protagonistas ingresen al mundo virtual, tengan capacidades extraordinarias, de las cuales carecen en el mundo real.

Nada de eso ocurre con Internet, cuya interfaz es puramente visual (aunque ocasionalmente posee algunos componentes auditivos) y bidimensional. Si bien se está estudiando la posibilidad de conectarse a Internet mediante algún dispositivo de realidad virtual, todos esos desarrollos están aún en pañales.

La equivocación que —en la opinión del autor de esta tesis— se comete al identificar a Internet con el ciberespacio, se traslada al concepto de ciberterrorismo. Si bien la definición de ciberterrorismo recién se aborda en el próximo apartado, se puede anticipar que

---

[10] Sterling, Bruce: *The Hacker Crackdown (La caza de hackers): Ley y desorden en la fronteraelectrónica*. Edición en español traducida por el equipo de Kriptópolis (www.kriptopolis.com) y publicada en 1999. En ese sitio se puede bajar el libro entero, lo cual no es ilegal, sino que forma parte de un acuerdo de freeware literario. El título original de la obra es *The Hacker Crackdown : Law and Disorder on the Electronic Frontier* y fue publicada por Bantam Books en 1993.

[11] Hendrix, Josh. *The Ciberpunk Project* (www.cyberpunkproject.org/idb/matrix_in_neuromancer.html)

[12] La primera novela de *Shadowrun* fue escrita por Robert N. Charrette con el título *Never Deal With a Dragon* y fue publicada en 1990 por ROC, una división de Penguin Books USA. Para mayor información, ver: www.fasa.com

[13] Matrix se estrenó en 1999. Fue dirigida por Andy y Larry Wachowski.

dicho concepto resulta en sí mismo excesivamente ostentoso, ya que, nuevamente, no hay componente cibernético alguno que justifique la utilización de prefijo *ciber*.

La expresión *ciberterrorismo* genera en el imaginario colectivo una imagen de amenaza más compleja que si se utilizara, por ejemplo, la expresión "terrorismo por medios informáticos", "teleterrorismo" o "terrorismo digital". Esa magnificación, sumada a la exageración actual del poder de los *hackers* que hacen numerosos filmes —al igual que la mayoría de los medios de comunicación— es explotada por quienes buscan infundir en la sociedad el temor al ciberterrorismo, como se verá más adelante.

Ciberterrorismo

En los años 80, Barry Collin, un investigador *senior* del *Institute for Security and Intelligence* en California acuñó el término *cyberterrorism* para referirse a "la convergencia del ciberespacio con el terrorismo".[14]

Mark Pollit, un agente del FBI que se dedicó a estudiar el tema, desarrolló la siguiente definición operativa: "El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos

subnacionales o agentes clandestinos". Como se observa, Pollit tomó una parte de la definición de terrorismo del FBI anteriormente citada.

Para contribuir a clarificar qué fenómenos pueden ser calificados como actos de ciberterrorismo, Dorothy E. Denning directora del *Georgetown Institute for Information Assurance* de la *Georgetown University*, explica lo siguiente:

> "Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo. Ataques que deriven en muertes o personas heridas, explosiones, colisiones de aviones, contaminación de agua o severas pérdidas económicas pueden ser ejemplos válidos. Serios ataques contra la infraestructura crítica de un país podrían ser actos de ciberterrorismo, dependiendo de su impacto. Los ataques que interrumpen servicios no esenciales o que son básicamente una molestia costosa no entran en esta categoría".[15]

Esa definición de Denning es la que se decidió adoptar con fines operativos para esta tesis. Por lo tanto, en el presente trabajo **quedan excluidas** del concepto de ciberterrorismo las siguientes prácticas:

- El hackeo de sitios *web* y la modificación de sus contenidos.
- Los "ataques de negación de servicio", destinados a paralizar durante unas horas las operaciones de un sitio, aunque sin causarle daño alguno.
- La intromisión no autorizada en redes privadas o gubernamentales, aún cuando esas intromisiones se produzcan en organismos vinculados a la seguridad, como el Pentágono, el FBI o la Fuerza Aérea.

---

[14] En el siguiente sitio se pueden leer algunas declaraciones de Barry Collin: http://www.af.mil/news/-Feb1998/ n19980206_980156.html

[15] Extracto del testimonio prestado por Dorothy E. Denning ante el *Special Oversight Panel on Terrorism,Committee on Armed Services*, de la cámara baja estadounidense, 23 de mayo de 2000. Ver texto completo en http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

• La intromisones en redes con propósitos delictivos: espionaje industrial, robo de bases de datos, robo de números de tarjetas de crédito, etcétera. Estas prácticas se podrían incluir en la categoría de ciberdelito (*cybercrime)*.[16]

• La diseminación de virus informáticos.

• La saturación deliberada de casillas de e-mail (*e-mail bombs*).

• La utilización de Internet por grupos terroristas con fines informativos o doctrinarios.

Capítulo II: Los hackers

Definiciones

Antes de seguir avanzando sobre el tema del ciberterrorismo, es necesario hacer algunas precisiones acerca de los denominados *hackers*. El significado de la palabra *hacker* varía según quien lo define. Los medios masivos, las agencias de seguridad y los mismos *hackers* tienen sus propias definiciones.

Para los efectos de esta tesis, resulta útil la definición de *hacker* proporcionada por el diccionario Merina–Webster: "Persona que accede ilegalmente a información almacenada en un sistema computacional".[17]

Para mayor precisión, el autor de esta tesis cree conveniente reemplazar la palabra "ilegalmente" por "sin autorización", dado que el marco legal varía según el país y en algunos casos, como la Argentina, el vacío legal en la materia es tal que si utilizáramos la palabra "ilegal" serían muy escasas las personas a las que se podría caracterizar como *hackers*.

Eric Raymond, compilador de *The New Hacker´s Dictionary*, enriquece la definición de *hacker* con algunos datos adicionales: Es alguien que irrumpe en el sistema computacional de otra persona, a menudo en una red; descifra contraseñas personales y usa sin licencia programas de computadoras, o quebranta intencionalmente de alguna u otra manera la seguridad de una computadora (...) puede hacerlo por lucro, maliciosamente, por alguna causa o propósito altruista, o simplemente porque allí encuentra un desafío.[18]

"El término *hacking* es usado rutinariamente hoy en día por casi todas los policías con algún interés profesional en el abuso y el fraude informático", explica Bruce Sterling. Y añade: La policía estadounidense describe casi cualquier crimen cometido con, por, a través, o contra una computadora, como *hacking* (...) *hacker* es la expresión que los asaltantes informáticos eligen para describirse a ellos mismos. Nadie que asalte un sistema de buena gana se describe a él mismo —raramente a ella misma— como un asaltante informático, intruso informático, *cracker* o, *wormer* (...).

(...) Los *hackers* se diferencian en su grado de odio a la autoridad y la violencia de su retórica. Pero en el fondo "son unos burladores de la ley. No respetan las actuales leyes

---

[16] La diferencia entre *cybercrime* y *cyberterrorism* es la misma que entre delito y terrorismo. El acto terrorista es delictivo, cuanto infringe la ley, pero los actos delictivos no son necesariamente terroristas.

[17] El diccionario Merina–Webster se puede consultar en el sitio www.m-w.com

[18] Raymond, Eric. *The New Hacker´s Dictionary*. Ver: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212220,00.html En realidad, Raymond hace una distinción entre *hackers* (programadores inteligentes) y *crackers*. La definición descripta corresponde al concepto de *cracker*, pero en este caso la utilizamos para definir a los *hackers*, ya que responde con precisión a la imagen que los medios masivos y las personas en general tienen de los *hackers*.

del comportamiento electrónico como esfuerzos respetables para preservar la ley y el orden y proteger la salud pública. Consideran esas leyes como las tentativas inmorales de desalmadas sociedades anónimas, para proteger sus márgenes de beneficio y aplastar disidentes (...). Los *hackers*, en su grandilocuencia, se perciben a sí mismos como una *elite* de exploradores de un nuevo mundo electrónico.

Los intentos para hacer que obedezcan las leyes democráticamente establecidas de la sociedad americana contemporánea, son vistas como persecución y represión.

Después de todo, argumentan, si Alexander Graham Bell hubiera seguido con las reglas de la compañía de telégrafos Western Union, no habría habido teléfonos. Si Benjamín Franklin y Thomas Jefferson hubieran intentado trabajar *dentro del sistema* no hubiera habido Estados Unidos (...).[19]

Origen de los hackers

Los hackers existen desde los años 60, es decir, desde antes de que existieran las computadoras personales. Por aquellas épocas eran personas que se encargaban de utilizar líneas telefónicas en forma ilegal.

Actualmente, quienes violan redes telefónicas son apodados *phreakers*. Uno de los primeros *hackers* de renombre fue John Draper, alias "Cap'n Crunch". En 1970, Draper descubrió que el silbato de juguete que se incluía en las cajas de la marca de cereales Cap'n Crunch coincidía exactamente con la frecuencia de la red telefónica de AT&T. Gracias a Draper, miles de personas comenzaron a hacer llamadas de larga distancia sin costo alguno.

Al poco tiempo la pasión por hackear líneas telefónicas se trasladó a los sistemas computacionales. Las grandes computadoras o *mainframes* han estado conectados entre sí desde los años 60, pero las computadoras personales, manejadas por individuos desde sus casas, empezaron a conectarse a finales de los años 70. De allí en más se comenzaron a popularizar los *Bulletin Board Systems* (BBS).

Un BBS puede definirse como una computadora que sirve como centro de información y mensajes para usuarios que se conectan desde las líneas telefónicas mediante módems. Un módem (abreviatura de moduladordemodulador*)*, es un aparato que traduce los impulsos digitales de las computadoras en señales analógicas audibles de un teléfono, y viceversa. Los módems conectan a las computadoras con los teléfonos y así pueden conectarse los unos con los otros.

La BBS creada por Ward Christenson y Randy Suess en febrero de 1978 en Chicago, Illinois, se considera generalmente como la primera BBS para computadoras personales que realmente merece el nombre. A través de esos boletines electrónicos, antecesores de Internet, se comenzó a intercambiar información acerca de distintos métodos de irrupción en computadoras ajenas.

Las tres generaciones

Distintos autores coinciden en señalar, a grandes rasgos, tres generaciones de *hackers:*

[19] Sterling, Bruce: The Hacker Crackdown. Law and Disorder on the Electronic Frontier. Bantam Books, 1993.

La primera estuvo integrada por los descendientes directos de los *phreakers*, pioneros en la materia, y se vinculó estrechamente con el crecimiento de los BBS.

La segunda generación de *hackers* se inició alrededor de 1990. Por aquella época las computadoras personales se hicieron realmente populares en los hogares, y dejaron de ser utilizadas sólo por ingenieros o técnicos. De 4.000 BBS existentes en todo Estados Unidos en 1985, se pasó a más de 30.000 en 1990. A esta segunda generación pertenece el argentino Julio Ardita, el primer *hacker* latinoamericano procesado en Estados Unidos. En 1995, con 20 años de edad, Ardita se "colgó" desde su casa de las redes de Telecom en Argentina y de allí logró acceder ilegalmente a la Marina de Estados Unidos y al mismísimo Pentágono. Tras ser rastreado por el FBI, fue detenido en Argentina y accedió a viajar voluntariamente a Estados Unidos para ser enjuiciado.

Según se puede leer en un documento del Departamento de Justicia norteamericano, Ardita tuvo acceso a documentación "sensible pero no calificada", sobre el diseño de radares y aviones militares.[20] Para quedar libre pagó una multa de 5.000 dólares y firmó un acuerdo de confidencialidad, comprometiéndose a no revelar nada de la información a la que accedió.

La tercera generación está integrada por los hackers de la "era de Internet", iniciada a partir de la popularización de la "red de redes", que tuvo como año clave a 1995. A continuación, se describen algunas características de esta tercera generación.

La democratización del *hacking*

La era de Internet generó la así llamada "democratización del *hacking*". Actualmente existen varios miles de sitios *web* que difunden gratuitamente herramientas destinadas a ataques informáticos, y que en muchos casos son tan fáciles de usar que cualquier usuario con mínimos conocimientos de computación puede manejarlas en muy poco tiempo.

Christopher Sullivan, miembro de un grupo de hackers denominado 2600.com (el nombre alude a los silbidos de 2.600 ciclos que eran necesarios para "engañar" a la compañía Bell Telephone), afirma que la mayoría de los *hackers* operan de la siguiente manera. Lo primero que hacen es visitar o buscar algunos de los sitios mencionados para *hackers*, como por ejemplo Netcraft.com, en los cuales hay *scripts* (rutinas, o pequeños programas) que escanean el sitio al cual se quiere violentar, con el fin de determinar cuál es su arquitectura tecnológica básica.

Esos *scripts* indagan en el servidor del sitio para determinar qué sistema operativo usa y que tipo de servidor de *software* emplean.[21] "Esa es la parte sencilla", explica Sullivan,[22] y señala que actualmente no hay forma de evitar que ese tipo de *softwares* revelen la información mencionada. Es decir, esos datos no se pueden mantener en secreto.

---

[20] Masana, Sebastián. *Confesiones de un ex hacker*. Artículo publicado en el sitio www.es.internet.com

[21] Los más comunes son el Internet Information Server de Microsoft, para Windows NT, y Apache, un *web server* para sistemas operativos basados en Unix. Otros servidores web son el Novell Web Server para usuarios de su sistema operativo NetWare, y la familia IBM de Lotus Domino, para OS/390 y AS/400. También se puede mencionar a los servidores Netscape FastTrack y Enterprise.

[22] Todas las citas de Ed Sullivan fueron extractadas del artículo *The Mind of a Hacker*, escrito por Andee Joyce para el sitio RetailTech.com.

Luego viene la parte más difícil: encontrar "agujeros" o fallas en la versión específica del *software* que corre ese sitio, que puedan proporcionar una "entrada" para romper su código.

La información sobre las fallas del software inmediatamente pasa a ser de público conocimiento dentro de la comunidad *hacker*. Hay sitios como Rootshell.com que publican esa información. También hay grupos de noticias o canales de *chat* especializados donde se comparten esos conocimientos. Eso al menos tiene un lado positivo: los fabricantes de software toman conocimiento rápidamente de las fallas de sus productos y se mueven rápidamente para solucionarlas.

Una vez que un hacker encuentra un "agujero", penetrar el sistema es solo una cuestión de persistencia. Hay varios *scripts* diseñados para romper códigos, y que sólo requieren conocimientos básicos de computación. La enorme mayoría de los intentos terminarán en fracaso, pero la promesa de un éxito potencial es incentivo suficiente para que miles de personas se larguen a intentarlo.

Clasificación de los hackers

Erik Ginorio, analista de seguridad de *Cisco System's Corporate Information Security Group*, hace una clasificación de *hackers* que es muy utilizada hoy en día por el periodismo especializado y por las empresas.[23] En su opinión, hay tres clases de hackers.

1) ***White Hat hackers*** (*hackers* de sombrero blanco). Son personas que no persiguen intereses delictivos, sino que por el contrario, creen que su misión (a veces remunerada y a veces no) es encontrar brechas en la seguridad de las computadoras y luego avisar a las partes involucradas para que puedan protegerse. En otras palabras, son *hackers* "buenos", que colaboran con las empresas.

2) ***Black Hat hackers*** (*hackers* de sombrero negro). Son los que reciben la mayor atención por parte de los medios. Se trata de individuos proclives a realizar una serie de tareas que van desde ingresar ilegalmente a distintos sitios y colocar información falsa o textos e imágenes obscenos, hasta robar números de tarjetas de crédito con la intención de cometer fraudes.

Ginorio cree que la gente más joven dentro de este grupo está básicamente interesada en el *defacement*, expresión que no tiene equivalente en español y que se refiere al acto de ingresar a un sitio *web* y modificar su contenido. "Después de todo, nada le da más prestigio a un *hacker* de 13 años que llenar a un sitio muy conocido con graffittis electrónicos", opina Ginorio. Ese tipo de personas son, en su opinión, el mayor subgrupo dentro de los *Black Hat* y el mayor grupo de *hackers* en general: "Cerca del 90% de las acciones de *hacking* son hechas para llamar la atención o difamar a alguien. En su mayor parte, esos actos no causan prácticamente ningún daño y son reversibles".

3) ***Grey Hat hackers*** (*hackers de sombrero gris*). Son aquellos que en el pasado realizaron actividades de *hacking*, pero que actualmente trabajan para empresas en el área de seguridad. Este tipo de *hackers* suelen ser contratados por las empresas, "siempre y cuando no hayan hecho anteriormente nada destructivo o claramente delictivo", dice Ginorio.

[23] Todas las declaraciones de Erik Ginorio fueron extractadas del artículo *The Mind of a Hacker*, escrito por Andee Joyce para el sitio RetailTech.com.

Por supuesto que la línea divisoria entre esos tres tipos de *hackers* es bastante delgada y existen quienes la suelen cruzar para un lado o para el otro, pese a lo cual esa clasificación resulta bastante útil, especialmente para las agencias gubernamentales que investigan el accionar de los hackers y para las empresas que contratan gente para sus departamentos de seguridad informática.

El lado oscuro del hacking

Una lujosa oficina de Park Avenue, en pleno corazón de Nueva York, recibió un fax que llevaría a los destinatarios a arrepentirse por no haber estrechado sus medidas de seguridad informática. En el fax figuraban, entre otras cosas, la contraseña informática del presidente de la compañía y sus números de tarjetas de crédito personales.

Igor Yarimaka y Oleg Zezov, dos kazajstaníes que decidieron hacer un uso lucrativo de sus habilidades con las computadoras, habían penetrado el sitio de la empresa, apropiándose de información confidencial. Y pedían 200.000 dólares por no informar a los clientes de esa prestigiosa casa de servicios financieros sobre el incidente.

El presidente de la empresa accedió a reunirse con los dos hombres en el vestíbulo de un hotel en Londres. Sin embargo, no estaba sólo: lo acompañaban varios agentes del FBI, quienes arrestaron a los jóvenes. El ejecutivo en cuestión era nada menos que Michael Bloomberg, presidente de la empresa que lleva su nombre. El operativo duró casi cuatro meses.

Los *hackers* cometieron el error de creer que en Bloomberg actuaría como muchas otras empresas cuya reputación depende en gran parte de la protección de sus datos y, en consecuencia, preferiría pagar para que no se difunda la noticia.[24]

Si bien, como ya se explicó, no es adecuado creer que todos los hackers son delincuentes, la relativa facilidad con la que se puede "quebrar" la seguridad informática de algunas empresas es un factor aprovechado por quienes buscan cometer distintos tipos de delitos.

Ya en 1998, casi todas las 500 empresas que figuran en la famosa lista de la revista Fortune habían sido penetradas en alguna ocasión por delincuentes informáticos. El FBI estima que ese tipo de delitos moviliza 10.000 millones de dólares anuales, y que sólo el 17% de las compañías agredidas, estafadas o chantajeadas electrónicamente efectúan las respectivas denuncias. La mayoría prefiere guardar el secreto para mantener la confianza de sus consumidores y accionistas.[25]

Capítulo III: El *hacktivismo*

Se denomina *hacktivismo (hacktivism*, en inglés*)* a la convergencia del *hacking* con el activismo social o político. El *hacktivismo* incluye la desobediencia civil electrónica, que traslada al ciberespacio el concepto tradicional de desobediencia civil.

[24] Anécdota de Bloomberg: Revista Punto-Com. Miami, octubre de 2000.

[25] Estadísticas extractadas del prólogo del libro *Cybercrime, Cyberterrorism, Cyberwarfare*, editado por el *Center for Strategic & International Studies* (1998). Para más información, ir al sitio www.csis.org

Los orígenes del *hacktivismo* se remontan a mediados de los años ochenta, la prehistoria de la *Web*. La primera versión de *PeaceNet* (red electrónica mundial dedicada a la paz, la justicia social y económica, los derechos humanos y la lucha contra el racismo, aparecida en 1986), permitió por primera vez a los activistas políticos comunicarse unos con otros a través de las fronteras internacionales con relativa rapidez y facilidad.[26]

Ese entorno, que operaba básicamente a través del sistema de BBS y donde predominaba el texto, se mantuvo hasta 1994, año en que se introdujeron los primeros navegadores con interfaz gráfica de usuarios. Por aquel entonces, el surgimiento del Netscape permitió, por primera vez, visualizar fácilmente en Internet páginas con fotografías e imágenes.

La expresión “desobediencia civil electrónica" fue acuñada por un grupo de artistas y pensadores llamado *Critical Art Ensemble*. En 1994, publicaron su primer libro sobre el tema, *The Electronic Disturbance* (El disturbio electrónico). A esta obra siguió dos años después *Electronic Civil Disobedience and Other Unpopular Ideas* (La desobediencia civil electrónica y otras ideas poco populares). Ambas obras están dedicadas a un estudio teórico de cómo trasladar las protestas de las calles a Internet.

Examinan las tácticas de la protesta callejera y elaboran hipótesis sobre cómo se pueden aplicar estas prácticas a la infraestructura de Internet. Antes de 1998, la desobediencia civil electrónica no dejaba de ser, en su mayor parte, una cavilación teórica. Pero tras la masacre de Acteal, en Chiapas, se produjo un giro hacia una posición más híbrida regida por la concepción de la infraestructura de Internet a la vez como un medio de comunicación y como un ámbito de acción directa.[27]

Con ese fin, se creó en 1998 el *Electronic Disturbance Theater* (EDT), por parte de tres artistas: Ricardo Domínguez (nació en Las Vegas en 1959, vive en Nueva York y es hijo de padres mexicanos), Brett Stalbaun (de San José, California) y Carmin Karasic.

Una frase citada por Domínguez en un mensaje que envió a un foro de activistas explica cuál es el vínculo entre artistas y activistas: "Los historiadores del arte saben que los grandes y afamados genios del renacimiento no sólo crearon pinturas y edificios, sino que además diseñaron fortalezas y construyeron máquinas de guerra. Si el fantasma de la guerra informática se hiciera realidad, los *hackers* tomarían el lugar de los históricos artistas-ingenieros".[28]

Los zapatistas y el primer "bloqueo virtual” a gran escala

Una "sentada" o "bloqueo virtual" es el equivalente electrónico de sus pares físicos. En ambos casos, el objetivo es centrar la atención sobre los manifestantes a través de la interrupción de las operaciones normales y del bloqueo en el acceso a determinados lugares.

Este concepto fue inaugurado por el *Electronic Disturbance Theater,* que en 1988 organizó una serie de acciones, primero contra el sitio del presidente mexicano Ernesto Zedillo, y luego contra los sitios de la Casa Blanca, el Pentágono, la Escuela de las Américas

---

[26] Wray, Stefan. La desobediencia electrónica civil y la world wide web del hacktivismo: La política extraparlamentaria de acción directa en la red (http://aleph-arts.org/pens/wray.html).

[27] Ibid.

[28] Domínguez, Ricardo, 26 de mayo de 1998. La frase pertenece a un joven activista alemán llamado Frederich Kittler. Se puede leer el texto completo en: http://www.aec.at/infowar/NETSYMPOSIUM/ARCH-EN/msg00138.html

y las bolsas de valores de Franckfurt y México. El propósito fue demostrar solidaridad con los zapatistas mexicanos.

Todo comenzó cuando en enero de 1998, un grupo activista italiano, llamado *Anonymous Digital Coalition* hizo circular la propuesta de realizar un bloqueo virtual sobre cinco sitios de entidades financieras mexicanas. Su sugerencia fue que si una gran cantidad de personas se ponían de acuerdo y apretaban el botón de Recargar de su navegador varias veces seguidas, los sitios podrían ser efectivamente bloqueados.

Basándose en esa teoría de acción simultánea, colectiva y descentralizada con un sitio determinado, Brett Stalbaun, del EDT, diseñó un software especializado —al que llamó FloodNet— que se encargó de automatizar la tarea de recarga sobre los sitios escogidos.[29]

Según Stalbaum, el Pentágono fue elegido debido a la creencia de que el ejército estadounidense entrenó allí a los soldados que llevaron a cabo varios abusos contra los derechos humanos en Latinoamérica. Por la misma razón fue elegida la Escuela de las Américas. La bolsa de Frankfurt, en cambio, fue escogida "porque representa el rol del capitalismo en la globalización utilizando las técnicas del genocidio y la limpieza étnica, la cual es la raíz de los problemas de Chiapas. La gente de Chiapas debería tener un rol preponderante en determinar su destino, en vez de ser forzadas a una relocalización a punta de pistola, hecho que es actualmente financiado por el capital occidental".[30]

Los integrantes del EDT distribuyeron el nuevo software a través de Internet. Todo lo que los interesados en participar de estas acciones debían hacer era visitar uno de los sitios de FloodNet. Al hacerlo, su programa de navegación bajaba a sus computadoras el *software* (un *applet* de Java), que accedería al sitio elegido como objetivo varias veces por minuto.

Adicionalmente, el *software* permitía a los manifestantes dejar sus proclamas en el *error log* del servidor del sitio agredido. Por ejemplo, al apuntar sus navegadores hacia un archivo no existente tal como *human_rights* (derechos humanos) en el servidor atacado, el mismo les enviaba —y almacenaba— el mensaje *human_rights not found on this server*

(derechos humanos no encontrados en este servidor).

El EDT estimó que unas 10.000 personas de todo el mundo participaron en el ataque realizado el 9 de septiembre de 1998 contra los sitios del presidente Zedillo, el Pentágono y la Bolsa de Franckfurt, enviando 600.000 *hits* por minuto a cada uno de ellos.

El Pentágono contraataca

El ataque ya había sido anticipado por el Pentágono. Cuando sus servidores detectaron la "invasión", lanzaron una contraofensiva contra los navegadores de los usuarios, redireccionándolos a una página con un *applet* (pequeña aplicación) llamado "*HostileApplet*." Una vez allí, el *applet* era bajado a sus navegadores, y les hacía recargar un mismo documento sin parar hasta que las computadoras fueran apagadas y vueltas a encender.

---

[29] Wray, Stephan. *The Electronic Disturbance Theater and Electronic Civil Disobedience*. Junio 17, 1998. Se lo puede leer en: http://www.nyu.edu/projects/wray/EDTECD.html

[30] Denning, Dorothy E. : *Hacktivism: An Emerging Threat to Diplomacy*. Artículo publicado en el sitio del American Foreign Service Association (http://www.afsa.org/fsj/sept00/Denning.html)

La bolsa de valores de Franckfurt reportó que estaba al tanto de la protesta, pero la misma no había afectado sus servicios. Según explicaron, normalmente reciben seis millones de visitas por día, por lo cual esta carga adicional no les generó inconvenientes.

El sitio del presidente Zedillo no contraatacó en esa ocasión, pero en una "sentada virtual" realizada en junio del año siguiente usó un *software* que provocó que los navegadores de los manifestantes abrieran una ventana detrás de otra hasta que sus computadoras debieran ser apagadas y vueltas a encender.

El EDT consideró al ataque como un verdadero éxito. "Nuestro interés es ayudar a la gente de Chiapas para que siga recibiendo el reconocimiento internacional que necesita para sobrevivir", dijo Stalbaum.[31]

En relación con el impacto de los ataques, Ricardo Domínguez afirmó: "El zapatismo digital es y ha sido uno de los usos de Internet políticamente más efectivos que conocemos. Ha creado una red de distribución de información con 100 o más nodos autónomos de soporte. Eso ha permitido al Ejército Zapatista de Liberación Nacional (EZLN) hablar al mundo sin tener que pasar por el filtro de los medios dominantes. Los zapatistas fueron elegidos por la revista *Wired* como uno de los 25 grupos online más importantes en 1998".[32]

Kosovo: La primera guerra peleada en Internet

El conflicto bélico en torno a la provincia serbia de Kosovo que tuvo lugar en 1999 es citado a menudo como la primera guerra peleada en forma paralela a través de Internet. Actores gubernamentales y no gubernamentales usaron la Red para diseminar información, difundir propaganda, demonizar a sus oponentes y solicitar apoyo para sus posiciones. Personas de todo el mundo usaron a Internet para debatir sobre el tema e intercambiar texto, imágenes y videoclips que no estaban disponibles a través de otros medios.

Los *hackers* hicieron oír sus opiniones tanto sobre la agresión de la OTAN como sobre la de Yugoslavia, interfiriendo servicios en computadoras gubernamentales y bloqueando sus sitios.

En abril de 1999, el diario *Los Angeles Times* señaló que el conflicto de Kosovo estaba transformando al ciberespacio en "una zona etérea de combate donde la batalla por las mentes y los corazones es peleada a través del uso de imágenes, listas de discusión y ataques de hackers".[33]

Anthony Pratkanis, profesor de psicología en la Universidad de California y autor de *Age of Propaganda: The Everyday Use and Abuse of Persuasion*, señaló: "Lo que estamos viendo ahora es sólo el primer round de lo que será una importante y altamente sofisticada herramienta en las técnicas de la propaganda de guerra... los estrategas bélicos deberían sentirse preocupados."[34]

---

[31] Ibid.

[32] Entrevista publicada en el sitio del EDT: http://www.thing.net/~rdom/ecd/ecd.html

[33] Ashley Dunn, *Crisis in Yugoslavia: Battle Spilling Over Onto the Internet*. Los Angeles Times, 3 de abril de 1999.

[34] Denning, Dorothy E. *Activism, hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Se puede leer el texto completo en: http://www.nautilus.org/infopolicy/workshop/ppers/denning.html

Es importante señalar que, mientras que la OTAN intentó silenciar a los medios de comunicación que difundían la propaganda del gobierno serbio de Milosevic, no bombardeó, intencionalmente, a los proveedores de servicios de Internet, ni cerró los canales satelitales que llevaban a Internet a Yugoslavia. La política fue mantener a Internet abierta. James P. Rubin, vocero por aquel entonces del Departamento de Estado, dijo: "El acceso pleno y abierto a Internet contribuirá a que los serbios conozcan la espantosa verdad acerca de los crímenes de lesa humanidad perpetrados en Kosovo por el régimen de Milosevic".[35]

Durante todo el desarrollo del conflicto, la población serbia tuvo pleno acceso a Internet, incluyendo los sitios occidentales. El *Washington Post* informó que, según fuentes oficiales de Estados Unidos e Inglaterra, el gobierno de Milosevic permitió que los cuatro proveedores de acceso a Internet de Yugoslavia permanecieran abiertos, con el objetivo de contribuir a diseminar información falsa y propaganda. El *Washington Post* también dijo que Belgrado, con una población de 1,5 millones de habitantes, tenía alrededor de 100.000 personas conectadas a Internet en abril de 1999. Además, había varios cibercafés donde los interesados que no tenían computadoras podían acceder a la Red.[36]

A pesar de que los serbios tenían acceso a programas televisivos occidentales, tanto a través de Internet como por medio de la televisión satelital y por cable, la mayoría no creía lo que escuchaba ni veía en tales medios. En general consideraban que la cobertura de las estaciones televisivas occidentales como la CNN y Sky News era tan tendenciosa como las de los canales oficiales yugoeslavos. Alex Todorovic, un serbio radicado en Estados Unidos que pasó un tiempo en Belgrado durante el conflicto, observó: "Mayoritariamente, los serbios descreen de los medios del resto del mundo. La CNN, por ejemplo, es considerada la voz oficial de Washington."[37]

El *hacktivismo* durante el conflicto de Kosovo

Manifestantes virtuales de ambos lados usaron "bombas de e-mail" (envío masivo de mensajes) contra sitios gubernamentales. El vocero de la OTAN Jamie Shea dijo que su servidor había sido saturado hacia fines de marzo por un individuo que les envió alrededor de 2.000 mensajes diarios. Fox News informó que cuando Richard Clarke, un residente de California, escuchó que el sitio de la OTAN había sido atacado por hackers de Belgrado, replicó enviando "bombas de e–mail" al sitio del gobierno yugoslavo. En pocos días llego a enviar medio millón de mensajes, con lo cual logró poner al servidor de e-mail del sitio fuera de servicio. Su proveedor de acceso a Internet, Pacific Bell, le cortó el servicio alegando que sus acciones habían violado la política de *spamming* (envío de mensajes no solicitados) de la empresa.[38]

Varios sitios fueron hackeados durante el conflicto de Kosovo. Según Fox News, El *Boston Globe* informó que un grupo estadounidense de hackers llamado Team Spl0it ingresó a sitios gubernamentales serbios y puso carteles tales como "Díganle a su gobierno que detenga la guerra". Fox también afirmó que el *Kosovo Hackers Group*, una coalición de

[35] Briscoe, David. *Kosovo-Propaganda War*. Cable de la agencia Associated Press, 17 de mayo de 1999.

[36] Dobbs, Michael. *The War on the Airwaves*.Washington Post, 9 de abril de 1999.

[37] Todorovic, Alex. *I´m Watching Two Different Wars*, Washington Post, 18 de abril de 1999.

[38] Denning, Dorothy E. Op. Cit.

hackers europeos y albaneses, reemplazaron por lo menos cinco sitios con carteles negros y rojos diciendo *Free Kosovo.*[39]

La agencia serbia de noticias SRNA reportó que el grupo de hackers serbios *Black Hand* borró todos los datos de un servidor de la marina estadounidense, según el diario de Belgrado *Blic*. Los miembros de los grupos *Black Hand* y *Serbian Angel* planearon acciones diarias destinadas a bloquear e interferir con las computadoras militares utilizadas por países de la OTAN.

Previamente, *Black Hand* se había atribuido la responsabilidad por la caída de un sitio albanés con información sobre Kosovo. "Continuaremos removiendo todas las mentiras que los albaneses étnicos ponen en Internet", le dijo a *Blic* un miembro del grupo mencionado.[40]

Hackers chinos entran en escena

Luego de que la OTAN bombardeara accidentalmente la embajada de China en Belgrado, varios *hackers* chinos fueron acusados de violentar distintos sitios gubernamentales estadounidenses. Según informó *Newsbytes,* el slogan "*Down with barbarians*" fue colocado, en chino en la página de la embajada estadounidense en Pekín, mientras que el sitio del Departamento del Interior mostró imágenes de los tres periodistas muertos durante el bombardeo, una multitud protestando por el ataque en Pekín y una bandera china flameando.

Según el *Washington Post*, el vocero del mencionado departamento, Tim Ahearn, dijo que sus expertos en computadoras habían rastreado a los *hackers* chinos. El mismo diario afirmó que en la página principal del Departamento de Energía fue colocada la siguiente proclama:

Protest USA´s nazi action! Protest NATO´s brutal action! We are Chinese hackers who take no cares about politics. But we can not stand by seeing our Chinese reporters been killed which you might have know.

Whatever the purpose is, NATO led by U.S.A. must take absolute responsibility. You have owed Chinese people a bloody debt which you must pay for. We won´t stop attacking until the war stops!"[41]

El caso del avión espía

El 1 de abril de 2001, un avión estadounidense de reconocimiento debió efectuar un aterrizaje de emergencia en la isla china de Hainan, 640 kilómetros al sudoeste de Hong Kong, luego de colisionar con un caza chino que había salido a interceptarlo. Ninguno de sus 24 tripulantes fue herido.

---

[39] Riley, Patrick. E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight. Fox News, 15 de abril de 1999.

[40] Denning, Dorothy E. *The Internet as a Tool for Influencing Foreign Policy* (versión corregida y actualizada). Texto disponible en: http://www.carta.org/campagne/scienza_tecnologia/hacker/Activism.htm

[41] Barr, Stephen. *Anti-NATO Hackers Sabotage 3 Web Sites*. Washington Post, 12 de mayo de 1999.

La colisión y los 11 días de detención que sufrió su tripulación causaron las peores tensiones entre Beijing y Washington desde el accidental bombardeo de la Embajada china en Belgrado.

China culpó a la tripulación estadounidense por causar el accidente y la acusó de violar su soberanía al efectuar un aterrizaje de emergencia no autorizado en Hainan. Washington, por su parte, atribuyó el incidente al piloto chino, diciendo que él había realizado una maniobra temeraria que derivó en la colisión de su caza con el EP–3. El piloto chino se lanzó en paracaídas y fue dado por muerto tras una prolongada búsqueda.

El conflicto entre ambos países terminó el 3 de julio, cuando las últimas piezas del avión espía fue retenido en China fueron transportadas hacia Filipinas por vía aérea desde la isla de Hainan.

Mientras duró el conflicto, se generó un importante "duelo" (mucho mayor que el que tuvo lugar durante el conflicto de Kosovo) entre *hackers* chinos y estadounidenses.

Según un artículo publicado en la revista *Wired* el 18 de abril de 2001, elgrupo de *hackers* estadounidenses PoizonBOx atacó a por lo menos un centenar de sitios chinos desde el 4 de abril.[42]

Según la misma fuente, un *hacker* conocido como Pr0phet (quien figura en la lista de Attrition.org[43] como responsable del *hacking* de dos sitios chinos), instó a los *hackers* estadounidenses a "enfocarse en China y desencadenar el infierno sobre sus servidores".

Pr0phet no creía que los ataques pudieran tener ninguna influencia política, pero su objetivo era "simplemente joder a los chinos por todos los medios posibles".

Un día antes, el FBI reconoció, en una nota publicada por el servicio informativo de Yahoo!, que fueron atacados algunos sitios estadounidenses. Si bien el FBI declinó dar mayores precisiones sobre los sitios agredidos, afirmó que dos de ellos pertenecían a la U.S. Navy, y otros dos eran sitios de comercio electrónico sin vínculos visibles con la crisis sino–estadounidense.

La *Hackers Union of China* se autoadjudicó el ataque a uno de estos dos sitios, perteneciente a una empresa con base en California, y colocó allí una lista de otros 10 sitios que fueron atacados en la memoria del piloto chino que murió en el accidente.[44]

Max Vision, un especialista en seguridad que había estado monitoreando el accionar de la *Hackers Union of China*, describió a ese grupo como "una banda muy bien organizada". En su sitio, cnhonker.com, el grupo se autodefine como una organización de seguridad de redes.

Un artículo del *Washington Post* reveló que una pequeña empresa estadounidense llamada Intelligent Direct Inc. fue agredida por *hackers* durante una semana entera. El presidente de la compañía, Dan Olasin, afirmó que cada vez que intentaba ingresar a su sitio

---

[42] Delio, Michelle. *Crackers Expand Private War*. Wired News, 18 de abril de 2001. Se puede leer el artículo completo en: http://www.wired.com/news/politics/0,1283,43134,00.html

[43] El sitio www.attrition.org lleva en forma constante un listado de los sitios hackeados alrededor del mundo, y es considerada la fuente más confiable de información y estadísticas sobre el tema, tanto por los *hackers* como por los medios de comunicación y los organismos oficiales estadounidenses.

[44] Weisman, Robyn. Artículo distribuido por Yahoo!, publicado originalmente en el sitio NewsFactor.com el 17 de abril de 2001.

www.zipcodemaps.com, se encontraba con que la página principal era reemplazada por una bandera china y mensajes como *China have atom bombs too*.[45]

Jia En Zhu, un *hacker* de 22 años que vive en Zhongguancun, un suburbio de Pekín que ha sido calificado como "El Silicon Valley de China", al ser entrevistado por la revista *Wired* afirmó que muy probablemente hayan habido ataques no reportados desde el primero de abril. "Mucha gente aquí habla sobre el episodio del avión. Nosotros no entendemos por qué el gobierno estadounidense no puede pedir disculpas por haber matado a nuestro piloto. Pero no tenemos mecanismos para decirles esto a ustedes en forma directa", dijo. "Estamos frustrados por la fría corrección con la que actúa nuestro gobierno. Queremos decirles a los estadounidenses que están actuando mal, y lo decimos a través de Internet".[46]

Hacktivismo independiente

El analista del sitio SecurityFocus.com Ryan Russell rechazó en su momento la posibilidad de que el gobierno chino alentara estos ataques, así como el grado de representatividad que los mismos puedan tener. "Se supone que protestan por el asunto del avión espía. Sin embargo, en general los sitios que atacaron no tienen la más remota relación con temas militares. Simplemente atacaron a un par de sitios porque eran vulnerables y parecían ser estadounidenses".

"Recientemente chequeamos los registros en nuestro sistema ARIS en relación con los ataques originados desde China, durante las dos semanas que siguieron al incidente del avión, y no hubo ningún incremento significativo", señaló Russell. "Lo que tenemos aquí es un puñado de tipos causando problemas y diciendo que representan a China, pero yo no creo que representen a nadie más que a ellos mismos", afirmó.[47]

A través de un artículo difundido en un grupo de noticias sobre seguridad informática, Brian Martin, del sitio Attrition.org, restó credibilidad a la información periodística que se publicaba sobre este tema, especialmente al artículo de la revista *Wired* citado anteriormente.

"Si uno observa tanto la trayectoria de pr0phet como la de poisonb0x, queda totalmente claro que ninguno de los dos tiene una agenda política. Pasaron 10 días entre el incidente del avión espía y la publicación del primer artículo en *Wired*. Durante ese lapso, ningún grupo hizo referencia política alguna. Fue sólo después de los artículos de *Wired* que una serie de

actos de *hacking* fueron interpretados en ese sentido. Claramente *Wired* tomó una historia sin substancia y creó noticias de la nada".

Además, agregó que los artículos de *Wired* hacían referencia a *hackers* que actuaban en el nombre de China, pero “la verdad es que no se puede verificar si realmente los ataques fueron hechos por hackers chinos o por cualquier otra persona que busque inflamar la situación”.[48]

---

[45] Eunjung Cha, Ariana. *Chinese Suspected of Hacking U.S. Sites*. Washington Post Staff Writer. 13 de abril de 2001. El artículo se puede leer en: http://www.washtech.com/news/media/8997-1.html

[46] Delio, Michelle. *A Chinese Call to Hack U.S*. Wired News, 11 de abril de 2001. Se puede leer el artículo completo en: http://www.wired.com/news/politics/0,1283,42982,00.html

[47] Weisman, Robyn. Op. Cit.

[48] Martin, Brian. *Cyberwar with China: Self-fulfilling Prophecy*. Artículo publicado en Attrition.org el 29

Actos de hacktivismo tras los atentados del 11 de septiembre

Los atentados terroristas que tuvieron lugar en Estados Unidos el 11 de septiembre de 2001 generaron una rápida reacción entre algunos miembros de la comunidad *hacker*. La primera acción concreta difundida por los medios masivos tuvo lugar al día siguiente, el 12 de septiembre. Un *hacker* ruso llamado Ryden atacó al sitio taleban.com, correspondiente a la denominada "Misión Afgana de Talibán". La página principal fue alterada y se colocó en la misma una foto de Osama Bin Laden, con un texto acusándolo por el atentado.[49] El mismo *hacker* ya había atacado al sitio taleban.com en marzo y en julio de ese mismo año, según los registros mantenidos por alldas.de y safemode.org.

Pocos días más tarde se anunció públicamente la creación del grupo *The Dispatchers*, creado por 100 *hackers* de distintos países decididos a perturbar a través de Internet a aquellas naciones y organizaciones que apoyen al terrorismo islámico. Uno de los principales integrantes del grupo era un *hacker* canadiense que decidió llevar a cabo esa alianza al constatar que entre las víctimas de los atentados contra las Torres Gemelas figuraban amigos y familiares suyos.[50]

Posteriormente, según un cable de la agencia France-Presse fechado el 10 de octubre, *The dispatchers* se atribuiría el haber puesto fuera de servicio a algunos sitios palestinos e iraníes.[51] Otras acciones retaliatorias, cuya autoría es desconocida, fueron las siguientes:

. El sitio oficial del Palacio Presidencial de Estado Islámico de Afganistán (wwww.afghan.gov.af) permaneció un tiempo fuera de servicio, luego de que su dirección fuera publicada en distintos *newsgroups* (grupos de noticias) en Internet, en los que indirectamente se alentaba a atacarlo. "Que el gobierno afgano sepa que es lo que nosotros pensamos acerca del asilo que le dan a Bin Laden", decía un texto publicado en el *newsgroup* talk.guns.politics.

. El sitio de la República Islámica de Paquistán (www.pak.gov.pk) también estuvo por momentos fuera de servicio, a pesar de las declaraciones publicadas en el sitio, en la cuales el presidente paquistaní Pervez Musharraf condenó severamente los ataques terroristas. La dirección del sitio había sido exhibida poco tiempo antes en el *newsgroup* alt.hackers.maliciuous, en un mensaje titulado "El gobierno pakistaní ama a los troyanos" (en alusión a los virus conocidos como troyanos).[52]

Young Intelligent Hackers Against Terror (YIHAT)

Una de las iniciativas antiterroristas más llamativas procedentes del mundo de los *hackers* fue la llevada a cabo por Kim Schmitz, un *hacker* alemán transformado en consultor de se-

---

de abril de 2001. Se puede leer en : http://attrition.org/security/commentary/cn-us-war.html

[49] Noticias.com, 14 de septiembre de 2001.

[50] Cortés, Angel. Artículo publicado en Noticias.com. 17 de septiembre de 2001.

[51] Lever, Rob. Cable de la agencia France-Presse, 10 de octubre de 2001.

[52] McWilliams, Brian. Artículo publicado en Newsbytes.com

guridad, quien abrió un sitio en Internet para reclutar a otros *hackers* a fin de rastrear flujos de fondos y otras evidencias que vinculen a Bin Laden con los atentados del 11 de septiembre.

Poco tiempo después del lanzamiento de su grupo, al que llamó YIHAT (*Young Intelligent Hackers Against Terror*), Schmitz afirmó que 34 personas de 10 países, junto con tres traductores de idioma árabe, se habían sumado a su iniciativa. Schmitz había sido acusado de ingresar ilegalmente a computadoras de la NASA y el Pentágono durante los ´90. "Creo que el mundo libre debe unirse ahora. Sólo podremos derrotar al terrorismo si luchamos contra el mismo en todas partes... en unos pocos años los terroristas tendrán armas biológicas y nucleares y no matarán a 5.000 personas sino a 5 millones con un solo golpe", dijo Schmitz en su sitio53.

David Endler, un analista de la empresa de seguridad iDefense, de Virginia, Estados Unidos, le dijo a un periodista de France-Presse que *hackers* de YIHAT ingresaron en un banco sudanés y obtuvieron información sobre cuentas vinculadas con Bin Laden. Supuestamente le dieron esa información al FBI.

"Sus motivaciones tal vez sean justas, pero sus acciones pueden causar daño y pueden traer aparejadas otras implicancias para la privacidad de las personas"54, dijo Endler en relación con los *hackers* que decidieron "hacer justicia" por su propia cuenta.

El *National Infrastructure Protection Center*, del FBI, se hizo eco de esa opinión y señaló que las conductas descriptas "son ilegales y punibles, con penas que pueden llegar a los cinco años de prisión. Los individuos que creen que están un servicio a la Nación a través de ese tipo de acciones, deberían saber que en realidad están jugando en contra".55

No todos los *hackers* se adhirieron a la postura activista. La legendaria organización con sede en Alemania llamada *Chaos Computer Club* (CCC), fundada 20 años atrás en Hamburgo, manifestó su oposición categórica a los llamamientos de otros *hackers* para atacar y sitios islámicos en Internet. En un e-mail, Andy Mueller-MaguHn, portavoz del CCC, afirmó: "Precisamente ahora, los medios de comunicación electrónicos como Internet pueden contribuir de forma importante a la comprensión entre los pueblos. Con la tensión actual, no podemos bloquear los medios de comunicación y abrir así un terreno aún más amplio a la incomprensión", añadió56.

53 Lever, Rob. Op. Cit.
54 Ibid.
55 Ibid.
56 Cortés, Angel. Op. Cit.

31

Capítulo IV: El uso de Internet por parte de distintos grupos terroristas o guerrilleros

Las Fuerzas Armadas Revolucionarias de Colombia (FARC)

En 1996, la comisión internacional de las FARC, el principal grupo insurgente de Colombia, recomendó crear una página interactiva para poder comunicarse con todo el mundo desde los frentes de combate, según le

relató un vocero de esa organización al corresponsal en Colombia del diario argentino Clarín[57].

Las FARC cuentan con aproximadamente 17.000 hombres y se estima que tienen presencia en el 40 por ciento del territorio nacional colombiano. Es la fuerza insurgente más grande de América Latina que sobrevive desde la década de los sesenta y, según fuentes militares, obtiene aproximadamente 600 millones de dólares anuales del tráfico de drogas, el secuestro y la extorsión.

La construcción del sitio se hizo a través de delegados internacionales como Marcos León Calarcá, quien desde la ciudad de México coordinó la colocación de un sitio en un servidor de la empresa mexicana Teesnet. Ese sitio funcionó hasta setiembre de 1996, cuando la empresa canceló el servicio por las implicaciones políticas internacionales que involucraba. Cuatro meses más tarde los rebeldes volvieron a lanzar su página en un servidor canadiense vinculado al campus de la Universidad de California en San Diego. Sin embargo, su presencia violaba las normas del servicio virtual de dicha universidad, que prohiben las páginas *web* que "promuevan daños o perjuicios contra cualquier grupo o individuo".

Las FARC estuvieron casi medio año fuera de Internet hasta que lograron acceder a un servidor en Canadá, conectado a la Universidad de California. Cuando en Estados Unidos se enteraron de la situación volvieron a sacarlos de la Red acusándolos de promover ataques contra terceros y de violar las normas informáticas norteamericanas. En 1999 consiguieron en forma

[57] Padilla, Nelson. *Internet, otro campo de batalla donde se libra la guerra colombiana*. Diario Clarín, 7 de julio de 2001. Se puede leer el artículo completo en: http://ar.clarin.com/diario/2001-07-07/i-04601.htm

clandestina otro servidor en el cual su sitio (www.FARC-ep.org) funciona actualmente en seis idiomas: español, inglés, francés, italiano, alemán y portugués. Por razones de seguridad, los miembros de las FARC no quieren revelar el nombre del servidor. "Contar dónde está nuestro servidor solamente ayudaría a nuestros enemigos", dijo por e-mail desde México a un periodista de la revista Poder Olga Marín, una de las principales representantes internacionales de las FARC[58]. Agregó, sin embargo, que el servicio cuesta 200 dólares al año, suma pagada por un grupo de apoyo internacional. Un solo miembro de las FARC, con base en la ciudad de México, es el responsable del diseño *web*, en tanto que el contenido, una mezcla de comunicados, historia de la organización y fotos diminutas, es suministrado por los comandantes y los combatientes.

En la página se pueden leer desde los partes de guerra a partir de 1997 hasta poemas escritos por guerrilleros. También se publica una revista

online y un programa radial llamado Radio Resistencia, en el cual se presentan entrevistas con comandantes rebeldes[59]. Además hay una página universitaria, porque buena parte de los mensajes están dirigidos a captar la atención de los jóvenes colombianos, que resultan potenciales militantes.
"Pelear sólo a través de Internet sería como disparar con balas de caucho. No utilizar Internet sería seguir peleando contra el Ejército con una escopeta", dijo Calarcá[60] al reconocer la importancia estratégica de este servicio.
Las FARC usan a Internet como un medio para intensificar su actividad política a través de un trabajo de *lobby* y propaganda. Según la agencia de noticias brasileña Estado, desde comienzos del 2001, personas influyentes, así como funcionarios gubernamentales de Brasil y dirigentes de organizaciones no gubernamentales de ese país -e incluso empresarios- comenzaron a recibir e-mails propagandísticos de las FARC, sin haberlos solicitado[61].

No todo es propaganda

Cuando en su calidad de Presidente electo Andrés Pastrana viajó a las profundidades de la selva para entrevistarse con el veterano comandante supremo de las FARC, Manuel Marulanda Vélez "Tirofijo" en julio de 1998, para iniciar las conversaciones de paz, los preparativos fueron

[58] Penhaul, Karl. *Novedad en el frente*. Revista Poder (ex Punto-Com). Para leer el artículo completo, ir a: http://www.revistapoder.com/NR/exeres/12BEF2DE-2EA0-4CA7-83A9-E8CD15021975.htm
[59] Scheeres, Julia. *Blacklisted Groups Visibles on Web*. *Wired News*, sin fecha. Se puede leer en: http://www.wired.com/news/politics/0,1283,47616,00.html
[60] Penhaul, Karl. Op. Cit.
[61] Pinto, Lucio Flavio. *A guerrilha na Internet*. Agencia de noticias Estado (Brasil). 2001. Se puede leer el artículo en: http://www.estadao.com.br/agestado/politica/2000/dez/09/139.htm

realizados minuto a minuto a través de Internet. En un episodio que parecía más tomado de James Bond que de la historia de la guerrilla más antigua de occidente, Marulanda -quien actualmente tiene más de 70 años- se mantenía ante su *laptop* conectado por teléfono satelital, enviándole por correo electrónico a un intermediario indicaciones exactas acerca de su paradero. Los mensajes eran retransmitidos de inmediato a Pastrana mientras volaba en un avión de la Cruz Roja al lugar de reunión en un campamento secreto de la guerrilla[62].
Con el advenimiento del Plan Colombia, financiado por Estados Unidos para combatir el comercio de heroína y cocaína en el sur de ese país, los jefes de las FARC súbitamente encontraron nuevos motivos para navegar. En medio de las selvas del sur colombiano, y ante la mirada de un periodista extranjero, un jefe guerrillero descargó un manual para aprender a pilotear un helicóptero Blackhawk, fabricado en Estados Unidos. El sitio

que suministra el manual es www.army.mil, del ejército norteamericano. "Esta información nos va a resultar muy útil", [63]dijo el comandante guerrillero, mientras buscaba puntos débiles en el diagrama del helicóptero para ver la mejor forma de planear un ataque. Veinte de esos helicópteros, que cuestan trece millones de dólares cada uno, le fueron donados al gobierno de Colombia por Washington.

Los organismos de inteligencia estadounidenses sostienen que las FARC han ingresado fraudulentamente en bases de datos confidenciales a través de Internet y han robado de ellas información acerca de viajeros, que luego han atrapado como rehenes en las carreteras como parte de operaciones de secuestros extorsivos. Un comandante regional de las FARC llamado Simón Trinidad se rió de esas informaciones. "En Colombia 50 familias dominan el sector financiero, industrial y exportador, y monopolizan la riqueza. No se necesita una computadora para averiguar quién es el dueño de la riqueza en este país"[64], dijo Trinidad, que fue gerente de oficina de una filial colombiana del Chase Manhattan Bank antes de unirse a las fuerzas rebeldes en 1987.

Ver una *laptop* con acceso a Internet en medio de la selva colombiana puede resultar un espectáculo digno del realismo mágico que popularizó en sus novelas García Márquez. Según la consultora Data Corporation (IDC), de Estados Unidos, a fines de 2000 había cerca de 700.000 usuarios de Internet en Colombia sobre una población de 40 millones, lo cual arroja una de las cifras per cápita más bajas del hemisferio (1,75 por ciento).

La baja cobertura telefónica también constituye un problema. Colombia tiene menos de 15 teléfonos por cada 100 habitantes, comparada con 68 por

[62] Penhaul, Karl. Op. Cit.

[63] Ibid.

[64] Ibid.

cada 100 habitantes en Estados Unidos, 24 por cada 100 en Argentina y 18 por cada 100 en Chile, siempre según datos de IDC.

Internet no es el único medio de información que utilizan los guerrilleros de las FARC. A través de antenas satelitales de Sky TV colgadas de los árboles, algunos de estos combatientes tienen acceso a más de 100 canales de deportes y entretenimiento provenientes de todas partes del mundo. "David Beckam es mi héroe. Lo veo en Sky cada vez que me lo permiten mis comandantes", le dijo un joven combatiente de las FARC llamado Andrés a un periodista extranjero[65], refiriéndose al entonces jugador estrella del equipo inglés de fútbol Manchester United.

La ETA

El uso de Internet con fines propagandísticos efectuado por la

organización separatista vasca ETA en España probablemente pase a la historia no por su originalidad ni por su intensidad, sino por los ataques que sufrió por parte de numerosos internautas españoles.

En 1997, la revista iWorld publicó:

> La comunidad española de internautas le ha plantado cara en la Red al grupo terrorista ETA y a su entorno, como reacción al secuestro y posterior asesinato del concejal del Partido Popular de Ermua (Vizcaya), Miguel Ángel Blanco Garrido. Al grito unánime de ¡Basta ya!, los internautas españoles han reproducido en los distintos servicios de la Red las masivas movilizaciones que se han repetido por todo el país desde que se conoció la noticia, uniéndose a la indignación general y a la repulsa por el brutal asesinato[66].

Pero la comunidad española de Internet no se conformó con sólo colocar mensajes de protesta. Llevados por la indignación, los internautas plantearon diversas iniciativas, entre ellas algunas tendentes a eliminar de la Red todas aquellas páginas *web* que sirven de apoyo a ETA o a su entorno radical. Estas actitudes de algunos internautas han sido polémicas, incluso se debatieron en el foro online de El País, el principal diario español.

La "línea dura" prevaleció. Un mes después del asesinato de Garrido se produjo un bombardeo de mensajes que intentó saturar al proveedor de servicios de Internet IGC (*Institute for Global Communication*) de San

[65] Ibid.

[66] Ferreira, Miguel Angel. *Los internautas españoles se unen contra ETA*. Revista iWorld, 1997. Ver el artículo completo en: http://www.idg.es/iworld/especial/basta_ya.html

Francisco, en Estados Unidos. El objetivo fue intentar desalojar al *Euskal Herria Journal*, una controvertida publicación pro-ETA editada por un grupo de simpatizantes desde Nueva York. Los atacantes alegaban que IGC "fomentaba el terrorismo"[67].

Como resultado de la acción, el servidor de e-mail de IGC se atascó. Muchos usuarios de IGC quedaron sin poder recibir su correo, y su línea telefónica de ayuda colapsó ante las llamadas de clientes enojados. Los atacantes también mandaron "correo basura" a los clientes y trabajadores de IGC, y colgaron sus páginas *web* a base de ordenes de compra con números de tarjeta de crédito erróneos. Luego amenazaron con repetir estas acciones contra todos los que usaran los servicios de IGC. Para detener el ataque, IGC bloqueó el acceso de todos los servidores atacantes, medida efectiva pero imposible de sostener en el tiempo[68]..

IGC cerró el sitio del *Euskal Herria Journal* el 18 de Julio de 1997.

Algunos días después del cierre, el sitio reapareció en otros tres servidores. Chris Ellison, portavoz de Campaña por la Libertad en Internet -grupo inglés que alojó uno de dichos sitios- manifestó que "la Red debe generar la oportunidad de leer y discutir sobre ideas controvertidas".[69]
La publicación electrónica sostuvo que su objetivo era "proporcionar información a veces ignorada por la prensa internacional" y "construir puentes de comunicación para un mejor entendimiento del conflicto"[70].
En un artículo publicado en el periódico francés *Le Monde*, el columnista Yves Eudes opinó que el bombardeo de e-mails representaba un "precedente que abría una nueva era de censura, impuesta por la acción directa de hackers anónimos".[71]
El gobierno español tomó posición por el lado de la censura. Varios sitios estadounidenses, principalmente el de la CNN, cubrían el conflicto, y como práctica habitual, ponían en sus artículos *links* a diferentes sitios vinculados con el tema. Allí figuraban enlaces al *Euskal Herria Journal*. Las autoridades españolas solicitaron que esos *links* fueran removidos. La CNN se manifestó sorprendida por esas demandas y se negó, sugiriendo que agregaría en su sitio más *links* a sitios que expresen la postura del gobierno español.[72]
Alrededor de un mes después de que IGC. echara de sus servidores a la controvertida publicación vasca, la Brigada Antiterrorista de Scotland Yard

[67] Artículo publicado en el sitio Ciberpol. Se puede leer en: http://www.ciberpol.com/spa/terror/usa_espia_eta.htm
[68] Ibid.
[69] Denning, Dorothy. Op. Cit.
[70] Ibid.
[71] Yves Eudes, *The Zorros of the Net*. Le Monde, 16 de noviembre de 1997. El artículo se puede leer traducido al inglés en el siguiente sitio: http://www.ehj-navarre.org/html/lmonde.html
[72] Ibid.

cerró el servidor en el Reino Unido del grupo Campaña por la Libertad en Internet, por alojar a dicha publicación. Tras ese episodio, el grupo inglés manifestó que trasladaría sus operaciones a Estados Unidos.
Un caso más reciente de *hacktivismo* anti-etarra se produjo el 23 de marzo de 2001, cuando piratas cibernéticos bloquearon la página principal del periódico vasco GARA (www.gara.net) donde la ETA publica con frecuencia sus pronunciamientos políticos o asume la responsabilidad por ataques perpetrados. Los piratas cibernéticos insertaron en el sitio el siguiente mensaje: "Esta *web* ha sido hackeada en recordatorio a las víctimas de ETA y sus familiares. Basta Ya. No somos *hackers*, somos españoles indignados".[73]

Hacktivismo pro etarra

Según un artículo publicado en el diario argentino La Nación, algunos cuadros de ETA decidieron efectuar un "contraataque virtual". Con tal objetivo, se dedicaron a rastrear el origen de miles de mensajes que le reclamaban cesar con la violencia, y con esos datos en su poder, bloquearon las páginas de algunos de los manifestantes virtuales[74].

El caso más notorio de hacktivismo pro etarra tuvo lugar en abril de 2000, cuando un grupo de activistas modificaron la página oficial del museo Guggenheim. Durante varias horas cambiaron el aspecto del sitio del museo más emblemático de Bilbao y lo llenaron con slogans independentistas y fotos de miembros encarcelados de la ETA. Las pancartas, en inglés y francés, calificaban como “opresor” al gobierno español[75].

Más allá de estos episodios, el uso de Internet por parte de militantes de ETA no ha evidenciado una concepción verdaderamente estratégica sobre los usos potenciales de la Red. Un artículo publicado en el sitio español Noticias.com en diciembre de 2000 afirmó que, según fuentes oficiales no identificadas, la ETA utilizaba a Internet como medio de información para adquirir datos valiosos acerca de sus potenciales víctimas. Tales datos eran extraídos mayoritariamente de sitios institucionales. Esto estaría generando en España un cierto retraimiento -en especial entre la clase empresaria- en cuanto a la información publicada en Internet. "La policía requisó a uno de los últimos comandos desarticulados una serie de disquetes con información extraída de Internet. Ese parece ser el nuevo y sencillo sistema que los terroristas utilizan para recabar información sobre individuos", dijo

[73] Goodman, Al. *ETA en la Red*. CNN en Español. El artículo completo se puede leer en: http://cnnenespanol.com/especial/2001/mundo.interactivo/stories/societies/eta/

[74] Caram, Cristian. *El lado oscuro de la Red.* La Nación, 4 de marzo de 2001.

[75] Ruisanchez, Pablo. Artículo publicado en el sitio Noticias. com el 18 de abril de 2000.

37

el artículo mencionado[76]. "El comando de ETA que opera en Catalunya pudo haber utilizado la Red para obtener datos sobre dos de las tres últimas víctimas de su estrategia rabiosa", prosigue. Esas dos víctimas fueron el guardia urbano Miguel Angel Gervilla Valladolid, asesinado de dos tiros en la cabeza y en el abdomen, y Francisco Cano Consuegra, el único concejal del Partido Popular en la localidad de Viladecavalls, también asesinado por ETA.

El IRA

El uso que el Ejército Republicano Irlandés (IRA) hace de Internet tiende a ser discreto y a evitar cualquier llamado a la lucha directa o a la violencia. Su estrategia de imagen busca evitar cualquier asociación con el terrorismo. No hay sitios ni publicaciones oficiales del IRA en Internet. La presencia

virtual de este grupo se da en forma indirecta, básicamente a través de su brazo político, el Sinn Féin. En su sitio (www.sinnfein.ie) hay un *link* a la versión *online* de *An Phoblacht / Republican News (*http://209.68.13.153/aprn/index.html*)*, una publicación semanal que viene bregando desde hace más de 25 años por la finalización del dominio británico en Irlanda del Norte, y que representa el ideario político del IRA.
El perfil moderado de los sitios vinculados al IRA hace que los casos de censura gubernamental sean escasos. El más llamativo tuvo lugar en Estados Unidos en octubre de 2001 –un mes después de los atentados contra las Torres Gemelas y el Pentágono- cuando un sitio acusado de apoyar al Real IRA (una facción disidente del IRA) fue cerrado por el FBI. El sitio (IRAradio.com), mantenido por John McDonagh y Travis Towle, dos residentes de Nueva York, transmitía un programa radial semanal llamado *Radio Free Eireann*.
La explicación oficial del gobierno estadounidense fue la siguiente: "El presidente Bush recientemente firmó una nueva ley que permite al FBI y la CIA confiscar activos sin previo aviso ante la presencia de evidencias razonables de que cualquier persona o empresa asista, apoye o haga algo que pueda ser calificado como terrorismo, o mantenga conexiones con terroristas de cualquier tipo"[77]. Asimismo, señalaron que el Real IRA tiene prohibido recaudar fondos en los Estados Unidos, y que cualquier persona que lo apoye puede ser enjuiciada y encarcelada.
También explicaron que si bien los autores del sitio afirman que no apoyan al terrorismo de ninguna clase, al revisar el código fuente del sitio se encontraron en los *meta tags* (lugar donde se escriben palabras que permanecen ocultas a los visitantes pero que son detectadas por los motores

[76] Ruisanchez, Pablo. Artículo publicado en el sitio Noticias.com el 21 de diciembre de 2000.
[77] Middleton , James. *FBI shuts down 'IRA' website.* Artículo publicado en vnunet.com (12-10-2001)

de búsqueda) expresiones como "bombs", "blowing up british", "down with the brits", "freedom" y "unrepentant fenian bastards".
Más allá de la censura oficial, existen varios casos de censura ejercida por servidores o universidades que tuvieron poca o ninguna difusión. Por ejemplo, en la página Irish Republican History and Information (http://wwwvms.utexas.edu/~jdana/history/repubhist.html) hay abundante información vinculada con Irlanda del Norte, pero al intentar hacer un click en alguno de los links que figuran bajo el subtítulo Irish Republican Army, se observa que los archivos fueron borrados.
• El archivo del link *History of the IRA* fue eliminado, y se puede comprobar que estaba almacenado en el servidor de la Universidad de Texas, en Austin.

• El archivo del link *The Irish Republican Army: Heroes Unifying a Nation*, también fue eliminado, y se observa que estaba en el servidor gratuito Angelfire.com.
• El archivo del link *The IRA: Peace or Posturing Does the IRA Really Want Peace?* También fue borrado, y pertenecía a la University of Winnipeg, en Canadá.

Ese fenómeno se reitera en forma permanente en Internet cuando de intenta acceder a sitios vinculados con grupos guerrilleros o terroristas, y evidencia que gran parte de las universidades y los servidores gratuitos escanean periódicamente sus servidores buscando información "comprometida" para eliminarla o bien solicitar a sus titulares que la eliminen.

Grupos extremistas islámicos

Como muchos otros grupos terroristas, los extremistas musulmanes encontraron en Internet un método conveniente para difundir propaganda y transmitir mensajes a sus seguidores alrededor del mundo.

Las autoridades estadounidenses siempre siguieron de cerca ese fenómeno. En febrero de 1998, Dale Watson, jefe de la sección de terrorismo internacional del FBI, informó a un comité del senado estadounidense que los principales grupos terroristas islámicos usaban a Internet para difundir propaganda y reclutar nuevos miembros.

A partir de los atentados del 11 de septiembre de 2001, los sitios que efectúan llamados a la "Jihad" o "Guerra Santa" fueron sometidos a una intensa vigilancia y en muchos casos fueron cerrados.

"Obtener información acerca de cómo recaudar fondos para una cruzada antioccidental, construir una bomba o hacer que los creyentes musulmanes se sumen a los campos guerrilleros de entrenamiento ha sido hasta ahora tan simple como ingresar a Yahoo! o algún otro portal de Internet", afirmó [39] Stephanie Gruner, columnista de *The Wall Street Journal*[78]. El buscador Yahoo!, afirmó Gruner, sirve como puerta de ingreso para docenas de sitios que ofrecen consejos múltiples sobre temas que van desde la utilización de armas de fuego hasta la creación de un estado islámico. Uno de estos sitios, localizado en Inglaterra, muestra un video donde se ve a un grupo de extremistas disparando a una foto de Bill Clinton.

A principios de octubre de 2001, las autoridades británicas arrestaron en Greenwich a Sulayman Balal Zainulabidin, un cocinero de 43 años, bajo la sospecha de actividades terroristas. Según Scotland Yard, el imputado fue el fundador de Sakina Security Ltd., un sitio basado en Londres que ofrece cursos de entrenamiento sobre armas.

Más allá de la acción gubernamental, a partir de los atentados del 11 de septiembre muchas compañías de Internet decidieron suspender por su cuenta a sitios sospechosos de apoyar al terrorismo.
Yahoo! Decidió eliminar de su buscador a *un web ring* (cadena de páginas entrelazadas) que albergaba a 55 sitios vinculados con el grupo Jihad Islámica.
La sección europea del buscador Lycos.com puso a un equipo de 20 personas para monitorear los sitios que figuran en su motor de búsqueda y remover a aquellos que alberguen contenido a favor del terrorismo u otras actividades ilegales.
Uno de los casos más resonantes fue el de Azzam.com, sitio a cargo de *Azzam Publications.* Dicha página, afiliada qoqaz.net fue víctima de una serie de allanamientos realizados en Alemania en septiembre de 2001. Azzam.com ofrece contenidos del tipo "Cómo me puedo entrenar para la Guerra Santa". La cantidad de visitas de ese sitio, disponible en más de una docena de lenguajes, se multiplicó por diez luego de los atentados de Estados Unidos, según un vocero de la empresa que prefirió omitir su nombre, quien respondió por e-mail a una pregunta formulada por un periodista.
Algunos de los sitios vinculados con Azzam fueron cerrados luego de que varias personas se quejaran ante las empresas de Internet que los albergaban. En uno de los casos, el sitio fue clausurado por pedido del FBI. El vocero de Azzam dijo que su empresa "nunca fue intimada por las autoridades", y agregó que "respeta las leyes de publicación del Reino Unido". Dijo también que Azzam ha condenado los recientes ataques contra Estados Unidos y no está de acuerdo con la decisión de las empresas de Internet que cerraron sus sitios. “¿Es esta la supuesta libertad de la que hablan tanto los estadounidenses?", se preguntó.
[78] Gruner, Stephanie. *Extremist web sites under scrutiny*. The Wall Street Journal, 8 de octubre de 2001.
40

Hizbollah

El grupo extremista Hizbollah tiene una importante presencia institucional a través de un sitio propio, que posee tres réplicas (*mirrors*, en la jerga informática) a fin de que si una es clausurada, se pueda acceder a las demás. El sitio y los tres mirrors funcionan perfectamente en las direcciones www.hizbulla.net, www.hizbollah.org, www.hizballah.org y www.hizbollah.tv.
El sitio está en árabe pero con una versión en inglés, donde entre otras cosas, se ofrece una amplia galería de fotos, archivos de audio con discursos propagandísticos y videos. Estos últimos, prolijamente

clasificados, muestran imágenes de temas tales como "Agresiones israelíes contra plantas de energía eléctrica en el Líbano y puentes en junio de 1999", "Aviones de guerra israelíes atacan al pueblo de Majdal Selim, mayo de 1999", o "La horrible matanza de Janta, donde fue masacrada una madre con sus seis hijos".
También se ofrecen partes de guerra del grupo armado Resistencia Islámica (Hamas), cuyo tono es similar al siguiente: "Resistencia Islámica destruyó un tanque israelí en Shabaa, el 14 de abril de 2001. Fuentes militares israelíes afirmaron que un soldado murió y otro fue herido en el ataque".

Hamas

Por otra parte, Hamas tiene su propio sitio oficial en Internet (http://www.palestine-info.com/hamas/). Allí se ofrecen comunicados y biografías de los líderes y mártires del movimiento.
En un *link* bajo el título *The Glory Record*, se numeran 85 momentos importantes en la historia de Hamas, la mayoría vinculados con episodios sangrientos. Por ejemplo, el número 2 dice: "El militante de 22 años Ahmed Hussein Abdallah apuñaló al sargento israelí de 27 años David Dan'ely, mientras este hacía guardia frente al kibbutz Metsa'a en el valle de Jordán, el 7 de octubre de 1988. El militante luego murió como un mártir asesinado por otro soldado que acudió a asistir al sargento israelí".
La sección de fotos muestra imágenes de palestinos, especialmente mujeres y niños, entre las ruinas de sus casas demolidas por ataques militares o por bien por topadoras israelíes.
41

Capítulo V: Introducción a la problemática del ciberterrorismo

Antecedentes. Juegos de guerra.

La película *Juegos de guerra* (1983) muestra a un joven e inocente *hacker* (Matthew Broderick) que accede ilegalmente a una computadora gubernamental para jugar a un juego de guerra termonuclear en un *mainframe* diseñado para simular estrategias de ataque y respuesta.
Desde aquella película, estrenada en plena guerra fría, varios expertos en seguridad se comenzaron a preguntar qué posibilidades reales podría haber de que alguien pueda interferir los sistemas computacionales destinados a la defensa.
En 1986, un libro llamado *Softwar* afirmó que los países del Pacto de Varsovia podrían incapacitar al mundo occidental lanzando ataques contra las computadoras militares y financieras de Estados Unidos y la OTAN79.

Tres años más tarde, la Guerra Fría terminó, pero para varios integrantes de organismos de inteligencia estadounidense, el peligro de un ataque electrónico siguió latente. Las hipótesis se ampliaron: ya no se trataba sólo de que algún país enemigo buscara atacar o inutilizar las instalaciones militares, sino que además se comenzó a especular con algún tipo de ataque contra la infraestructura civil de la nación.

La primera acción preventiva importante a nivel oficial fue la creación por parte del gobierno estadounidense de *The Critical Technologies Institute* (1991), esponsoreado por la *National Science Foundation.* Este

[79] Citado en el prólogo del libro *Cybercrime...Cyberterrorism... Cyberwarfare*, documento desarrollado por el Center for Strategic and International Studies (CSIS), noviembre de 1998. Disponible en: www.csis.org

organismo elaboró una serie de recomendaciones divididas en acciones inmediatas, acciones a corto plazo y acciones a mediano plazo. Entre estas últimas figuraba la creación de mecanismos de alerta y de un organismo de coordinación[80].

Cinco años más tarde, el ex Director de Inteligencia Central John Deutch, en su testimonio ante un comité del Congreso, afirmó: "*Hackers* criminales estuvieron vendiendo sus servicios a estados-villanos (*rogue states*)". Y agregó que "están analizando varios esquemas para agredir los intereses vitales de Estados Unidos a través de intrusiones ilegales en computadoras"[81].

Bill Clinton, el primer presidente de la era de Internet

"Ahora que nos aproximamos al siglo XXI, nuestros enemigos han ampliado los campos de batalla del espacio físico al cibernético... En lugar de invadir nuestras playas o enviar bombarderos, estos adversarios pueden intentar ataques cibernéticos contra nuestros sistemas militares esenciales... Si nuestros hijos han de crecer libres, debemos afrontar esas nuevas amenazas con el mismo rigor y determinación que empleamos contra las amenazas a nuestra seguridad más severas de este siglo"

Bill Clinton, 22 de mayo de 1998

Clinton fue el primer presidente estadounidense de la era de Internet. De hecho, fue durante su gestión cuando la "red de redes" se difundió masivamente entre la población y los procedimientos de *hacking* -al igual que la cantidad de *hackers*- se multiplicaron.

Cuando Clinton asumió su primer mandato, un *hacker* era un especialista en informática -por lo general altamente capacitado- que invertía muchísimas horas en investigar y adquirir conocimientos vinculados al acceso a redes de computadoras. Cuando Clinton dejó el gobierno, existían al menos 15.000 sitios de Internet que ofrecían en

forma gratuita manuales, instrucciones y programas para realizar distintos tipos intrusiones y ataques informáticos.
Fue en 1994 cuando, con la aparición del *Netscape Navigator*, la información a través de Internet se hizo más accesible (ya que permitió incorporar imágenes), con lo cual los hackers movieron toda su parafernalia instalada en los viejos BBS (*Bulletin Board Sistems*) a sitios de Internet accesibles a todo el mundo.
[80] Citado en: Scassa, David. *Paper on Cyberterrorism*. 2000 (Documento disponible en www.worldnet.net).
[81] Ibid.
43
Actualmente, casi no se requieren conocimientos previos para realizar algunas acciones elementales de *hacking*. Se trata sólo de seguir una serie de instrucciones paso a paso. La alta vulnerabilidad de los sistemas instalados hace que cualquier adolescente de clase media que dedique el tiempo suficiente pueda estar preparado muy rápidamente para realizar algún tipo de ataque o intrusión exitosa.
Clinton también debió afectar el cambio de siglo y "la falla del milenio" (*the Millenium Bug*). La imposibilidad de la mayoría de las computadoras instaladas para registrar fechas de cuatro dígitos hizo temer la paralización o mal funcionamiento de empresas, servicios básicos y hospitales al ingresar al año 2000. Evitar esos problemas implicó el desarrollo de una serie de políticas, conducidas y financiadas en parte por el gobierno federal (Ver más adelante en este capítulo el subtítulo “La falla del milenio”).

La Comisión Presidencial para la Protección de la infraestructura Crítica

En julio de 1996, un mes después de que John Deutch afirmara ante el Congreso que varios *hackers* estaban vendiendo sus conocimientos a estados-villanos, Clinton anunció la formación de la Comisión Presidencial para la Protección de la Infraestructura Crítica (*The President´s Commision on Critical Infrasructure Protection),* conocida en inglés por la sigla PCCIP. El fin de ese organismo era estudiar las infraestructuras que constituyen el soporte de la vida cotidiana de Estados Unidos, determinar sus vulnerabilidades ante una amplia gama de amenazas, y proponer una estrategia para protegerlas en el futuro.
Ocho tipos de infraestructuras fueron identificadas:
Telecomunicaciones, bancos y finanzas, energía eléctrica, almacenamiento y distribución de gas y petróleo, aprovisionamiento de agua potable, transportes, servicios de emergencia y servicios gubernamentales.

En el informe final, lanzado en octubre de 1997, la mencionada comisión concluyó que las amenazas contra la infraestructura crítica eran reales y que, debido a su mutua dependencia e interconexión, las áreas analizadas eran vulnerables en diferentes aspectos. "La explotación intencional de esas vulnerabilidades podría tener serias consecuencias
44
para nuestra economía, nuestra seguridad y nuestro estilo de vida", se afirma en el informe[82].

Al evaluar la posibilidad de ataques tanto físicos como virtuales, la PCCIP concluyó que "los medios físicos de explotar las vulnerabilidades probablemente siguen siendo la mayor amenaza para nuestra infraestructura hoy en día. Pero casi todos los grupos a los que consultamos hablaron con preocupación de las nuevas amenazas cibernéticas, y enfatizaron la importancia de desarrollar enfoques que nos sirvan para proteger nuestra infraestructura contra las mismas antes de que se materialicen y nos produzcan un daño mayor en los sistemas".

La PCCIP señaló que la posibilidad de un ataque cibernético implicaba un cambio cualitativo en relación a todos los conceptos conocidos de seguridad. "En el pasado hemos estado protegidos de ataques hostiles contras nuestra infraestructura por anchos océanos y vecinos amistosos. Pero en el ciberespacio, las fronteras nacionales ya no son relevantes. Los electrones no se detienen a mostrar sus pasaportes. Ciberataques potencialmente serios podrían ser concebidos y planeados sin una preparación logística detectable. Además, podrían ser ensayados de manera invisible y montados en cuestión de minutos o aún de segundos sin revelar la identidad ni la ubicación del atacante"[83].

En otro apartado, el informe afirma: "Esperar que ocurra un desastre es una estrategia peligrosa. Ahora es el tiempo de proteger nuestro futuro".

La Comisión afirmó que varios operadores calificados de computadoras demostraron su habilidad para ganar acceso a redes sin autorización "Cualquiera sea su motivación, su grado de éxito al ingresar en redes para alterar datos, extraer información financiera propietaria o introducir virus, demuestra que (...) en el futuro, algún grupo interesado en provocar serios daños a los Estados Unidos podría hacerlo utilizando esos mismos medios".[84]

Creación del Centro Nacional de Protección de Infraestructura (NIPC)

En febrero de 1998, como respuesta al mencionado informe de la PCCIP, y teniendo en cuenta también la gran cantidad de intentos de intrusión que recibieron varias instituciones militares, así como el

Departamento de Defensa y numerosas empresas privadas, el Departamento de Justicia y el FBI crearon el Centro Nacional de

82 Citado por Denning, Dorothy E., Op. Cit. El informe de la Comisión fue publicado en el sitio

83 Ibid.

84 *Cybercrime...Cyberterrorism... Cyberwarfare...* Op. Cit..

45

Protección de Infraestructura (*National Infrastructure Protection Center*, NIPC). La dirección de ese organismo, que opera en la sede central del FBI en Washington, fue confiada inicialmente a Michael Vatis (en marzo de 2001 sería reemplazado por Ronald Dick).

El NIPC nació para ser el punto clave de coordinación de las "ciberdefensas" nacionales. Para ello, dicho organismo se encargó de reunir a representantes de agencias gubernamentales, funcionarios de los distintos estados norteamericanos y de los gobiernos municipales, y representantes del sector privado, para "proteger la infraestructura crítica de la nación"[85].

La Decisión Directiva Presidencial 63

En base a las recomendaciones de la PCCIP, Clinton emitió en 1998 la Decisión Directiva Presidencial 63 *(Presidential Decision Directive -PDD-63)* mediante la cual se adoptaron una serie de medidas. Una de las más importantes fue la creación del cargo de Coordinador Nacional de Seguridad, Protección de la Infraestructura y Contraterrorismo (*National Coordinator for Security, Infrastructure Protection, and Counterterrorism).* El primer jefe de este organismo fue Richard Clarke, un miembro del Consejo de Seguridad Nacional de la Casa Blanca (*White House National Security Council*, NSC) desde 1992[86].

Otra medida clave fue la creación de la Oficina de Aseguramiento de la Infraestructura Crítica (*Critical Infrastructure Assurance Office*, CIAO). Este organismo depende del Departamento de Comercio. Jeffrey Hunker[87], otro integrante del *White House National Security Council*, asumió como director. Posteriormente sería reemplazado por John Tritak[88].

Se estableció también la creación del Consejo Nacional de Aseguramiento de la Infraestructura (*National Infrastructure Assurance Council*, NIAC). Ese consejo se constituyó a través de 30 miembros del gobierno federal y de gobiernos estatales y municipales, junto con integrantes del sector privado. Las diferencias con el NIPC no son demasiado claras. El NIAC se encargó, entre otras cuestiones de los Centros de Intercambio y Análisis de Información (*Information Sharing and Analysis Centers*, ISACs) establecidos en todo el país con el objeto de intercambiar datos sobre vulnerabilidades, ciberataques e intrusiones.

85 En el sitio del NIPC (www.nipc.org) se puede encontrar la historia de este organismo e información adicional sobre el mismo.

[86] Biografía y currículum de Richard Clarke: http://www.info-sec.com/ciao/bioclarke.html
[87] Antecedentes de Jefrey Hunker: Ver http://www.info-sec.com/ciao/biohunker.html
[88] Antecedentes de John Tritak: Ver http://www.fiestacrow.com/Tritak.htm
46

Paralelamente, el Departamento de Defensa creó su propia red de seguridad, llamada Fuerza de Tareas Conjunta-Red de Defensa de Computadoras (*Joint Task Force-Computers Network Defense*, JTFCND).

La falla del milenio

En 1998, Clinton comenzó a encarar el problema de "la falla del milenio" (al cual se hizo alusión en este capítulo, en el subtítulo “Bill Clinton, el primer presidente de la era de Internet”). El 14 de julio, en un discurso frente a la Academia Nacional de Ciencias (*National Academy of Sciences)*, Clinton rompió su silencio e hizo el primer reconocimiento público de la preocupación por el tema. Eso motivó algunas críticas por parte de políticos opositores y de algunos empresarios, quienes se cuestionaron si no sería demasiado tarde para enfrentar el problema.

"Le dejé bien en claro a cada miembro de mi gabinete que el pueblo estadounidense tiene el derecho de esperar servicios ininterrumpidos por parte del gobierno, y eso es lo que espero que proporcionen”,[89] afirmó Clinton, quien fijó como límite el mes de marzo de 1999 para que los organismos federales solucionen ese problema.

Al tiempo que advirtió sobre la necesidad de “cerrar la brecha" existente entre los esfuerzos del sector público y el privado en lo referente a la preparación de sus sistemas computacionales para el cambio de siglo, Clinton bosquejó una serie de pasos para hacer que la transición no sea demasiado brusca. Si el *millennium bug* no era sobrellevado como correspondía, dijo Clinton, se podría generar en el 2000 una "oleada de inconvenientes" o aún peor, grandes interrupciones en servicios esenciales tales como energía eléctrica, teléfonos y viajes aéreos.

En 1999, Michael Vatis, jefe del NIPC, advirtió sobre la eventual presencia de “extranjeros infiltrados” entre los técnicos abocados a solucionar la “falla del milenio”. Vatis señaló que esos terroristas potenciales podrían colocar virus troyanos y códigos maliciosos en los sistemas computacionales que habían sido contratados para reparar. La infraestructura de los Estados Unidos, advirtió Vatis, podría estar en riesgo[90].

[89] Anter, Spencer. *Clinton too Late on Y2K?* Wired News, 15 de julio de 1998. Ver artículo en: http://www.wired.com/news/politics/0,1283,13736,00.html
[90] Ginorio, Erik. *Hunting Phantoms*. The Industry Standard Magazine, 31 de julio de 2000. El artículo se puede buscar en www.thestandard.com
47

El plan *Cyber Corps*

Volviendo al tema de la prevención ante un eventual ataque, en enero de 1999, Clinton dio el próximo paso: el lanzamiento del plan *Cyber Corps*. Dicho plan contemplaba iniciativas específicas tales como:
—La creación de redes de detección (*detection networks*). En primer lugar, dichas redes se crearían para el Departamento de Defensa, y luego para otras agencias clave. Su finalidad sería alertar al personal apropiado cuando un sistema computacional crítico ha sido invadido.
—La creación de centros de información en el sector privado de tal manera que las empresas estadounidenses puedan trabajar en forma conjunta con el gobierno para manejar las "ciberamenazas".
—Proporcionar financiamiento a fin mejorar las capacidades de los especialistas en computación del gobierno capaces de prevenir y responder a las crisis sufridas por las computadoras.
Un año más tarde, en enero de 2000, el CIAO lanzó el Plan Nacional para la Protección de los Sistemas de Información (*National Plan for Information Systems Protection*) version 1.0. El objetivo de dicho plan era coordinar el accionar de las distintas agencias para abordar las cuestiones vinculadas con la infraestructura crítica dentro del gobierno federal.
[48]

Capítulo VI: Principales hipótesis y predicciones sobre el ciberterrorismo

Las hipótesis de Barry Collin

Barry Collin, un investigador *senior* del *Institute for Security and Intelligence en California*, quien en los años 80 acuñó el término ciberterrorismo (tal cómo se explicó en el Capítulo I) elaboró años atrás una serie de hipótesis sobre posibles actos ciberterroristas. Esas hipótesis fueron -y todavía son- usadas masivamente por periodistas, políticos y funcionarios de organismos de seguridad, para referirse a la amenaza del ciberterrorismo. Por lo tanto, contribuyeron a formar una determinada idea en el imaginario colectivo estadounidense acerca de las posibles consecuencias de un atentado terrorista informático.
Las hipótesis de Barry Collin son las siguientes:
• Un ciberterrorista podría acceder remotamente a los sistemas de control de procesamiento de una planta elaboradora de cereales, cambiar los niveles de suplementación de hierro, y enfermar (e incluso eventualmente matar) a los niños de Estados Unidos mientras disfrutan de su desayuno. También podría realizar alteraciones similares en plantas de alimentos para bebés. La supuesta ventaja potencial para el ciberterrorista de este tipo de ataque es que no tendría que estar en la fábrica para ejecutar ese tipo de atentado.

• Un ciberterrorista podría interferir a los bancos, las transacciones financieras de dinero y los centros bursátiles. Esa manera, los habitantes del país perderían su confianza en el sistema económico. Dice Collin:

¿Se atrevería un ciberterrorista a intentar ingresar físicamente al edificio de la Reserva Federal, u otro equivalente? Difícilmente, desde el momento en que sería inmediatamente arrestado. Es más, un gran camión estacionado cerca del edificio sería detectado en forma automática. Sin embargo, en el caso de un ciberterrorista, el perpetrador podría estar sentado en otro continente mientras que los sistemas económicos de la nación colapsan, alcanzando una situación de desestabilización[91].

• Un ciberterrorista podría atacar a la próxima generación de sistemas de tráfico aéreo, y hacer que dos grandes aeronaves civiles choquen entre sí. “Ese es un escenario realista, desde el momento en que el ciberterrorista también podría interferir los sensores del interior de la cabina”, dice Collin, y señala que maniobras similares pueden ser realizadas con las líneas de ferrocarriles[92].

• Un ciberterrorista podría alterar las fórmulas de remedios o productos farmacéuticos, causando una gran cantidad de pérdidas humanas.

• Un ciberterrorista podría cambiar remotamente la presión de los gasoductos, causando fallas en las válvulas, y desencadenando una serie de explosiones e incendios. “De la misma manera, la red eléctrica se vuelve cada día más vulnerable”, afirma Collin[93].

En síntesis, el ciberterrorista, según Collin, se asegurará de que la población de un país no pueda comer, beber, viajar ni vivir:

Las personas encargadas de velar por la seguridad de la Nación no estarán advertidas ni podrán anular al ciberterrorista, que probablemente se encontrará en el otro lado del mundo.

Lamentablemente esos ejemplos no son de ciencia-ficción. Todos esos escenarios pueden tener lugar hoy. Como muchos saben, algunos de esos incidentes ya han ocurrido en varias naciones. Muchos de esos actos ocurrirán mañana. [94]

Uno de los principales críticos de Barry Collin es el agente del FBI Mark Pollitt, quien a fines de los 90 escribió un ensayo titulado *Ciberterrorismo: ¿Fantasía o realidad?* (*Cyberterrorism: Fact or Fantasy*?, en el cual analiza las posibilidades reales de ataques ciberterroristas, dejando en claro

que sus opiniones son estrictamente personales y no representan el punto de vista del FBI.

Al analizar la factibilidad de las hipótesis de Collin, Pollitt concluye que actualmente existe el suficiente involucramiento humano en los procesos de

[91] Collin, Barry. *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*. Sin fecha. Artículo disponible en el sitio http://afgen.com/terrorism1.html

[92] Ibid.

[93] Ibid.

[94] Ibid.

control como para que el ciberterrorismo no alcance el riesgo de riesgo que le atribuye Collin.

En el ejemplo de la contaminación de los cereales infantiles, Pollitt señala que la cantidad de hierro (o cualquier otra sustancia nutritiva) que haría falta para enfermar a alguien severamente (suponiendo que eso sea posible) es tan grande que los operarios de la fábrica lo notarían. Se quedarían sin hierro en la línea de producción y el producto además tendría un sabor distinto y nada agradable. Además, los fabricantes de alimentos realizan análisis de rutina destinados a detectar cualquier eventualidad. "Esa es una necesidad comercial en un mundo altamente litigante"[95], señala Pollitt.

En el ejemplo el control de tráfico aéreo, Pollitt sostiene que las personas a cargo notarían los problemas y tomarían acciones correctivas. Los pilotos, dice Pollitt, son entrenados en lo que se denomina *situational awareness*. Desde el primer día de aprendizaje, se les enseña a ser conscientes no sólo se su ubicación, dirección y altitud, sino también de las ubicación de otras aeronaves. Es común que los pilotos descubran errores cometidos por los controladores de tráfico aéreo. Son las fallas humanas las que derivan en colisiones aéreas. La formación básica de los pilotos incluye la hipótesis del colapso de los sistemas de tráfico aéreo, con lo cual los pilotos son entrenados para operar en la ausencia de todo control.

Pollitt no pretende afirmar en su análisis que las computadoras son seguras y libres de vulnerabilidades. Su idea es que, a pesar de esas vulnerabilidades, es casi imposible que un ciberataque pueda tener consecuencias devastadoras. "A medida que incorporamos más y más tecnología en nuestra civilización, debemos asegurarnos de que exista el suficiente control e intervención humana como para salvaguardar a aquellos a quienes la tecnología sirve", [96]dice Pollit.

Hacia un análisis cauteloso

William Church, ex oficial de inteligencia del ejército estadounidense, fundó en 1996 el *Centre for Infrastructural Warfare Studies* (CIWARS) con el objeto de realizar un informe sobre las vulnerabilidades de la infraestructura estadounidense. Ese informe fue financiado por un grupo

privado llamado *The Internet Science Education Project* y fue utilizado como referencia por la *Presidential Commission On Critical Infrastructure Protection* creada por Bill Clinton, a la cual se hizo alusión en el capítulo V (ver subtítulo *La Comisión Presidencial para la Protección de la Infraestructura C*rítica).

Church dirige una empresa de San Francisco que se encarga de monitorear la seguridad electrónica de sus clientes. Sin embargo, contrariamente a lo

[95] Citado por Denning, Dorothy E., Op. Cit.

[96] Ibid.

que se podría esperar en alguien con sus características, las opiniones de Church en relación al ciberterrorismo siempre fueron precavidas.

En una entrevista que concedió a la revista Techweb en 1998, Church efectuó un comentario que con el tiempo, resultó premonitorio. Cuando le preguntaron si grupos como el de Bin Laden podrían utilizar armas cibernéticas o si, por el contrario, el impacto visual de un edificio explotando por el efecto de una bomba seguía siendo prioritario para ese tipo de grupos terroristas, Church dijo: “Efectivamente, acaba de dar en el clavo. Los grupos terroristas con los que lidiamos hoy son altamente proclives al impacto visual”[97].

“No debemos descartar la posibilidad de que algún grupo haga la transición a lo no visual, pero por el momento, la política del impacto visual sigue siendo predominante”, agregó, tres años antes de que los canales de television de todo el mundo mostraran el derrumbe de las Torres Gemelas.

Al ser interrogado acerca de cuáles son sus hipótesis de ataques ciberterroristas, Church señaló: “Un escenario escenario posible sería que un grupo terrorista, sin pretender generar víctimas fatales, quisiera efectuar algún tipo de proclama. Hoy eso se podría materializar”.

Church se mostró partidario de “separar la hipérbole de la realidad”. Señaló que “A pesar de que el gobierno de Estados Unidos ha citado a algunos grupos guerrilleros de Sri Lanka como los responsables de haber usado las primeras armas ciberterroristas, eso carece de sentido. Lo que hicieron fue un ataque por e-mail. Eso es acoso, no es terrorismo”[98].

En la misma entrevista, Church reconoció que “han habido intentos no organizados de interrumpir la infraestructura estadounidense. Y se han concretado algunas interrupciones, ciertamente. Pero nunca hubo grupos organizados que hayan llevado a cabo ese objetivo”. Entre los pocos casos ocurridos, Church recordó el de un *hacker* sueco que desconectó el servicio telefónico 911 –la línea de emergencias- en Florida, Estados Unidos. “Pero aún en ese caso no hay pruebas de que haya tenido intenciones hostiles”,

aclaró.
En otra entrevista concedida a la revista argentina CompuMagazine en febrero de 1998, en relación con la posibilidad de una guerra infraestructural, Church respondió: “La guerra infraestructural consiste en usar una combinación de medios virtuales y físicos de manera de lograr el máximo efecto posible. Pero para esto hace falta una organización y medios de magnitudes militares, y no un puñado de *hackers*, como aseguró hace unos meses el FBI[99]”.

[97] Borland, John. *Analyzing The Threat Of Cyberterrorism*. TechWEb News, 23 de septiembre de 1998.
[98] Ibid.
[99] Aldegani, Gustavo. *Entrevista a William Church.* Revista CompuMagazine No. 115, febrero de 1998.

“Con 10 *hackers* profesionales –agregó- se podría lograr una acción única, como paralizar las comunicaciones durante un par de horas, pero sostener esta acción como requiere una guerra hace que se necesite una organización muy potente que permita que los ataques se continúen de tal manera que lleguen a tumbar la infraestructura de un país”.

¿Un Pearl Harbor electrónico?

Como parte del apoyo retórico que acompañó al pedido de financiamiento para el plan FIDNET, en 1999 Clinton dijo: “Mientras que hasta ahora nuestros enemigos se apoyaron en bombas y balas, terroristas y potencias hostiles podrían transformar a una computadora *laptop* en un arma potente capaz de hacer un gran daño”.[100]

En el mismo contexto, el entonces consejero especial de la Casa Blanca Richard Clarke, señaló: “Hay un gigantesco *tsunami* que está por impactar contra nosotros... será mejor que respondamos antes de que ocurra un Pearl Harbor electrónico”.[101]

La expresión *Pearl Harbor electrónico* fue lo suficientemente impactante como para pasar a formar parte del discurso habitual de la prensa y de la clase política.

Dicha expresión no fue un invento de Clarke:

• En 1993, Paul A. Strassmann, *Chief Information Office* (algo así como *gerente de sistemas*) del Departamento de Defensa durante la administración de George Bush (padre), dijo: "No hay dudas. La única pregunta es cuándo. Pero un Pearl Harbor electrónico ocurrirá”[102].

• En 1996, el vice Fiscal General Jamie Gorelick dijo a un subcomité del Senado: “La posibilidad de un Pearl Harbor electrónico representa un peligro muy real para los Estados Unidos”.[103]

• En 1999, el representante republicano de Pennsylvania Curt Weldon dijo que no era una cuestión de “si ocurriría” sino de “cuándo ocurriría” un Pearl Harbor electrónico[104].

Incluso una vez completada la transición al 2000 y superada la “falla del milenio”, La alusión al Pearl Harbor electrónico siguió siendo moneda corriente.

100 *Government Monitoring*. Computer Law, 13 de septiembre de 1999. Se puede leer el artículo en: http://www.mgrossmanlaw.com/articles/1999/government_monitoring_of_computers.htm

101 Ibid.

102 Citado por Iacobuzio, Theodore. *Ground Zero*. Bank Systems + Technology. Noviembre de 1993.

103 Ibid.

104 Citado por Ginorio, Eric. *Hunting Phantoms.* The Industry Standard, 31 de julio de 2000. El artículo se puede leer en: http://www.thestandard.com/article/display/0,1151,16974,00.html

53

En abril de 2001, ya durante la presidencia de George Bush (h), el republicano Newt Gingrich, presidente de la Cámara de Representantes de Estados Unidos entre 1995-1999, escribió un artículo titulado *La pregunta no es si habrá un ciber Pearl Harbor, sino cuando ocurrirá:*

La seguridad de las aerolíneas estaría seriamente comprometida si las computadoras que manejan el tráfico aéreo fueran dominadas por ciberterroristas (...) Una acción de ese tipo podría causar numerosas víctimas. Pensemos en el caos que se generaría si un grupo terrorista dominara las computadoras del aeropuerto internacional O´Hare (en Chicago) que controlan el congestionado corredor aéreo del medio oeste.

Desde paralizar nuestros sistemas de comunicaciones hasta bloquear nuestro sistema financiero, pasando por la generación de apagones eléctricos, hay una cantidad de grandes de interrupciones que podrían perjudicar nuestra economía, disminuir nuestra calidad de vida y desestabilizar a la Nación (...)

Imaginen un mundo en el cual la Alemania Nazi o la Unión Soviética de Stalin hubieran sido los primeros en desatar el poder destructivo del átomo. Bien, ahora imaginen un mundo en el cual los líderes electos democráticamente tienen menos imaginación y mayor resistencia que sus adversarios tiránicos a apostar por tecnologías aún no fueron testeadas. El resultado podría ser terrible, y posiblemente fatal, para nuestra libertad y nuestro estilo de vida. *105*

La profusión de la expresión *Pearl Harbor electrónico* (se pueden encontrar más de 500 variaciones en Internet a través de los buscadores) motivó la siguiente definición del *Crypt Newsletter*, una publicación virtual sobre seguridad informática:

Electronic Pearl Harbor (EPH): Una trivialidad popularizada

por gente del estilo de Alvin Toffler, ex generales de la guerra fría, charlatanes empresariales surtidos y periodistas, por nombrar a unos pocos. EPH se usa para designar a un nebuloso apocalipsis electrónico que se cierne sobre las computadoras y las redes de Estados Unidos. En el mundo real, es un sinónimo de la frase ´*Watch your wallet!*´ (¡Cuide su billetera!), ya que quienes la usan generalmente lo hacen en un intento de

[105] Gingrich, Newt. *A cyber Pearl Harbor is not a question of if, but when.* Infosecurity Magazine, abril de 2001. (www.infosecuritymag.com)

convencer a los ciudadanos que pagan sus impuestos de financiar proyectos ultrasecretos o mal definidos tendientes a protegerlos"[106].

En algunos casos, las hipótesis del Pearl Harbor electrónico ingresaron al terreno de la ciencia-ficción. Tal fue el caso del libro *Information Warfare: How to survive Cyber Attacks,*[107] de Michael Erbschloe y Jon Vacca. Anton Chuvakin, de la empresa *SecurityWatch Research,* efectuó el siguiente comentario sobre dicho libro:

El capítulo más excitante es la descripción de una *ciberguerra de un trillón de dólares* (*trillion dollar cyberwar*) dirigida contra el mundo y llevada a cabo por una banda de 10 hackers malintencionados. Combinando virus por e-mail, *hacking* y la revelación de información sensible con ataques físicos a compañías teléfónicas y centros de cómputos, el grupo causa un mes entero de problemas, desencadenando una ola de pánico, conflictos armados y otros eventos del tipo del día final.[108]

En el libro, Erbschloe señala al respecto:

Pearl Harbor 2 (PH2) es un escenario de guerra virtual, generada por un grupo de diez personas de distintas partes del mundo. Todos ellos tienen altos conocimientos y habilidades informáticas y se conocieron a través de salas de *chat* en Internet. Todos tienen distintos antecedentes culturales y son gente educada e inteligente.

Un día deciden unirse parea lanzar un ataque terrorista sostenido. Cada uno tiene sus propias razones para participar: algunos por diversión, otros porque están enojados con la gente que los rodea, y otros simplemente por que están alienados[109].

Si bien el episodio descripto es ficticio, el libro no es de ficción, y el episodio que lleva por título *Pearl Harbor 2 (PH2)* tiene el objeto de

pronosticar un escenario factible.

[106] El texto completo se puede leer en el siguiente sitio: http://www.soci.niu.edu/~crypt/other/harbor.htm

[107] En el sitio www.amazon.com se puede encontrar toda la información pertinente a ese libro, de la editorial Osborne/McGraw-Hill.

[108] Chuvakin, Anton. Comentario del libro *Information Warfare: How to Survive Cyber Attacks*, de *Michael* Erbschloe (Ver: http://www.securitywatch.com/lit/network_security/infowar.html)

[109] Ibid.

55

Mitos y realidades sobre los virus informáticos

La utilización de virus informáticos como si fueran armas es una preocupación presente tanto en los organismos de seguridad estadounidenses como entre los funcionarios públicos y periodistas poco informados.

El siguiente extracto del libro *Information Warfare: How to survive Cyber Attacks,* mencionado en el apartado anterior, *es* un claro ejemplo del poder que el imaginario colectivo suele atribuir a los virus de computadoras:

> 9:00 A.M., 3 de diciembre de 2001. Es de mañana en Nueva York. Un virus de computadoras que se transmite por e-mail similar al *Love Bug* comienza a esparcirse por las computadoras de *Wall Street* y de varias empresas de toda la costa Este de Estados Unidos. El virus posee distintas variantes que circulan al mismo tiempo. Todas ellas atacan computadoras que usan el *Microsoft Outlook* como programa de e-mail, y hacen que dicho programa reenvíe el virus a los primeros 50 nombres encontrados en la libreta de direcciones de cada computadora. (...)
>
> En menos de cuatro horas el virus se replica tres mil millones de veces alrededor del mundo. Dentro de 24 horas, el virus se ha replicado 36.000 millones de veces (...) con los correos electrónicos *offline*, las direcciones de e-mail de los servicios de atención al cliente de las principales empresas alrededor de mundo quedan inutilizadas (...) Al ser suspendidas las transacciones *on-line*, quienes practican comercio electrónico acuden al teléfono (...) las líneas telefónicas se ven saturadas y colapsan (....) la gente acude entonces a sus teléfonos celulares con conexión a Internet, pero los agresores han diseminado también virus que circulan entre los teléfonos (...)[110]

Un ejemplo acerca de la desinformación que circula en torno a los virus es ilustrada en un artículo publicado en la edición de diciembre de 1996 del *Law & Enforcement Bulletin* del FBI. El artículo fue escrito por académicos de las universidades estatales de Michigan y Wichita. Luego de una introducción sobre el delito informático y la psicología de los *hackers*,

el artículo presenta a varios virus como ejemplos de herramientas informáticas vandálicas.

[110] Chuvakin, Anton. Op. Cit.

56

"Un virus llamado Clinton -escribieron los autores- fue diseñado para infectar programas (...) pero se erradica a sí mismo cuando no puede decidir qué programa infectar"[111]. Tanto los autores como el FBI vivieron un papelón cuando se enteraron de que no existía un virus llamado Clinton. Había sido una broma, al igual que los demás ejemplos de virus citados en el artículo, todos los cuales habían sido publicados en la columna del *Fool´s Day* (un día en el cual se suelen hacer bromas, como ocurre con el *día de los inocentes* en Argentina) de una revista de computadoras.

El artículo del FBI era una versión condensada de una monografía presentada por los mismos autores en un encuentro de la *Academy of Criminal Justice Sciences* en Las Vegas en 1996. Titulado *Tendencias y experiencias en el delito vinculado a la computación: hallazgos de un estudio nacional* (*Trends and Experiences in Computer-Related Crime: Findings from a National Study*), el informe se refirió a una redada en la cual agentes federales arrestaron a una peligrosa banda de *hackers*. "Los *hackers* ingresaron a una computadora de la NASA responsable de controlar al telescopio *Hubble* y se sabe que también redireccionaron llamadas telefónicas de la Casa Blanca hacia la Universidad Marcel Marceau, un instituto de mímica", escribieron los autores. Esa anécdota también fue parte de una broma hecha con ocasión del *Fool' s Day*[112]. Cuando el FBI decidió hacer las correcciones, ya se había enviado la revista a 55.000 profesionales y analistas políticos, muchos de los cuales deben haber tomado al artículo como verdadero.

En un artículo de la revista *Issues in Science and Technology* publicado en 1998 y firmado por George Smith, se ofrece una clara explicación de por qué los virus no pueden ser utilizados como armas en el contexto de un ataque ciberterrorista de gran envergadura:

Ningún virus ha demostrado tener utilidad como arma, por razones fácilmente comprensibles. Primero, es casi imposible, incluso para el mayor programador de virus, anticipar la complejidad y heterogeneidad de los sistemas que el virus encontrará. Los virus informáticos representan el anatema de las exigencias militares. En la era de las bombas inteligentes, los virus están muy lejos de poder ser considerados como munición de precisión.

Los virus son tan impredecibles que probablemente infecten

tanto a los enemigos como a los amigos o aliados. Dado que los militares alrededor del mundo usan programas antivirus enlatados que se venden en cualquier negocio, no hay forma de

[111] Citado por Smith, George. *An Electronic Pearl Harbor? Not Likely.* Revista *Issues in Science and Technology*, otoño de 1998.

[112] Ibid.

57

que se puedan prevenir de sus propias creaciones. Lo que puede infectar al enemigo, también te puede infectar a ti (...) Además, cualquier grupo que planee un ataque terrorista por medio de virus, debería tener en cuanta la rápida reacción de industria mundial de programas antivirus, la cual, luego de varios años de experiencia, está muy bien preparada para proporcionar rápidos antídotos[113].

En cuanto a la hipótesis de que un grupo de profesionales empleados por alguna organización militar o terrorista pueda alcanzar un éxito mayor que el de un grupo de alienados *hackers* adolescentes, Smith señaló:

Armar ese equipo no sería sencillo. Si bien no es difícil para cualquiera con habilidades básicas en programación escribir un virus malicioso, desarrollar un virus verdaderamente sofisticado requiere un conocimiento íntimo de los sistemas operativos que está diseñado para infectar y que podría llegar a encontrar. Esos hechos reducen considerablemente el área de potenciales profesionales que podrían ser contratados (...) El error humano está siempre presente. Es un desagradable hecho de la vida que todo *software*, sin importar cuán detalladamente haya sido concebido, esconda errores desapercibidos por sus autores. Y los virus no son la excepción. Normalmente contienen errores, a veces tan espectaculares como apenas llegan a funcionar (...)[114]

[113] Ibid.

[114] Ibid.

58

Capítulo VII: La amenaza del ciberterrorismo: ¿una excusa para la invasión gubernamental de la privacidad?

Introducción

En enero de 2000, un alto directivo del FBI no identificado, citado por la revista *Wired*, afirmó: “El suministro de energía eléctrica en Estados Unidos es vulnerable a los hackers” [115]. Un alto ejecutivo del *North American Electric Reliability Council* (asociación conformada por las

empresas generadoras de energía eléctrica) desmintió la afirmación del FBI y dijo a la revista *Wired* que no tenía noticias de que ningún mecanismo de control energético estuviera conectado a módems ni a líneas telefónicas[116].
El debate tuvo lugar en momentos en que el *Electronic Privacy Information Center* (EPIC), una organización civil dedicada a resguardar la protección de la privacidad de los ciudadanos, denunció públicamente que la iniciativa FIDNET elaborada por la administración de Clinton (ver el capítulo V) tenía como objetivo encubierto vigilar irrestrictamente a los ciudadanos.
Ese es solo un ejemplo de cómo, en momentos en que la sociedad estadounidense debate temas vinculados con la privacidad, florecen declaraciones poco serias por parte de los funcionarios de los organismos de seguridad acerca de los eventuales alcances de que podría tener un acto ciberterrorista.
Por tal motivo, y para contextualizar el marco en el que se produjeron varias de las predicciones apocalípticas al estilo de "Pearl Harbor electrónico", a continuación se explicarán los ejes claves de la puja mantenida entre los organismos de seguridad y las organizaciones civiles de defensa de la privacidad, en torno a las comunicaciones electrónicas.

El *chip clipper*

El primer gran conflicto en torno a la privacidad en la era de las telecomunicaciones tuvo lugar en los años '80. El eje fue el *chip Clipper*, un pequeño artefacto criptográfico destinado a proteger las comunicaciones privadas pero dejando abierta la posibilidad de que agentes

[115] McCullagh, Declan. *Cyber Safe of Gov´t Surveillance?* Revista Wired, 1 de febrero de 2000.
[116] Ibid.
59

gubernamentales obtengan las "llaves electrónicas" necesarias para descifrar las comunicaciones tras obtener una autorización legal.
En 1984, el presidente Ronald Reagan decretó la controversial Decisión Directiva de Seguridad Nacional 145 (*National Security Decision Directive 145*). La misma le otorgó a la agencia secreta NSA el control sobre todos los sistemas de computación gubernamentales que contengan información "sensible pero desclasificada". Eso fue seguido por una segunda iniciativa promulgada por el consejero de la NSA John Poindexter, que extendió la autoridad de la NSA a los sistemas computacionales no gubernamentales.
A manera de respuesta, en 1987, el congreso estadounidense aprobó el Acta de Seguridad Computacional *(Computer Security Act)* con el fin de limitar el rol de la NSA en el desarrollo de estándares para las comunicaciones civiles. La *Computer Security Act* reafirmó el hecho de que el Instituto Nacional de Estándares y Tecnología (*National Institute for*

Standards and Technology, NIST) era el responsable de la seguridad de los sistemas computacionales que contengan información desclasificada que no sea de origen militar o gubernamental. La NSA quedó limitada a proporcionar asistencia técnica en el área civil. El Congreso consideró que no era apropiado que un organismo de inteligencia militar tuviera control sobre la diseminación de información desclasificada. Desde entonces, la NSA buscó la forma de socavar la autoridad del NIST.

En 1989, la NSA firmó un "Memorándum de entendimiento" (*Memorandum of Understanding*, MOU) que propuso transferir de vuelta a la NSA la autoridad cedida al NIST. El MOU sugirió también la creación de un grupo de trabajo conjunto para el desarrollo del controversial *chip Clipper*. Dicho chip estaba destinado a la encriptación de llamadas telefónicas. Dos "agentes de custodia" (*escrow agents*) gubernamentales conservarían las "llaves" necesarias para que el gobierno pueda descifrar los mensajes de aquellos ciudadanos bajo vigilancia del FBI u otro organismo de seguridad.

La propuesta era utilizar el *chip Clipper* para las transmisiones de voz, y un artefacto similar, llamado *Capstone*.

En 1993, el presidente Bill Clinton anunció públicamente la iniciativa del *chip Clipper*. "Durante demasiado tiempo, no hubo prácticamente diálogo entre nuestro sector privado y los organismos de seguridad para resolver la tensión entre la vitalidad económica y los verdaderos desafíos que implica la protección de los ciudadanos estadounidenses", se explicó en el comunicado de prensa del lanzamiento. "En vez de usar a la tecnología para conciliar los intereses a veces contrapuestos del crecimiento económico, la privacidad y la seguridad, las políticas previas han

60

enfrentado al gobierno con la industria y a los derechos a la privacidad con los organismos de inteligencia". [117]

Para conciliar los intereses mencionados, la iniciativa del *chip Clipper* fue lanzada como obligatoria para los organismos gubernamentales, pero optativa para las empresas y organismos civiles.

El gobierno creyó que al definir esa tecnología como estándar gubernamental, los empresarios y los consumidores también la aceptarían y la utilizarían, a pesar de la posibilidad existente de que el gobierno, autorización legal de por medio, pudiera interceptar las comunicaciones. En otras palabras, el éxito de la propuesta del *Chip Clipper* se basaba en la aparente falta de disponibilidad de *softwares* criptográficos potentes en el momento del lanzamiento de la iniciativa.

Sin embargo, ya en 1993 existían programas de encripción importantes

distribuidos a través de Internet y disponibles fuera de los Estados Unidos. Tal era el caso del PGP, desarrollado por Phil Zimmerman

Phil Zimmerman y el PGP

El programa de encripción *Pretty Good Privacy*, desarrollado por Phil Zimmerman, estuvo en el centro de uno de los mayores debates que se realizaron en los últimos años en Estados Unidos en torno a la privacidad electrónica.

Zimmerman estudiaba ciencias de la computación en la *Florida Atlantic University* cuando descubrió la potencial utilidad de las computadoras para crear métodos de encripción. La base seguía siendo la misma: modificar los mensajes de tal forma que nadie, salvo el destinatario, pudiera descifrarlos. Pero las computadoras hacían posible implementar sistemas mucho más dificultosos de descrifrar que cualquier código que una persona pudiera inventar por su cuenta.

En 1976, dos investigadores de la *Stanford University*, Whitfield Diffie y Martin Hellman publicaron un ensayo sobre un nuevo tipo de criptografía, diferente a todo lo existente, llamado *New Directions in Cryptography.* En el mismo explicaron los fundamentos de la denominada criptografía de clave pública[118].

[117] El texto completo del anuncio presidencial se puede leer en: http://www.epic.org/crypto/clipper/white_house_statement_4_93.html

[118] Hasta mediados de los años ´70, los sistemas de encripción se basaban en la existencia de una clave secreta, conocida sólo por el emisor y el receptor del mensaje. Si las dos partes (conocidas en la convención criptográfica como Alice y Bob) estaban separadas geográficamente , era necesario efectuar algún arreglo previo (por ejemplo, enviar a una persona con la clave a encontrarse con la otra) para transmitir datos en forma segura. Para las comunicaciones a través de redes de acceso público, como Internet, ese sistema resultaba demasiado poco práctico.
En el modelo criptográfico de clave pública, denominado modelo Diffie-Hellman, cada uno de los usuarios tiene una clave pública (que no es secreta y puede ser difundida sin problemas) y una clave privada (que sí es secreta). De esa manera, Alice le manda un mensaje a Bob encriptándolo con la clave

Al leer esos escritos, Zimmerman se sintió inspirado: su sueño era encontrar un método de codificación a través de computadoras que pudiera ser utilizado por cualquier persona.

El primer problema que Zimmerman tuvo que sortear fue que las computadoras personales disponibles por esa época eran demasiado precarias. El algoritmo RSA (utilizado para el sistema de clave pública) requería una enorme cantidad de cálculos matemáticos con números de hasta 300 dígitos. Recién en 1986 Zimmerman pudo programar en lenguaje C el software necesario para ese tipo de operaciones.

Posteriormente, decidió alejarse del tema debido a que, como el algoritmo RSA estaba patentado, los programas que el escribiera no podrían ser vendidos.

En 1991, el gobierno estadounidense presentó el proyecto de Ley del Senado 266, una medida antiterrorista que contenía una cláusula según la cual se establecerían severas limitaciones a las comunicaciones y la encripción de archivos a través de sistemas que carecieran de una "puerta trasera" (*back door*) que pudiera ser abierta por el Gobierno. Una medida de ese tipo haría ilegales a los programas de encripción desarrollados por particulares.

La ley fue modificada luego de un fuerte *lobby* por parte de distintos organismos defensores de los derechos civiles. Sin embargo, ante la posibilidad de que el acceso a la encripción sea declarado ilegal, Zimmerman lanzó la primera versión de su programa de PGP y se la dio a un amigo, el cual la subió a una gran cantidad de carteleras electrónicas (BBS).

Rápidamente se difundieron copias por todo el mundo, aún a pesar de que por aquella época eran relativamente pocos los individuos que tenían acceso a los BBS fuera del área académica o gubernamental.

En febrero de 1993, Zimmerman fue informado de que el Departamento de Justicia Estadounidense lo estaba investigando para determinar si había exportado ilegalmente sistemas criptográficos que figuraban en la categoría de "municiones" en el *International Traffic in Arms Regulations* (ITAR), un tratado internacional para la regulación de ventas de armamentos. Tres años más tarde las investigaciones finalizaron y se declaró a Zimmerman libre de cargos.

Durante ese tiempo, el PGP se transformó en un estándar. Su reputación creció a medida que varios criptoanalistas intentaron quebrar la codificación y fallaron. En varios países se formaron equipos de programadores con el fin de mejorar el programa. De esa manera, la

pública de Bob, quien lo puede descifrar utilizando su clave privada. A su vez, Bob le contesta a Alice encriptando el mensaje con la clave pública de ella. La única persona capaz de descifrarlo es Alice, utilizando su clave privada. Para mayor información, hacer una búsqueda con las palabras clave "public key" en el sitio del diccionario virtual de seguridad informática What Is? (www.whatis.com)

62

cuestión legal vinculada a la exportación caducó; si un ciudadano británico bajaba una copia de la versión británica del programa de un BBS de Londres, no estaba en absoluto alcanzado por el ITAR.

Los asuntos legales vinculados con el patentamiento del algoritmo RSA[119] finalizaron en 1993 cuando Zimmerman hizo un trato con una compañía de Arizona llamada Lemcom, la cual había obtenido una licencia de RSA para ver *software* basado en ese algoritmo. Mediante el contrato, Lemcom obtuvo los derechos para vender una versión comercial del PGP, llamada *Viacrypt*, mientras que Zimmerman obtuvo los derechos legales para

distribuir la versión gratuita.
Zimmerman se transformó en una especie de héroe para los fanáticos de las computadoras y para los activistas de los derechos civiles. Su caso generó una gran polémica que alcanzó estado público en todo Estados Unidos.
A lo largo de 1994, en un solo servidor de acceso público del MIT se bajaron entre 500 y 1000 copias diarias del PGP.

La privacidad en la era de Internet

Los debates en torno a los límites a la invasión gubernamental de la privacidad en relación con las computadoras se acentuaron durante el gobierno de Bill Clinton (1993-2001), debido en parte a tres grandes hechos, ya analizados en el capítulo V:
a) La penetración masiva de Internet
b) La *democratización* del hacking, tema analizado en el capítulo V.
c) La llamada *falla del milenio*.
A mediados de 1999, a través de un proyecto de ley titulado Acta de Seguridad Electrónica del Ciberespacio (*Cyberspace Electronic Security Act*, CESA), el Departamento de Justicia propuso modificar la legislación de tal manera de que, bajo ciertas circunstancias, se "postergue" por 30 días el aviso de notificación a los sospechosos cuyos hogares o lugares de trabajo van a ser allanados. La idea diseñada por la administración de Clinton era permitir que agentes federales ingresen de incógnito en las viviendas de los sospechosos para revisar sus computadoras, descifrar sus códigos de encripción y colocar "puertas traseras" para monitorear el flujo de información.
"La imagen de un helicóptero negro aterrizando en el patio de tu casa del cual desembarca un grupo de comandos decididos a obtener tus llaves de

[119] Para más detalles, ver: Grossman, Wendy. *Net.Wars.* Capítulo 4. NUY Press, 1998

PGP ya no pertenece a quienes viven enunciando paranoicas teorías conspirativas", dijo Declan McCullagh, columnista de la revista *Wired*[120].
En una carta de siete páginas enviada al Congreso, la fiscal general Janet Reno y el vicesecretario de Defensa John Hamre, escribieron: "Cuando traficantes de drogas y terroristas usan la encripción para esconder sus comunicaciones, las fuerzas de la ley deben ser capaces de responder de una manera que no entorpezca una investigación ni alerte a los sospechosos". En la misma carta, hablan sobre la necesidad de que los agentes federales puedan "buscar las claves" sin notificar inmediatamente al sujeto. Según la legislación estadounidense, los allanamientos en busca de material comprometedor (con la excepción de las "pinchaduras"

telefónicas) exigen que la policía notifique a la persona que se ingresará a su propiedad.

La propuesta desató una serie de protestas por parte de distintas organizaciones. “El proyecto es peligroso. Si se implementara, sería difícil demostrar que los datos utilizados como evidencia no han sido colocados en las computadoras por los mismos agentes federales. Están proponiendo alterar archivos de computación. Eso es muy serio”[121], dijo Barry Steindardt, director asociado de la *American Civil Liberties Union*.

Dave Banisar, del *Electronic Privacy Information Center* (EPIC), señaló: “Lo que están diciendo es que quieren eliminar la Cuarta Enmienda, o modificarla a tal punto que pierda su espíritu”[122].

Finalmente, la iniciativa fue desestimada.

El proyecto FIDNET

Como se dijo en el capítulo V, en 1999 la *Critical Infrastructure Assurance Office*, (CIAO) lanzó el *National Plan for Information Systems Protection*. El 28 de julio de ese mismo año, el *New York Times*[123] reveló el esbozo de un plan sujeto a la aprobación de Clinton, que se lanzaría en octubre, con el nombre de FIDNET, acrónimo de *Federal Intrusion Detection Network* (Red Federal de Detección de Intrusiones).

Dicho plan comprendía un sofisticado sistema centralizado de control de redes informáticas, públicas y privadas, para proteger la seguridad nacional de posibles ataques ciberterroristas. Incluía también el rastreo de transacciones bancarias, telecomunicaciones y otros sectores neurálgicos.

El *software* del sistema estaba diseñado para que los agentes gubernamentales pudieran rastrear el flujo de información que entra y sale de las redes públicas -con excepción de las militares- y de los ordenadores

120 McCullagh, Declan. *Clinton Favors Computer Snooping.* Wired Magazine, 19 de enero de 2000.

121 Ibid.

122 Ibid.

123 Citado en: Towsend, Rosa. *EE.UU. prepara un sistema de control de redes informáticas.* Diario *El país* (España), 29 de julio de 2000.

de corporaciones y redes de centros de negocios. Entre otros objetivos, pretendía evitar atentados contra las redes eléctricas, de comunicaciones, agua y transporte. Los controladores tendrían también acceso, teóricamente, al correo electrónico y documentos informáticos[124].

Los grupos de defensa de los derechos civiles inmediatamente consideraron que la iniciativa FIDNET podría ser el principio de un estado policial de dimensiones desconocidas. La intromisión del Gobierno en aras de la seguridad nacional se prestaba a abusos, opinó en aquel momento James Dempsey, abogado del Centro para la Tecnología y la Democracia[125]. Esta y otras organizaciones no gubernamentales, como la

Unión de Libertades Civiles, comenzaron a presionar a la Casa Blanca y al Congreso para que el plan sea dejado de lado o se definan claramente sus límites.

Citando a un memorámdum del Departamento de Justicia obtenido a través del Acta de Libertad de Información (*Freedom of Information Act, FOIA),* durante una audiencia en el Congreso, Marc Rotemberg, director ejecutivo del EPIC, explicó que el mismo Departamento de Justicia tenía ciertas dudas acerca de si el monitoreo de redes de FIDNET constituía *wiretapping* (escucha ilegal).

John Tritak, director de la CIAO, se defendió argumentando que el *wiretapping* tenía que ver con las comunicaciones de voz, a las cuales la Casa Blanca no pretendía monitorear. "El plan FIDNET fue designado para identificar tráfico de correo electrónico que pueda contener códigos maliciosos", dijo. En otro comunicado, el Consejero General del EPIC, David Sobel, afirmó: "Existe un peligro real de que se esté desarrollando una mentalidad de guerra fría dentro del gobierno federal en lo que se refiere a las amenazas percibidas en Internet y en la tecnología de comunicaciones en general[126]". Y agregó: "Esas propuestas representan una amenaza mucho mayor a

nuestras libertades de la que podría representar cualquier eventual ataque contra nuestra infraestructura". Posteriormente, la iniciativa de FIDNET fue abandonada.

El *Carnivore*

En julio de 2000 se informó públicamente sobre la existencia de un sistema de monitoreo de comunicaciones a través de Internet del FBI llamado *Carnivore.*

Según el FBI, el *Carnivore* es "un sistema basado en computadoras destinado a permitir, en cooperación con los proveedores de acceso a

[124] Ibid.

[125] Ibid.

[126] Grossman, Mark. *Gauging the Trhreath of Cyberterrorism*. Legal Times, 20 de septiembre de 1999.

65

Internet, que se cumplan las órdenes judiciales vinculadas con la recolección de datos y de cierta información sobre un usuario específico objeto de la investigación"[127].

Según el FBI, el *Carnivore* filtra el tráfico de información y envía a los investigadores sólo aquellos paquetes de datos que ellos están legalmente utilizados a obtener.

Ante las acusaciones de que ese método de control era equivalente al *wiretapping,* el FBI negó que ambos sistemas pudieran ser comparables. Según fuentes oficiales, el *Carnivore* se parece más a los sistemas

conocidos como *pen-registers* y *trap-and-trace*. El *pen-register* es un artefacto que se coloca en las líneas para registrar todos los números telefónicos a los que llama el sujeto de la investigación, así como la duración de la llamada y otros datos. El *trap-and-trace* registra todos los números telefónicos desde los cuales se llama al sujeto investigado.
Esos dos métodos, que proveen información limitada, son considerados menos intrusivos que la escucha telefónica, por lo cual los requisitos legales necesarios para obtener una orden judicial son significativamente menores.
El *Carnivore*, según el FBI, se asemeja más a estos dos sistemas , ya que lo que hace es obtener una copia de todos los e-mails "dirigidos hacia" o "enviados desde" una cuenta específica.
De esa manera, el *Carnivore* no hace un monitoreo amplio, sino más bien quirúrgico. Sólo revisa los casilleros del e-mail "De" y "Para", y siempre en relación a un sujeto específico.
La autorización judicial exige los siguientes datos:
• Nombre del sospechoso.
• Delito por el que se lo investiga.
• Datos sobre su cuenta (e-mail exacto).
Las autorizaciones son concedidas por un plazo de un mes, o a lo sumo dos.
Apenas se reveló la existencia del *Carnivore* en julio de 2000, el EPIC realizó un pedido de información invocando la *Freedom of Information Act*. En la solicitud se le pidió al FBI que libere públicamente toda la información concerniente al *Carnivore*, incluyendo su código fuente y otros detalles técnicos que permitan analizar sus implicancias sobre las cuestiones vinculadas con la privacidad.
Posteriormente, el EPIC le pidió al Departamento de Justicia que acelere el proceso.
Durante una audiencia mantenida el 2 de agosto de 2000, el juez de distrito James Robertson ordenó al FBI que se reporte en la corte el 16 de ese mes y que identifique el material a liberar y el cronograma en el cual se

[127] Graham, Robert. *Carnivore FAQ*. Ver www.robertgraham.com/pubs/carnivore-faq.html

haría su difusión. Fue así como el FBI identificó 3.000 páginas de material, pero se negó a comprometer su apertura en una fecha determinada.
En enero de 2001, el FBI completó el pedido del EPIC, revisó sus datos anteriores, y concluyó que en realidad tenía 1.756 páginas de material vinculado al tema. 1.502 fueron reveladas parcialmente y 254 se mantuvieron sin revelar.

El EPIC insistió en que eso no era suficiente. El 25 de marzo de 2002, la corte ordenó al FBI que inicie una nueva búsqueda de documentos para revelar. Esa nueva búsqueda fue dirigida por el *General Counsel and Congressional & Public Affairs*, y su plazo máximo de finalización fue fijado para el 24 de mayo de 2002[128].

Echelon

En enero de 1998, un detallado informe del Parlamento Europeo reveló la existencia de una red masiva de espionaje tecnológico manejada por Estados Unidos. Según se comprobó, esa red llevaba a cabo rutinariamente el monitoreo de comunicaciones telefónicas, faxes y e-mails de ciudadanos de todo el mundo, pero particularmente de la Unión Europea y de Japón. El informe, titulado *An Appraisal of Technologies of Political Control*[129] (Una evaluación de las tecnologías de control político), estuvo a cargo del *Scientific and Technological Options Assessment (STOA) committee* del Parlamento Europeo. Su revelación causó una fuerte conmoción en la prensa europea.

El *New York Times* también se hizo eco. “Partiendo de diversas fuentes, como universidades, organismos de inteligencia y organizaciones no gubernamentales, el estudio ofrece una descripción y evaluación de una serie de tecnologías de control político (...) que incluyen sistemas de vigilancia electrónica, recolección de datos y artefactos destinados al procesamiento y filtrado de información”, señaló un artículo del mencionado periódico estadounidense[130]. Según la misma fuente, los autores del informe identificaron una tendencia hacia “la militarización de la policía y la paramilitarización de la fuerza militar en Europa, lo que significa que la tecnología usada por la policía y el Ejército converge y amenaza con tornarse casi indistinguible”.

[128] El EPIC mantiene una página en Internet donde se actualiza permanentemente la información del caso: http://www.epic.org/privacy/carnivore/default.html

[129] Se puede leer el informe completo en: http://cryptome.org/stoa-atpc.htm

[130] Giussani, Bruno. *European Study Paints a Chilling Portrait of Technology's Uses*. The New York Times, 24 de febrero de 1998. Artículo disponible en: http://www.nytimes.com/library/cyber/euro/022498euro.html

67

El *New York Times* reveló que el sistema estadounidense de espionaje electrónico es dirigido por la NSA y lleva el nombre clave de Echelon. Echelon consiste en una vasta red de estaciones de espionaje electrónica localizada alrededor del mundo en la cual participan cinco países: Estados Unidos, Inglaterra, Canadá, Australia y Nueva Zelanda. Esos países, agrupados bajo un acuerdo secreto llamado UKUSA, espían a los ciudadanos interceptando diariamente las comunicaciones electrónicas. Las computadoras de la NSA se encargan luego de revisar esa

información, buscando determinadas palabras clave, a través de los denominados “diccionarios Echelon”.
La columna vertebral de Echelon se asienta sobre los satélites Intelsat e Inmarsat, los cuales son responsables de la gran mayoría de las comunicaciones telefónicas entre los países y los continentes. Los 20 satélites de Intelsat siguen una órbita geoestacionaria, fijada sobre distintos puntos definidos del Ecuador. Esos satélites transportan primariamente tráfico civil, pero también transmiten algunas comunicaciones diplomáticas y gubernamentales, de particular interés para los países que integran el UKUSA.
Los satélites ajenos a Intelsat son monitoreados desde distintas estaciones. La estación de Shoal Bay, en Australia, intercepta a una serie de satélites de Indonesia., y la estación de Leitrim, en Canadá, intercepta las comunicaciones de satélites latinoamericanos, incluyendo el de la compañía telefónica mexicana Morelos.
Desde el primer momento, Estados Unidos negó sistemáticamente la existencia de Echelon. Sin embargo, un informe lanzado a principios de 2001 por el *Temporary Committee on the Echelon Interception System* (Comité Temporario sobre el Sistema de Intercepción Echelon) luego de siete meses de investigaciones, concluyó que Echelon “Sí existe, a pesar de las negativas oficiales de los Estados Unidos”[131].
El informe recomendó la “autoprotección” a los ciudadanos y las compañías europeas, e intimó a la Comisión Europea y a sus estados miembros a “diseñar medidas apropiadas para promover, desarrollar y fabricar *softwares* de encripción europeos”, y sobre todo, a “apoyar proyectos vinculados con *software* de encripción de código abierto y simple de utilizar”. Asimismo, sugirió que todos los organismos e instituciones europeas “encripten sistemáticamente sus e-mails”.
El informe investigó varias acusaciones según las cuales las agencias de inteligencia estadounidenses habrían interceptado secretos comerciales europeos con el fin de otorgar una ventaja competitiva a las empresas norteamericanas, pero concluyó que “no se ha encontrado evidencia sustancial al respecto”.

[131] Ver el boletín del EPIC del 30 de mayo de 2001: http://www.epic.org/alert/EPIC_Alert_8.10.html
68

La privacidad después de los atentados del 11 de septiembre

Los atentados del 11 de septiembre de 2001 produjeron una suerte de “derechización de la opinión pública norteamericana”, en palabras del especialista en relaciones internacionales Carlos Escudé[132], que fue aprovechada por el gobierno de derecha de Bush. Fue así como se inició

una fuerte ofensiva tendiente a permitir que las investigaciones gubernamentales vinculadas al terrorismo puedan omitir algunos derechos civiles. Aquí nos centraremos en lo concerniente a la privacidad electrónica, pese a que la mencionada ofensiva fue mucho más abarcativa.
Poco después de los atentados, el fiscal general de los Estados Unidos, John Ashcroft, declaró que él, unilateralmente y sin informarlo a la prensa, había instituido el espionaje de las comunicaciones entre abogado y cliente para los sospechosos sin ciudadanía estadounidense dentro del territorio norteamericano. “De un plumazo violó las enmiendas cuarta y sexta de la Constitución, que prohiben efectuar registros y apropiaciones irrazonables (en este caso de información), y garantizan el derecho a la representación por un abogado”, señaló Escudé[133].
El 13 de septiembre de 2001, dos días después de los atentados, el Senado de ese país aprobó la *Ley para combatir el terrorismo del 200*1, que amplió los poderes de la policía para intervenir las comunicaciones y aumentó el rango de situaciones en las que puede supervisarlas.
El proyecto, presentado por Orrin Hatch (Partido Republicano, Utah) y Dianne Feinstein (Partido Demócrata, California), estableció que cualquier fiscal federal o de alguno de los estados puede disponer la instalación del sistema de vigilancia *Carnivore* del FBI.
"Es imprescindible ofrecer a los organismos de seguridad todas las herramientas posibles que permitan buscar y llevar ante la justicia a los individuos que han producido una masacre de semejante magnitud en nuestra misma casa", dijo Hatch durante el transcurso del debate[134].
Según la nueva ley contra el terrorismo, los fiscales pueden autorizar períodos de vigilancia de 48 horas de duración como máximo sin orden judicial alguna. La vigilancia se limitó en principio a las direcciones de los sitios *web* que se visitan y los nombres y la dirección de correo electrónico de los usuarios. No abarca el contenido de las comunicaciones.

[132] Escudé, Carlos. *Un lugar peligroso*. Página/12, 12 de septiembre de 2001. Se puede leer el artículo en el Sitio no oficial de Carlos Escudé: http://www.geocities.com/smasana/torres1.htm

[133] Escudé, Carlos. *La crisis de los derechos cívicos en los Estados Unidos*. Diario BAE, marzo de 2002. Se puede leer el artículo en la Página no oficial de Carlos Escudé: http://www.geocities.com/smasana/bae11.htm

[134] McCullan, Declan. *Aprueban ley que permite al FBI realizar espionaje en Internet*. Revista Wired en español, 17 de septiembre de 2001. Se puede ver el artículo completo en: http://wired.terra.com.ar/wired/politica/01/09/17/pol_3.html

69

Entre las situaciones que no exigen una orden judicial se mencionan las siguientes: "Amenaza inmediata contra la seguridad nacional de Estados Unidos, amenaza inmediata contra la salud o la seguridad pública, o ataques contra la integridad o el funcionamiento de sistemas de

computación protegidos"[135]. Quedan incluidas, pues, la mayor parte de las actividades de *hacking.*

Durante el transcurso del debate previo a la aprobación de la ley, Patrick Leahy (Partido Demócrata, Vermont), presidente de la Comisión de Asuntos Jurídicos del Senado, insinuó que el proyecto iba mucho más allá de combatir el terrorismo y podía afectar la privacidad de los ciudadanos. También denunció que sólo había tenido oportunidad de leer el proyecto 30 minutos antes de que se iniciara la sesión.

"Tal vez el Senado quiera seguir adelante y adoptar medidas que permitan intervenir las comunicaciones de los ciudadanos", dijo Leahy. "Tal vez quieran contar con herramientas para ingresar en las computadoras privadas. Y tal vez esto nos haga sentir más seguros. Puede ser. Pero también es posible que esto mismo sea un ejemplo de la falta de seguridad que han logrado implantar los terroristas en nuestra sociedad. Es posible que hayan conseguido ampliar el alcance del Gran Hermano en nuestro país".[136]

Dos días más tarde, el presidente Bush envió al congreso un borrador de un proyecto con la intención de ir aún más lejos. Entre otras cosas, se proponía expandir los alcances de *la Foreign Intelligence Surveillance Act* para extender la duración de la vigilancia electrónica y permitir un intercambio mayor de información con los gobiernos extranjeros amistosos. "Nos gustaría cambiar la ley de tal forma que una aprobación para escucha telefónica pueda ser obtenida para todas las jurisdicciones que trabajan en una investigación, dada la particular movilidad de los individuos y su capacidad de comunicación", dijo el fiscal general John Ashcroft[137].

La ley antiterrorista sancionada el 26 de octubre de 2001 con el nombre de *USA Patriot Act* amalgamó las potestades del FBI y la CIA, eliminando la separación entre el espionaje en el extranjero y el interior del país, vigente desde larga data en los Estados Unidos. La legalidad del espionaje electrónico quedó limitada sólo por condiciones que, por tan ambiguas, son fáciles de ignorar.

Dicha ley expirará en diciembre de 2005 a menos que el Congreso decida prorrogarla. Sin embargo, la revista *Wired* denunció que "sólo una pequeña parte de la *USA Patriot Act* expirará en el 2005. Algunas secciones permanentes permiten a la policía llevar a cabo vigilancias sobre las

[135] Ibid.

[136] Ibid.

[137] McCullan, Declan. *Bush Bill Rewrites Spy Laws.* Wired Magazine, 19 de septiembre de 2001. Se puede leer el artículo completo (en inglés) en: http://www.wired.com/news/politics/0,1283,46953,00.html

comunicaciones de Internet sin autorización judicial en determinadas

circunstancias; también permite revisar en secreto hogares y oficinas sin notificar al propietario, y compartir información judicial confidencial con la CIA".

Un comunicado de la organización no gubernamental *Electronic Frontier Foundation*, señaló que "las libertades civiles del pueblo estadounidense sufrieron un fuerte golpe con esta ley, especialmente en lo referido al derecho a la privacidad de nuestras actividades y comunicaciones *online*. No hay evidencia alguna de que las libertades civiles hasta ahora hayan obstaculizado la investigación o el juzgamiento de grupos terroristas".[138]

Posteriormente, por orden del poder ejecutivo se creó la Oficina de Seguridad de la Patria (*Office of Homeland Security, OHS*) que no está sujeta a la supervisión del Congreso y donde el nombramiento del personal es prerrogativa exclusiva del Poder Ejecutivo. "La misma palabra *homeland* es exótica en el léxico cívico y político norteamericano, y sus matices semánticos están más asociados a las dictaduras europeas que a la democracia liberal del Contrato Social", señaló Carlos Escudé[139].

El EPIC solicitó un pedido de información sobre la *Office of Homeland Security* apelando al Acta de Libertad de Información. Sin embargo, en una respuesta enviada a la Corte de Distrito en Washington, el Departamento de Justicia argumentó que la *Office of Homeland Security* no es una "agencia" y por lo tanto no está sujeta al Acta de Libertad de Información. El escrito afirmó que las funciones de la OHS son "solamente aconsejar y asistir al Presidente, y no ejerce ninguna autoridad sustancial independiente". Así , buscó equiparar a la OHS con el *National Security Council*, el cual en 1996 fue exempto de cumplir con las obligaciones de información que establece el Acta de Libertad de Información. [140]

[138] Electronic Frontier Foundation. *EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities. 31 de octubre de 2001. Ver:* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html

[139] Escudé, Carlos. *La crisis de los derechos cívicos en los Estados Unidos*. Diario BAE, marzo de 2002.

[140] Se puede obtener información actualizada sobre las gestiones del EPIC en relación con la *Office of Homeland Security* en el sitio: http://www.epic.org/open_gov/homeland/

71

Capítulo VIII: La prevención del ciberterrorismo, un negocio millonario

Una razón para tomar con cierto escepticismo las reiteradas advertencias sobre posibles ataques ciberterroristas difundidas durante los últimos años es que quienes se muestran más alarmados son muchas veces aquellos que más se benefician con los millonarios gastos gubernamentales destinados a prevenir esa amenaza.

En 1997, un informe del *Defense Science Board* recomendó la inmediata inversión de 580 millones de dólares en el sector privado para la investigación y desarrollo del *hardware* y *software* necesario para lidiar con el ciberterrorismo. Uno de los principales autores de ese

informe fue Duane Andrews, vicepresidente ejecutivo de SAIC, una empresa proveedora de servicios de seguridad informática que también ofrece servicios de consultoría141.

Durante un discurso pronunciado en enero de 1999 ante la Academia Nacional de Ciencias en relación al plan *Cyber Corps* para combatir al ciberterrorismo, el presidente Bill Clinton dijo que le pediría al Congreso la suma de 1.460 millones de dólares en el próximo presupuesto federal para financiar el proyecto. Esa suma implicaba un incremento del 40% de los gastos dedicados a esa área hasta el momento. “Todos los estadounidenses deben entenderlo: El gobierno tiene que financiar esta iniciativa”, dijo Clinton142.

Suzan Revah, periodista del sitio de noticias tecnológicas CNETNews, señaló que las compañías especializadas en *software* de seguridad Network Associates —que ya llevaba 15 años como contratista gubernamental— y Axent Technologies, eran sólo dos de las empresas que se beneficiarían si el Congreso aprobaba ese plan143.

“Esta es una buena noticia para nosotros”, dijo Marvin Dickerson, *señor product marketing manager* de Network Associates, en relación al discurso de Clinton. “Las personas con las cuales hacemos negocios tendrán mucho más dinero para gastar”, reconoció144.

141 Smith, George. Op. Cit.

142 Revah, Suzan. *Clinton outlines anti-cyberterrorism plan.* CNET News. 22 de enero de 1999.

143 Ibid.

144 Ibid.

72

En octubre de ese mismo año, el poder Ejecutivo solicitó 8,4 millones de dólares para poner en marcha el proyecto FIDNET. Además, el plan solicitó 50 millones para la implementación de medidas de seguridad necesarias en todas las dependencias gubernamentales, 17 millones para la capacitación y el entrenamiento en tecnologías de la información de personal del gobierno federal, y 7 millones más para destinar a investigación y desarrollo. La presentación del proyecto ante el congreso estuvo a cargo de John Tritak, director de la CIAO, y Michael Vatis, director del NIPC.

“El NIPC obtuvo mayor financiamiento para continuar defendiendo a los Estados Unidos de la amenaza fantasma”, señaló un artículo de la revista especializada en informática *The Industry Standard*145. “Las principales compañías de seguridad inmediatamente se alinearon con la postura del gobierno. La empresa Secure Computing firmó un contrato con la National Security Agency (NSA) para diseñar un
sistema operativo seguro, y Network Associates y otras empresas de seguridad informática se mostraron ansiosas por vender sus productos antivirus, herramientas de escaneo y *firewalls* al Gobierno para ayudarlo a detener a los ciberinvasores”.

Un contrato de 5000 millones de dólares

En junio de 2000, pasado ya el temor a la “falla del milenio”, la NSA anunció su intención de tercerizar parcialmente su infraestructura tecnológica, dando cabida a empresas del sector privado, con las cuales se firmaría un contrato a 10 años por el valor de 5 mil millones de dólares. Según el *Washington Post*, tres consorcios empresarios del sector privado, liderados por grandes corporaciones estadounidenses, fueron convocados para participar en la licitación146,.

Una vez firmado el contrato, la NSA cesantearía a entre 1.200 y 1.500 empleados y a 800 empresas o personas contratadas. La agencia señaló que el gigantesco contrato cubriría cuatro áreas: computadoras distribuidas, manejo de la seguridad corporativa, redes y telefonía.

Si bien la prevención del ciberterrorismo representa una función secundaria dentro del rol de la NSA, la magnitud de las cifras mencionadas da una clara idea del beneficio económico que representa para los contratistas tecnológicos gubernamentales la existencia de una supuesta amenaza informática contra la infraestructura nacional.

Finalizado el gobierno de Clinton, George Bush se mostró en un primer momento un tanto más escéptico que su antecesor en cuanto a la necesidad

145 Ginorio, Erik. *Hunting Phantoms*. The Industry Standard Magazine. 31 de julio de 2000.

146 Citado en un cable de la agencia Reuters titulado *NSA Outsourcing Tech Overhaul* (sin firma), 7 de junio de 2000.

de invertir enormes sumas en la prevención del ciberterrorismo, y algunos de los organismos creados por Clinton para tal fin fueron total o parcialmente desmantelados. Sin embargo, luego de los atentados del 11 de septiembre de 2001, la postura gubernamental retomó los lineamientos que signaron a la política de Clinton en relación con el tema.

El mismo día de los atentados, el Gobierno destinó 10 millones de dólares al financiamiento de la guerra contra el ciberterrorismo, materializada en la creación de la Oficina de Ciberseguridad, dirigida por Richard Clarke, el "zar" del antiterrorismo informático durante la presidencia de Clinton.

"Puede que los políticos no sepan la diferencia entre un *byte* y un *nibble*147, pero son expertos en gastar dinero. Y luego de los atentados del 11 de septiembre, los legisladores parecen proclives a firmar cheques inusualmente grandes", señalaron dos periodistas de la revista *Wired*148.

Para el presupuesto del año fiscal 2003, la administración de Bush solicitó la suma de 52.000 millones de dólares para destinar a la actualización tecnológica del gobierno federal, lo que implica un incremento de 4.000 millones de dólares en relación al presupuesto del 2002149.

El incremento del gasto gubernamental impacta también sobre el sector civil. Las principales industrias estadounidenses, incluyendo a la banca, transporte y servicios de energía, han establecido acuerdos comerciales para mejorar sus defensas ante los ciberataques, cooperando con la *Office of Homeland Security*. Como resultado, la empresa International Data Corp. predijo que el mercado del *software* de seguridad para Internet crecerá de 6.000 millones de dólares en el 2001, a 14.600 millones de dólares en el 2006150.

María Cirino, CEO de la firma Guardent Corp, dijo que su empresa espera duplicar su facturación y llegar a los 30 millones de dólares en el 2004 vendiendo servicios de seguridad en redes. Desde su *data center* ubicado en Rhode Island, Guardent monitorea en forma remota las redes de computación de sus más de 1000 clientes y se encarga de detener las intrusiones.

Las empresas del sector tecnológico niegan ser las principales

beneficiarias del incremento en el gasto gubernamental. “Si hubo un aumento significativo en el gasto luego del 11 de septiembre, no lo estamos viendo”151, dijo John Worral, vicepresidente de marketing de RSA Security Inc. “El Congreso ha destinado una gran cantidad de dinero a la seguridad,

147 El *nibble* es una unidad de informática equivalente a medio byte (cuatro bits).

148 McCullagh, Declan, y Polen, Ben. *Fighting Evil Hackers With Bucks*. Wired Magazine, 11 de octubre de 2001. Se puede leer el artículo en: http://www.wired.com/news/politics/0,1283,47479,00.html

149 Cifras extractadas de Kerber, Ross. *Waiting for the security payout*. The Boston Globe, 6 de marzo de 2002. El artículo se puede leer en: http://www.boston.com/dailyglobe2/154/business/Waiting_for_the_security_payout+.shtml

150 Ibid.

151 Ibid.

pero eso no significa que la industria de la seguridad informática vea los beneficios inmediatamente”, agregó.

Cuando el FBI anunció a principios de marzo de 2002 que reestructuraría sus prioridades y pondría mayor énfasis en luchar contra el ciberterror y construir una base de información tecnológica, William Whyte, director de investigaciones de Ntru Cryptosystems Inc .(empresa que desarrolla *software* de seguridad para tarjetas inteligentes) se apresuró a señalar que el anuncio del FBI no incluyó una solicitud de mayor presupuesto. Esa omisión, en su opinión, significa que “el FBI se está enfocando en un uso más eficiente de sus recursos”.152

Las grandes sumas de dinero destinadas a la seguridad informática por el gobierno federal podrían contribuir a enmascarar casos de corrupción. En julio de 2000, Compaq aceptó pagar la suma de 4,5 millones de dólares para poner fin a la disputa surgida en torno a una empresa que compró en 1998 (Digital Equipment Corp.), la cual fue acusada de sobrefacturar la instalación de computadoras y redes para el Departamento de Defensa. Digital Equipment había obtenido un contrato de 235 millones de dólares, y la sobrefacturación pudo ser comprobada.

152 Ibid.

Conclusiones

La palabra ciberterrorismo, acuñada en los años 80, nació con el estigma de la exageración. De hecho, su significado carece de cualquier componente cibernético que justifique la utilización del prefijo *ciber*. “Teleterrorismo” o “terrorismo digital” hubieran sido expresiones más realistas, aunque menos impactantes, para designar a este fenómeno que consiste en la realización de actos terroristas a distancia por medios informáticos.

No se ha registrado hasta el momento ningún atentado que corresponda a esas características, pese a que los medios de comunicación y los políticos estadounidenses usaron en los últimos años -y siguen usando- la palabra ciberterrorismo con bastante frecuencia.

La factibilidad de que ocurra un atentado ciberterrorista con víctimas fatales o grandes daños a la infraestructura estadounidense es muy escasa. En primer lugar, porque las empresas que prestan servicios en áreas vitales

incluyen en sus procedimientos críticos un nivel de intervención humana directa que torna casi imposible provocar grandes daños utilizando una computadora conectada a un módem y ubicada a miles de kilómetros de distancia del objetivo.
Cuando a un alto ejecutivo del *North American Electric Reliability Council* (una asociación de empresas generadoras de electricidad) le comentaron que, según el FBI, el suministro de energía eléctrica era vulnerable al ataque de los *hackers,* dijo: “No tengo noticias de que ningún mecanismo de control energético esté conectado a módems ni a líneas telefónicas”. Eso mismo ocurre en la mayoría de las industrias vinculadas a la infraestructura.
Igualmente remota es la posibilidad de que un grupo de *hackers* intervenga las comunicaciones de un controlador de tráfico aéreo y envíe información errónea a las aeronaves para hacerlas colisionar, como sugiere otra hipótesis muy difundida por los medios de comunicación.
Los pilotos de las aerolíneas son entrenados para operar en la ausencia de todo control. Desde el primer día se les enseña a determinar por sí mismos su velocidad, dirección y altitud. Incluso muchas veces los pilotos descubren y corrigen errores cometidos por los controladores de tráfico aéreo.
76
77
Más allá de las dificultades técnicas que impedirían concretar acciones ciberterroristas de envergadura, existe otra cuestión: los grupos terroristas actuales suelen buscar el impacto visual. Generar imágenes de explosiones, fuego, muertos y ambulancias en las pantallas de televisión es hoy el objetivo de la mayoría de los grupos terroristas.
En 1998, un periodista le preguntó al especialista en ciberterrorismo William Church si grupos como el de Bin Laden podrían utilizar armas cibernéticas o si, por el contrario, el impacto visual de un edificio explotando por el efecto de una bomba seguía siendo prioritario. Church respondió: “Acaba de dar en el clavo. Los grupos terroristas son altamente proclives al impacto visual”. Tres años más tarde, las imágenes de las Torres Gemelas derrumbándose le darían la razón.
El sobredimensionamiento de la supuesta amenaza ciberterrorista, que llevó a varios políticos estadounidenses a pronosticar un “Pearl Harbor electrónico”, tiene por lo menos dos causas definidas. Una de ellas es que quienes más hablan en los medios de comunicación sobre los posibles escenarios catastróficos son quienes más se benefician con el miedo ante el ciberterrorismo: los ejecutivos de las empresas informáticas.
Como se explicó en esta tesis, durante el gobierno de Clinton se tomaron una serie de medidas destinadas a luchar contra el ciberterrorismo que implicaron una inversión gubernamental en seguridad informática de varios miles de millones de dólares. Posteriormente –y sobre todo después de los atentados del 11 de septiembre- el gobierno de Bush decidió adoptar una política similar.
Otra razón para la proliferación de comentarios exagerados sobre posibles

actos ciberterroristas es que, desde los años 80, los medios de comunicación estadounidenses son la arena en la que se dirime un intenso debate acerca de la privacidad de los ciudadanos en relación con los medios electrónicos. Mientras las agencias de seguridad gubernamentales buscan tener mayor poder para espiar las computadoras y las comunicaciones de los sujetos considerados sospechosos, distintas ONGs y organismos defensores de los derechos civiles se resisten a facilitar la intromisión del gobierno en la privacidad de los individuos.

Por lo tanto, se podría inferir que diseminar entre la población el miedo ante el ciberterrorismo es una forma de ganar apoyo político para la sanción de leyes que otorguen mayor flexibilidad a los organismos de seguridad para realizar sus tareas de espionaje interno.

Sebastián Masana, 8 de julio de 2002