RADICALITZEM *la vida*

La majoria de llibres de Virus editorial es troben sota llicències lliures i per la seva lliure descàrrega. Però els projectes autogestionaris i alternatius, com Virus editorial, necessiten un important suport econòmic. En la mesura que oferim bona part del nostre treball pel comú, creiem important crear també formes de col·laboració en la sostenibilitat del projecte. Subscriu-t'hi!!

La mayoría de libros de Virus editorial se encuentran bajo licencias libres y para su libre descarga. Pero los proyectos autogestionarios y alternativos, como Virus editorial, necesitan de un importante apoyo económico. En la medida en que ofrecemos buena parte de nuestro trabajo para lo común, creemos importante crear también formas de colaboración en la sostenibilidad del proyecto. ¡Subscríbete!

Satèl·lit
sense quota

-5%
5 compras
mínimo anual
Pack bienvenida
Punto de lectura
+ postal

Càpsida

60€
-5%
En toda la librería online
4 libros
Virus editorial
sin límite de precio
Pack bienvenida
Bolsa #RadicalitzemLaVida
+ Punto de lectura
+ postal
Descuentos
En grupos de lectura
i otras actividades

Replicant

100€
8 novedades
Virus editorial
durante un año
Pack benvinguda
Bolsa #RadicalitzemLaVida
+ Punto de lectura
+ postal
-5%
En toda la librería online
Descuentos
En grupos de lectura
i otras actividades

https://www.viruseditorial.net/es/editorial/socios

Reunión de Ovejas Electrónicas (ROE)

CIBERACTIVISMO

Sobre usos políticos y sociales de la Red

VIRUS editorial

Reunión de Ovejas Electrónicas (ROE)

CIBERACTIVISMO

Sobre usos políticos y sociales de la Red

Maquetación: Virus editorial

Cubierta: PCC

Primera edición: junio de 2006

Lallevir S.L.
VIRUS editorial
C/Aurora, 23 baixos
08001 Barcelona
T./fax: 934413814
C/e: virus@pangea.org
http://www.viruseditorial.net

Impreso en:
Imprenta LUNA
Muelle de la Merced, 3, 2º izq.
48003 Bilbao
T.: 944167518
Fax: 944153298

I.S.B.N.: 84-96044-72-6
Depósito Legal:

ÍNDICE

ESTRATEGIAS DE FUTURO EN CLAVE DE PRESENTE (Y ALGÚN PESCOZÓN DEL PASADO)

Víctor Sampedro Blanco

«El Occidente, drogado de devenir, inclina su presente hacia el futuro y nos fuerza a todos a entender que, para responder a su desafío, debemos combatirlo en el terreno que ha elegido: el presente.»
Fátima Mernissi, *El harén político*

No pretendo pontificar sobre la valía de las intervenciones y las tácticas ciberguerrilleras. Tampoco herir más sensibilidades de las necesarias. No vaya a ser que abortemos «las embrionarias subjetividades revolucionarias, reticulares, rizomáticas...» que puedan leernos. Que vaya usted a saber qué ocurriría si, tras leer este libro, actuasen ustedes como guevaristas de Internet. Imaginémonos practicando foquismo telemático, durante al menos media hora al día, desde el ordenador de la gran (o ridícula) corporación para la que trabajamos, haciéndole la Pascua. Por soñar que no falte y, por otra parte, nada más reaccionario que un agorero de lo que todavía no se ha intentado.

Sin embargo, para disfrutar de cualquier recetario (aunque este libro no pretenda serlo) hay que reconocer qué es lo que se cocina y —sobre todo— para quién. No vaya a ser que al final montemos el tres estrellas Michelín del activismo más guay y no un comedor autogestionado para analfabetos funcionales de la Red, como yo... o casi. Pues reconozco mi escasa competencia informática. Apenas me da para procesar textos, intercambiar correos y «navegar» (con pulso bastante temblón y timón inseguro) por Internet.

Los tres argumentos que aquí esgrimo parten de unas cuantas lecturas sobre la materia y reflejan esa indigencia tecnológica, nimia si se compara con la de tantos para los que un ratón es sólo un bicho, una amenaza para la cosecha, un compañero de miseria. Desde mi ignorancia (por otra parte, opulencia), agradezco haber leído este libro: ahora creo saber más, para hacer y decir más con el ordenador. Necesito, sin embargo, que no se me vaya la olla ante tanto menú desplegado en mi pantalla. Y, por eso, me doy unos cuantos toques, para aplacar la bulimia ciberguerrillera que me ha entrado. Por tanto, que ninguno de los autores se dé por aludido en exclusiva y todos (yo el primero) en general.

Toda estrategia de futuro, desconectada del presente e ignorante del pasado, resulta tan triste como la «nuvel cusin» esa: llena los ojos y apenas enga-

ña el estómago. Para no quedarnos con hambre, me gustaría recordar tres certezas o, como mínimo tres certidumbres, avaladas por todos los estudios y hasta el sentido común. Primero: la tecnología es neutra; sobran, por tanto, el optimismo y el pesimismo exacerbados. Segundo: una nueva tecnología pasa *siempre* por una crisis de control, que acaba siendo superada, también *siempre*, por los usos institucionales (del poder) y las prácticas cotidianas (de las gentes) que terminan «normalizando» esas tecnologías, domesticándolas. Tercero: la ciberguerrilla (como cualquier otra forma de contestación y resistencia) o teje comunidades libres e interpela al poder (las dos cosas) o resulta ser (en el mejor de los casos) una guerra de mentirijilla, mera pose revolucionaria: fuegos fatuos para fatuos activistas, pagados de sí mismos y de sus arsenales, que, por otra parte, no pasan de pura retórica.

Sueños y pesadillas

Un nuevo espacio público surgió cuando la computadora aumentó las capacidades de procesar y almacenar información desde el hogar. La interconexión de los ordenadores en Internet hizo posible transmitir conocimientos, generados desde infinitas terminales. La comunicación resultaba, por fin, horizontal, interactiva, reticular, anónima, muy económica, con difusión ilimitada y en tiempo real. Ante tal lista de adjetivos era lógico que entrase el vértigo y surgieran dos discursos antagónicos. Encarnan dos posturas clásicas, que se repiten a lo largo de la historia con cada novedad técnica. Por una parte, están los optimistas que saludan el cambio y se las prometen más felices que nunca. Por otra, nunca faltan los pesimistas, que abominan de toda novedad y no encuentran su sitio en el nuevo escenario tecnológico, a no ser como plañideras nostálgicas o víctimas propiciatorias del futuro.

Los optimistas destacan que la Red potencia las posibilidades individuales y los horizontes de emancipación colectiva. En los años setenta del siglo XX se acuñó el término «sociedad de la información y el conocimiento», donde la opulencia mediática habría transformado la base social e, incluso, el poder. Más tarde, Internet actualizó el vocabulario con el concepto fetiche de «sociedad-red». La interconexión y la descentralización alcanzaban su apogeo. Se acababan los monopolios sobre el saber y su transmisión. Asistíamos al advenimiento del conocimiento colectivo, sin dueños ni fronteras... la autogestión y la autodeterminación individuales acabarían socializadas en comunidades caracterizadas por el dinamismo y la innovación...

Ante tal despliegue retórico, los pesimistas del ciberespacio necesitan vestir dos paños, según se apunten a la crítica posmoderna en plan progre o a la moda retro. Ciertos agoreros, inspirados por Michael Foucault, denuncian que vivimos la pesadilla de una «sociedad panóptica» (que todo lo ve). Internet reproduciría un modelo de control semejante a las prisiones donde el carcelero, sin moverse de su garita, vigila celdas casi transparentes, sin resquicio para la intimidad o el secreto. Para los optimistas la pantalla de ordenador proyectaba sueños emancipadores. Para los panópticos representa una cámara de seguridad. Es la mirilla con

la que el Poder nos disciplina, nos mantiene a raya. Todo el tiempo, amenazando con registrar o reventarnos el disco duro.

De otra forma, pero en el mismo bando, el pesimismo retro hacia las nuevas tecnologías se enfanga en «la cloaca de Internet». La Red es considerada un caos «anárquico y anarquizante», un flujo pestilente de mensajes sin rigor, ni criterio de veracidad, ni ética. Los chivos expiatorios resultan ser los «grupos radicales y violentos» en lo político y la pornografía y la pederastia en lo moral. En los medios y en la calle se alimentan estas admoniciones. La multiplicación de los controles paternos y legales es su corolario. Los padres de la patria y del hogar son los celadores necesarios para que Internet no se desmande (siga sin mando).

En suma, los optimistas creen habitar un supermercado tecnológico, donde ejercen como soberanos, consumidores y productores. Su fuerza «mitopoiética» es mucha; el activismo cibernético se alimenta del mito de que la revolución puede alcanzarse sin levantarse del ordenador y los activistas se convierten en el futuro panteón ciberguerrillero. Hasta ahora la soberanía comunicativa residía en elegir una cadena de televisión entre muchas. Ahora, se nos promete mucho más: interactuar, generar e intercambiar flujos comunicativos a gran escala y con enorme impacto. No es extraño que el discurso optimista arraigue entre quienes tienen mayor capacidad de consumo tecnológico, inversión empresarial y visibilidad social. Así cualquiera. Pero en el fondo no es una teoría para guerrilleros, sino de soberanos y para soberanos. Para los que sostienen la e-economy (corporativa o alternativa, qué más da) que se desinfla cada dos por tres. Como es tan precaria, la mitopoiesis necesita realimentarse cada cierto tiempo desde las mejores tribunas mediáticas (convencionales o de contrainformación, qué más da).

Los pesimistas, como en tantas otras ocasiones, no sólo pecan de realismo, sino que tienden a la vagancia derivada de su fatalismo. Sus argumentos promueven la inactividad, la parálisis. Aciertan cuando esgrimen la proporción de la población mundial que ni siquiera tiene acceso telefónico; y más aún cuando, dentro de esos excluidos, recuerdan la mayoría de gentes del Sur, de mujeres, y hablan de lenguas hegemónicas. Vuelven a dar en el clavo señalando que los desarrollos empresariales y legales de Internet apuntan a todo menos a la esperanza. Pero se equivocan si no abren los ojos y las orejas para percibir en qué medida se han ampliado los proyectos de cambio social y la posibilidad de conectarlos entre sí. Nunca como ahora se han escuchado tantas voces, ni tantos coros. Otra cosa es lo que canten y nuestra capacidad de atender y entender.

En el fondo, los dos polos de este debate carecen de sentido. Son percepciones selectivas de las posibilidades y los límites de la tecnología, la cual, lejos de encarnar un modelo social en sí misma, es neutra: su bondad depende de sus efectos y, por tanto, de quién los decida. Dicho de otra forma, una tecnología no es nada más que un conjunto de dispositivos asociados a unos procedimientos, que aumentan la eficacia y la eficiencia. La eficacia reside en alcanzar los fines pro-

puestos. La eficiencia consiste en lograr esos objetivos con el mínimo coste y el máximo beneficio. Por tanto, resulta obvio que para evaluar las NTIC (nuevas tecnologías de la información y la comunicación) hemos de determinar para qué objetivos se emplean y quién demonios se beneficia de ellas. La respuesta es diferente en Finlandia y en Sudán. ¿Por qué?

Crisis de control tecnológico, ¡y que nos dure!

Toda nueva tecnología es dirigida hacia unos fines y acaba siendo asociada a unos costes sociales. La asignación de costes y beneficios depende de dos factores: uno, la actuación de las instituciones y, dos, cómo la utilicen los ciudadanos. Consideremos por un momento la televisión. Por una parte, los poderes económicos y políticos, el Estado y el Mercado, determinan en gran medida la oferta televisiva: depende de las licencias de emisión o las políticas audiovisuales (Estado) y de las cuotas de audiencia del mercado publicitario. Es decir, los políticos (favoreciendo a las empresas que, supuestamente, les trabajan el voto) y los mercaderes (primando la oferta que da lucro) influyen y mucho en lo que podemos ver en televisión. Pero también importan las prácticas de uso y consumo, lo que la gente hacemos con la televisión.

La serie de TVE *Cuéntame* es la primera que aborda en clave cotidiana y familiar la memoria histórica de la dictadura franquista. No se emitió antes porque los dirigentes de TVE han pertenecido a partidos que hicieron una transición basada en el olvido, con pactos asentados en silencios. Además, es una serie muy cara, difícil de producir y sin tantos beneficios publicitarios como otros formatos más baratos. Por ultimo, la población española asumió, de forma mayoritaria, la amnesia suficiente para seguir votando cada cuatro años «sin mirar atrás». No ha sido el caso de los partidos nacionalistas periféricos ni de sus votantes, que buscaron legitimarse en la denuncia de la represión franquista. Por eso, las televisiones vasca y catalana sí han emitido programas de «revisión» histórica, obviamente con un mensaje interesado. Cuando emiten episodios de *Cuentáme* cargados de conflicto político, sube la audiencia vasca y catalana. Como no son mayoría, los guionistas no pueden «meter más caña». Por tanto, si sumamos la penuria de la producción audiovisual independiente, el control político de las cadenas y la desmemoria histórica de los españoles, podemos entender por qué TVE no ha servido —como en la mayoría de países que sufrieron dictaduras, Finlandia incluida— para revisar el pasado reciente... sino para sublimarlo.

Creo escuchar ya al lector tecnófilo: Internet no puede compararse con ningún medio precedente. Pero ese argumento se ha aplicado a toda nueva tecnología, que ha acabado por hacerse «vieja». Vieja, en el sentido de entender que no aporta nada «nuevo». Nadie, con sentido del ridículo, postularía la fotocopiadora como una tecnología cargada de potencial revolucionario. Por eso induce a la sonrisa leer lo publicado apenas treinta años. El escritor alemán Hans Magnus Enzensberger, cuando era un extraparlamentario en los setenta (del siglo XX), expli-

caba el enorme riesgo que encarnaba la fotocopiadora tanto para el estalinismo como para el capitalismo. Éste es «un ejemplo»[1] de cómo...

> *Los nuevos medios están orientados hacia la acción, no hacia la contemplación; hacia el presente, no hacia la tradición. Su actitud hacia el tiempo es completamente opuesta a la representada por la cultura burguesa, la cual aspira a la posesión, esto es, duración y preferentemente eternidad. Los medios no producen objetos almacenables y subastables. Acaban por completo con la «propiedad intelectual», es decir, la transmisión de capital inmaterial, específico de clase.*[2]

Si con la fotocopia venía la debacle del Muro de Berlín y el ocaso de las grandes editoras (¡en 1972!), ¿qué no pasaría con la tele en color? Así de perdidos andaban los pronósticos. Y aún hay quien sostiene que el comunismo cayó porque la televisión occidental se veía tras el Telón de Acero. Ahora Hollywood filma las crónicas televisivas de la ocupación de Irak y Putin hace la versión gore de la liberación de rehenes chechenos. Mercados, Estados y espectadores de lo que en otro trabajo llamamos «entretenimiento desinformativo» mantienen el espectáculo en pie.

Las razones del fracaso de la fotocopiadora como instrumento revolucionario resultan evidentes. ¿Algún gobierno aprobó alguna ley que permitiese la fotocopia libre a algún colectivo «desfavorecido» o «sin afán de lucro»? Como las empresas culturales no tienen como fin democratizar el conocimiento promovieron leyes contra las fotocopias «ilegales». Y proponen alguna medida más dura, como aplicar en las bibliotecas públicas un pago adicional por cada persona que lea un libro. No parece haberse cumplido el fin de la «transmisión de capital inmaterial, específico de clase», que auguraba Enzesberger. ¿Tienen razones institucionales los gobernantes y los empresarios para mantener una disposición diferente con las NTIC? ¿Nos permiten «acabar por completo con la "propiedad intelectual"»?

A los fines institucionales —hacer dinero y acumular poder— se suman las prácticas sociales. La fotocopia tampoco encontró ni generó suficientes comunidades con discursos propios y ganas de difundirlos. Así ha ocurrido en la escuela y la universidad: dos supuestos centros de conocimiento. Los padres de la patria y sus leyes educativas, los padres de los estudiantes y sus AMPAS (sin hache), junto con los maestros han convencido a los estudiantes de que la fotocopia es una tecnología eficaz y eficiente sólo para aprobar los exámenes. De ahí que los estudiantes y los tunos acudan a la fotocopiadora en masa durante el mes de mayo. No para fotocopiar libros, sino los apuntes del empollón. Por lo que respecta a los profesores, afortunado es el centro que cuenta con alguno que de vez en cuando fotocopia y pincha en el corcho algún chiste o artículo de periódico. Precisamente en

1. Enzensberger, Hans Magnus (1972) *Elementos para una teoría de los medios de comunicación*. Barcelona, Anagrama, pp. 16 y 17.
2. Ibidem, pp. 28 y 29.

los «centros del saber» la fotocopia sirve, sobre todo, para difundir apuntes al dictado y chascarrillos mediáticos.

De nuevo se presiente incómodo al cibernauta que cuestiona la comparación de las NTIC con la fotocopia (que, sin embargo, también prometía la reproducción ilimitada de mensajes) y con la televisión (que, supuestamente, brinda acceso «universal» y en tiempo real a toda «realidad» imaginable, sin requerir alfabetización). Remontémonos, para provocar aún más a los tecnófilos, a los tiempos de la máquina de vapor y el telégrafo.

Quizás estemos asistiendo a lo que se conoce como una *crisis de control tecnológico*. Toda nueva tecnología plantea retos a las instituciones y a las gentes, de modo que pasa por periodos de descontrol. La potencia tecnológica aún no está del todo encuadrada en unos fines económicos, políticos o sociales. De este modo, el Estado y el Mercado pueden ser cuestionados *temporalmente*. Vanguardias de usuarios, siempre de los grupos dominantes (hombres, propietarios —al menos de recursos técnicos—, con cierto nivel educativo o estatus), plantean retos a quien gobierna y comercia. Formulan proyectos que cuestionan los modos tradicionales de hacer dinero y hacerse con el poder. Los optimistas se aferran a estos períodos y sueñan con que sean indefinidos. Pero con el tiempo esa vanguardia acaba trabajando en un sistema tecnológico que cierra los horizontes de emancipación, ajustándolos a las instituciones y a los grupos privilegiados. Algunos tecnófobos sienten y denuncian ese control creciente e inevitable.

El vapor supuso algo semejante a la digitalización. Ambas tecnologías permitieron trascender los parámetros de tiempo y espacio, al comprimirlos dotaron a la comunicación de un alcance hasta entonces desconocido. El telégrafo hizo posible, por primera vez, la transmisión «inmaterial» de los conocimientos. Y cuando se estaba implantando, permitió numerosos actos de piratería y formar comunidades situadas, literalmente, en la frontera del progreso. Cuentan los historiadores que la desconexión entre la rapidez para desplazarse con el vapor y ciertos problemas para comunicarse mediante el telégrafo hicieron resurgir una piratería marítima más sofisticada y con menos riesgos[3]. Era posible convencer a las navieras de que un barco —desviado a otro puerto para vender ilegalmente parte de la carga— había sufrido un percance, sin poderse comunicar por alguna tormenta. Esto justificaba la demora y la pérdida parcial del flete. Es decir, los bucaneros del vapor anticiparon a los hackers que, mientras simulan trabajar para la compañía que paga Internet, realizan actos de reapropiación o sabotaje.

El telégrafo también disparó la creación de nuevas comunidades en el Oeste norteamericano. Las sectas religiosas vieron impulsadas sus creencias y valores por la inmaterialidad y la ubicuidad telegráficas. Ese poder casi-divino ahora estaba disponible también para los humanos. Se instalaron así multitud de comunida-

3. Beniger, James R. *(1986) The control revolution. Technological and Economic Origins of the Information Society.* Harvard University Press. En las páginas 194-202 se detalla el despliegue de mecanismos de "control y *feedback*" desarrollados en EE.UU. entre 1780 y 1850 para acabar con tales desmanes.

des pioneras en la frontera. Eran pioneras en el sentido geográfico, tecnológico y filosófico... como las cibercomunidades. Se llegó a argumentar que el vapor y el telégrafo, sustentos de la prensa moderna (imprenta mecánica y servicios de noticias), habían roto ya las fronteras entre los pueblos y los límites del desarrollo. La Aldea Global se invocaba ya en el XIX.

> *La unanimidad* [entre las sectas religiosas] *que, a primera vista, habría parecido sobrenatural se hizo posible gracias al telégrafo y la prensa. Éstos congregaban y difundían «el ansia de la empatía cristiana, con los lazos de la gracia plena, entre multitudes reunidas simultáneamente en cada ciudad, uniendo de hecho la nación en una sola plegaria». Y no por casualidad estas movilizaciones coincidieron con el Cable Atlántico* [línea telegráfica transcontinental, entre Europa y EEUU, claro], *porque era portador de «la avanzadilla de la última victoria espiritual». En los albores de 1858, por primera vez se hizo vital para el imaginario americano el proyecto posible de una tecnología cristianizada.*[4]

La cita nos remite a la continuidad que se percibe en los discursos con los que Ronald Reagan defendía el escudo nuclear de la «Guerra de las Galaxias» o los de la «Guerra preventiva» de G. W. Bush. La lucha contra el Mal basa sus propuestas bélicas en la prepotencia tecnológica de los EE.UU., que a su vez se esgrime como símbolo de supremacía civilizatoria. De hecho, son argumentos próximos a las exaltaciones de la Comunidad Universal de Todos los Santos Cibernéticos de más de un gurú. Como nos recuerda cualquier repaso histórico, los sucesivos adelantos tecnológicos sirvieron para desarrollar ejércitos de masas, y sin ellos sería inexplicable la Primera Guerra Mundial: la Gran Carnicería que inauguró y presagió las siguientes del siglo XX. Las cirugías bélicas del XXI (atentados «selectivos» o «masivos» y la «guerra en red» del/contra el terrorismo) no parecen habernos ahorrado ni un ápice de barbarie.

Desde la Revolución Industrial hemos asistido a suficientes determinismos tecnológicos de tono enajenado. Podríamos haber aprendido algo de tanto desafuero mitopoiético. Aburren (por reiterados e ilusos) los pronósticos de cómo el capitalismo conlleva e incluso alimenta potencialidades liberadoras y hasta de autodestrucción. Posibilidades que cada cierto tiempo se ven encarnadas por una nueva tecnología. Unos ven los cambios con esperanza y otros con miedo. El pionero que se sentía dios al telégrafo resultaba tan ridículo como el ludista que destruía las máquinas. Hoy en día sólo han cambiado de máscaras. Quizás fuese más fructífero considerar, desde la modestia y cierta serenidad, cómo podemos aflojar las mordazas institucionales y liberar las prácticas sociales que funcionan como bozales de las NTIC.

4. Perry Millar (1956), citado en Carey, James (1989) *Communication and Culture*. Unwin Hyman, p. 17.

Estos dos objetivos me parecen imprescindibles, si no queremos deleitarnos lamiéndonos el ego o las heridas. Y, de hecho, los usuarios de las NTIC más lúcidos no prescinden de ninguna de esas metas. Por una parte, se resisten a que los mecanismos de control político y económico limiten sus modos de hacer y decir las cosas en Internet. Por otra, socializan las herramientas y los usos tecnológicos que escapan al poder. Arramplan con la LSI, intentan bloquear la red Echelon y abren los weblogs o los talleres de Linux a todo menda con ganas de bregarse. Desde esos dos ámbitos de acción —el institucional y el social— sería posible ampliar —en el tiempo y entre la gente— la crisis de control tecnológico a la que asistimos. También son planos necesarios para disfrutar la crisis, mientras dure, y prolongarla cuanto podamos. Si Internet está generando un nuevo espacio público, la capacidad liberadora del mismo va a depender de nuestra habilidad para interpelar desde él al Poder —no sólo simbólicamente— y para autoorganizarnos en redes, no sólo virtuales, sino de carne y hueso.

Periferias que no se queden al margen

Las NTIC han transformado los espacios públicos y generado otros nuevos; los ponen en contraste, crean contradicciones. Me refiero a lugares metafóricos —creados por todos los dispositivos comunicativos—, donde nos juntamos en calidad de ciudadanos para debatir los consensos y el devenir colectivos. Parece obligado repensar un espacio público que responda a un proyecto de democracia radical: asentada en las raíces sociales y no en máquinas de vapor, postes de telégrafo o bits. Además, podríamos sopesar para qué fines y a quiénes queremos que sirvan las NTIC. Lo que sigue sólo pretende abrir líneas de debate. Tómese, por tanto, más como un intento de reflexión que quiere ser compartida y que es provisional.

Los rasgos del nuevo espacio público y los límites de las NTIC también son provisionales. Como hemos dicho antes, dependen de políticas, mercados y prácticas ciudadanas, que de hecho varían según los países y a lo largo del tiempo. Intentaré referirme a unos acontecimientos recientes, que se quieren zanjar con discursos optimistas y pesimistas bien ramplones. Me refiero a las movilizaciones del 13 de marzo, las concentraciones de desobedientes civiles ante las sedes del PP, en el día de reflexión previo a las Elecciones del 2004. Lo que sigue son algunas conclusiones del libro *13-M: Multitudes on line* (Libros de la Catarata, Madrid, 2005), que escribimos sobre aquellos hechos. El 13-M fue catalogado como «la inauguración de la era de las multitudes» (T. Negri) o como «*flash mobs* de miserables manipulados» (el Partido Popular). Optimistas y pesimistas volvieron a la carga, imputando a las NTIC todo el poder de emancipación o de instrumentalización de la ciudadanía, vigilante o borrega, según el caso. Empecinados en adjetivar, nadie parece dispuesto a aprender de lo ocurrido y, en cambio, sí a pasar página (la escrita por unos pocos).

Entre la masacre del 11 de marzo y las elecciones del día 14, Internet permitió romper el bloqueo desinformativo al que se plegaron los medios. La telefo-

nía móvil sirvió para coordinar la desobediencia civil no violenta, primero en la manifestación institucional del día 12 (convocada por TODOS los medios convencionales, en contra de ETA) y, después, en las concentraciones del día 13 (denunciando la ocultación y la mentira). Ignorar que desde la Red se minó el monopolio estatal de la información y que la versatilidad de los SMS sirvió para coordinar protestas, supondría negarnos la posibilidad de repetirlo. Ahora bien, el resultado político fue la alternancia en el poder, pasando éste a manos de otro partido moderado.

Estos hechos apuntarían a que las NTIC son aún «periféricas», guardan escasas conexiones con la esfera pública «central». Es decir, no permiten entrar en los debates que gestionan los medios convencionales masivos y las instituciones del poder[5]. Los dos días siguientes a las elecciones, el PP logró mayor visibilidad que los colectivos que convocaron el 13-M. Los medios convencionales recogieron con más atención la convocatoria con SMS de las manifestaciones en apoyo a los líderes derrotados o contra Pedro Almodóvar, que les acusaba de haber intentado dar un golpe de Estado. La eficacia del PP —en términos de mensajes introducidos en la esfera pública central, la que llega a casi todos— fue muy superior a la de los desobedientes del día 13.

Después de la «trascendencia electoral» de las protestas del 13-M, todo lo dicho entonces en la calle o en Internet acabó resultando «periférico». Otros, los que ocupan el centro (el ideológico y el de la esfera pública) se permitieron el lujo de intercambiar acusaciones, sin probarlas ni retractarse cuando se demostraban falsas. Como en las dictaduras, parece imposible denunciar la mentira en público, ante todo el mundo. Como en las cortes medievales o los autoritarismos cunden las teorías de la conspiración, de un lado y de otro[6].

Sólo la debilidad de la esfera pública alternativa que construyen los ciudadanos con las NTIC (y la correlativa sumisión de los medios convencionales) explica un debate colectivo tan falso —por mentiroso— y tan cutre —por limitado— sobre el mayor atentado terrorista (subversivo) de la historia de Europa.

Una esfera pública democrática se define porque es el ámbito de la sorpresa, de lo inesperado; sobre todo para quien gobierna en nombre del pueblo. Nada resulta tan previsible como la (auto)censura del discurso prefabricado, una vez que se pone a funcionar. El éxito de la estrategia guerrillera reside en pillar por sorpresa al enemigo. ¿Creen ustedes que lo estamos logrando? Porque sorprender no

5. Conceptos desarrollados en Sampedro, Víctor (2000): *Opinión pública y democracia deliberativa. Medios, sondeos y urnas*. Madrid, Icaria.

6. Una teoría de la conspiración, la más conocida, afirma desde *ABC*, *La Razón*, *El Mundo* o la COPE que la policía engañó al partido que les mandaba y pagaba (y que, supuestamente, iba a ganar de nuevo las elecciones). Tricornios afines al PSOE además habrían toreado durante tres días a los servicios de inteligencia extranjeros (con los que, supuestamente, colaboran en la Guerra Global contra el Terrorismo). Por primera vez en la historia de la "joven —pero bien constituida— democracia española", los uniformados habrían mordido la mano que les alimentaba y habrían traicionado sus sagrados valores corporativos: lo del honor y el prestigio del Cuerpo. A eso se suma que etarras e integristas paseaban juntos en los patios de las cárceles (¿hay otros sitios donde pasear en el mako?) o tomaban té celebrando las bombas de Madrid (¿esperaban que un musulmán se pusiese ciego de txikitos?, ¿a alguien le sorprende el enésimo brindis al sol de ETA?). La otra teoría de la conspiración señala a la posibilidad de que el PP habría intentado suspender las elecciones; imputación nunca comprobada porque ningún medio hasta ahora ha exigido a la Junta Electoral Central que detallase todas las denuncias presentadas en la tarde del 13 y la madrugada del 14.

debiera entenderse como dar la nota, en el sentido de dar el espectáculo. Bastante nos vemos y leemos ya en los medios convencionales haciendo el payaso (con el culo al aire o versión *Full Monty*) o haciéndonos los interesantes (versión artista-activista modernillo).

Las nuevas tecnologías por sí mismas no ayudan a consolidar nuevas identidades colectivas. Esto es así porque las NTIC son más propensas a generar discrepancias que consensos, a enfatizar las diferencias sobre las coincidencias. Y ello es así, al menos, por dos razones. La primera: porque la interacción virtual sustituye (y muchas veces elimina) el contacto interpersonal, el único que confiere sentimientos de solidaridad y de responsabilidad compartidas. La segunda: porque el anonimato de los usuarios de las NTIC garantiza la menor implicación personal; pero de ahí, también, su capacidad de extensión en colectivos heterogéneos y muy amplios. El 13-M salieron a las calles en marchas desobedientes multitudes de ciudadanos. ¿Quiénes eran? ¿Dónde están?

Dar la nota, hoy en día, implica desvelar las mentiras del poder, encarando las mentiras propagadas sistemáticamente, por Sistema: el mismo Sistema que despliega controles institucionales y visibiliza sólo las prácticas sociales que normalizan la disidencia. Sorprender, *más allá* de dar el espectáculo, implica impactar, alterar la relación de fuerzas y los consensos de la opinión pública, entre las instituciones y el cotidiano. Y eso se hace tejiendo plataformas y redes que van *más allá* de lo virtual, de la periferia que tejen las NTIC. Ese Más Allá no es ningún paraíso tecnológico, sino el Más Acá que siempre hemos sabido que teníamos que trabajar: un espacio visible y audible, en las fisuras de los medios convencionales, de las instituciones y de las prácticas sociales. ¿O es que no queremos que los suplementos especializados, las políticas de innovación, las escuelas y las universidades acojan Linux como algo propio? Si tal cosa ocurriese, ¿no nos surgirían mil nuevas oportunidades de intentar cambiar los medios, la política y las formas de generar conocimiento colectivo? Como dice el EZLN, de nada sirve una guerrilla cuyo fin más alto no sea desaparecer. Retomando el símil de la insurgencia: desaparezcamos como el pez en el agua de la que se alimenta (como el maquis en el pueblo que le apoyaba).

Una vez más (y ya la última), si hablamos de abrir «zonas temporalmente autónomas» en la Red, no debiera ser para que acaben convertidas en un nicho de mercado —por alternativo que sea—, ni en las sedes de una vanguardia carente de crítica y autocrítica. Sino para sacarlas a la calle, en sentido literal: las calles de las embajadas, de las sedes de los partidos y los parlamentos, los kioskos de prensa, las ondas de radio y televisión... Tampoco nos vamos a engañar sobre nuestras posibilidades de éxito. Aprendamos de nuestras derrotas. Por favor, ya vale de ciberactivismo en plan *Love Parades*. En su lugar, como propone la Fiambrera Obrera, que proliferen los PornoLabs y la desobediencia matrimonial a la Ley de Extranjería. Redes y amor de carne y hueso, en lugar de cibersexo.

DEL TAM-TAM AL DOBLE CLICK UNA HISTORIA CONCEPTUAL DE LA CONTRAINFORMACIÓN

Sara López Martín
(acdc@nodo50.org) y
Gustavo Roig Domínguez
(gustavo@nodo50.org).
miembros de la Asamblea de Nodo50

REDES SOCIALES, COMUNICACIÓN Y ACTIVISMO POLÍTICO

Para explicar en qué consiste eso de *contrainformar* o qué es la *contrainformación* podríamos comenzar desgranando el discurso más elemental que nace en las redes sociales y se articula en oposición a la información convencional, es decir, el modelo de los medios de comunicación de masas (MCM). En sus fases de desarrollo originarias, esta oposición es un elemento recurrente en el imaginario de los movimientos sociales (los nuevos movimientos sociales occidentales de los sesenta y setenta o incluso en los novísimos movimientos sociales de los noventa y del siglo presente), aparece como una estructura del discurso basada en la *reactividad*, en la negación de imágenes y de modelos políticos, frente a los que se *construye una identidad compartida* y se da forma a un movimiento *autónomo* respecto al estado y al mercado. Si nos acercamos lo suficiente, apreciamos que sobre las dificultades expresivas que experimentan determinados sujetos colectivos prevalece la necesidad de definir qué dimensiones de la realidad deberían ser transformadas y, en relación con ellas, un esfuerzo por poner en pie un conjunto de *significantes identitarios propios*; palabras con las que al mismo tiempo que se identifica al adversario, se define el sujeto antagonista y se posiciona el movimiento que irrumpe en el escenario político: el anticapitalismo, los movimientos antiguerra, antipatriarcales, antimilitaristas e incluso el nihilismo punk del antitodo desde el que determinados sectores de la juventud se incorporan a la *contracultura underground* de las metrópolis occidentales de los setenta y primeros ochenta[1].

1. *«Busco en la basura /Algo mejor*
Busco en la basura /Algo nuevo
Busco en la basura /Solución»
Eskorbuto: *Busco en la Basura.*
http://www.eskorbuto.net/modules.php?name=Content&pa=showpage&pid=3

ECN
(e-mail enviado a una lista)

De casualidad, he entrado en la página de la ECN (hacía meses que no lo hacía) y me he encontrado con un triste mensaje de ultimátum en el que anuncian que, por problemas económicos —se mantienen con cuotas y al parecer deben bastante dinero al ISP— y también de «motivación», están planteándose la posibilidad de cerrar el sitio (http://www.ecn.org/).

Hace mucho que no les sigo la pista, y no he mantenido contacto con ninguno de sus admins desde el 2001, que estuve con Sandrino, el presidente de la asociación —Isole— (alguno de los antiguos, como el gran jerry cornelius, creo que ya están «jubilados»), pero me ha apenado mucho leer

En cualquier caso, y retomando el tema de la contrainformación, cabe pensar en la posibilidad de que la denominación comprenda directamente una actitud de rechazo a las prácticas y contenidos de los modelos de comunicación convencionales a los que se concibe como elementos sistémicos que in-forman: *dan forma, modelan socialmente, construyen opinión pública, generan condiciones de legitimidad dominante, son articulados y articulan a un tiempo relaciones de poder, de dominio y estructuración social*. Los primeros balbuceos más o menos conscientes de las prácticas contrainformativas definen con claridad el modelo que rechazan en sus dimensiones operativas. Lo insertan dentro de que lo que se entiende y se critica desde la Escuela de Frankfurt como *industria cultural*[2] y lo identifican como un proceso de producción de datos tecnologizado, unidireccional, jerárquico y vertical: los medios convencionales (TV, la radio o la prensa escrita) representan el modelo industrial y mercantilizado de producción cultural, apuntalado desde los falsos discursos de la objetividad informativa y la profesionalidad laboral, de cuya suma se obtendría como resultado *lo informativo, la información*. Contra ese modelo nacen las primeras prácticas contrainformativas, lo que nos da margen para pensar que en ese contexto la contrainformación nace *contra la información* concebida como mercancía, como píldora azul[3] o placebo alienante y funcional al dominio en las sociedades capitalistas avanzadas, en las que el papel de

2. Un conjunto de citas de interés sobre la industria cultural ilustra el origen del rechazo a los MCM: «Cine, radio y revistas constituyen un sistema. Cada sector está armonizado en si mismo y constituye un sistema. [...] El cine y la radio no necesitan ya darse como arte. La verdad de que no son sino negocio que les sirve de ideología que debe legitimar la porquería que producen deliberadamente. Se autodefinen como industrias, y las cifras publicadas de los sueldos de sus directores generales eliminan toda duda respecto a la necesidad social de sus productos. [...] La desconsiderada unidad de la industria cultural da testimonio de la que se cierne sobre la vida política. Distinciones enfáticas, como aquellas entre películas de tipo a y b o entre historias de seminarios de diferentes precios, más que proceder a la cosa misma, sirven para clasificar, organizar y manipular a los consumidores. Para todos hay algo previsto, a fin de que ninguno pueda escapar; las diferencias son acuñadas y propagadas artificialmente. [...] Reducidos a material estadístico, los consumidores son distribuidos sobre el mapa geográfico de las oficinas de investigación de mercado, que ya no se diferencian de las de propaganda, en grupos según ingresos, en campos rojos, verdes y azules.» (Horkheimer, M. y Adorno, Th. (2003): *Dialéctica de la Ilustración*. Madrid, Editorial Trotta).
3. En *Matrix* (la película de los hermanos Wachowski, 1999) la píldora roja despeja el cerebro de fantasías alienantes y sitúa al individuo frente a la realidad: la explotación del hombre en un mundo gobernado por máquinas. Por el contrario, la píldora azul te mantiene en el nivel de consenso, agnosia y fantasía óptimo para mantener el régimen de dominio y explotación.

esto aunque, como todo, tiene un final y no significa necesariamente algo malo si a cambio se generan otros proyectos (aunque no parece que sea así). Los sindominantes más antiguos lo saben de sobra y compartirán la triste noticia conmigo pero, para quienes lleven menos tiempo en SD, decirles que el hacktivismo político no lo inventaron los hacklabs, tampoco el zapatismo, ni siquiera M&M o el nodo50. Mucho antes del «sub», mucho antes de la Web, a finales de los años ochenta, un grupo de hackers italianos conectó varias BBSs vinculadas a centros sociales okupados y radios libres de Roma y del Nordeste y crearon la red ECN (European Counter Network), con intención europeísta (tuvo nodos en Londres y París, y en Madrid fue invitada la Agencia UPA, que declinó la oferta, los viejos del Molo/Diagonal seguro que se acuerdan). Al final la ECN se consolidó como un proyecto de BBSs italianos ——con foros muy activos y un material político impagable que algunos leíamos con avidez desde

los *media* como fábricas de *lo real* se coloca como elemento central, en la misma medida en que el desarrollo científico-técnico lo hace en el ámbito de la producción material.

Reducir esta nueva posición crítica (este incipiente modelo comunicativo) del modelo de comunicación hegemónico a su simple rechazo seria injusto y analíticamente mezquino. Pese a cuanto pueda haber de cierto en lo que acabamos de exponer, no suele ser habitual encontrar un enfoque más o menos contextualizado (al menos en lo que tiene que ver con la dimensión histórica) del análisis de las prácticas comunicativas de los movimientos sociales. Acotar y limitar lo contrainformativo a una mera reacción de oposición no aporta más que una perspectiva limitada, ángulo estrecho que nos coloca en una posición forzada, incómoda, desde la que asomarnos al modelo.

Lo cierto es que el término se ha impuesto y forma parte del imaginario del activismo mediático. En cualquier caso «contra» puede no sólo ser una reacción, una negación o un rechazo, sino también significar «diferencia», «proposición», «alternativa». En la práctica, mas allá del sentido literal del término, e incluso más allá de una enunciación consciente, *el término cobra pleno sentido y adquiere entidad propia al convertirse en la práctica comunicativa de los movimientos sociales* que, en términos de contenido, producen información desde sus propias acciones y desde sus propios discursos. Lo que en un primer momento es una *reacción organizada frente a la imposibilidad de ver satisfechas la necesidad de visibilidad de acciones y discurso en medios considerados hostiles*, pasa a convertirse con el tiempo en la construcción de un modelo [práctico] de acción comunicativa propio que pone en práctica un nuevo tipo de relación con los dispositivos técnicos de comunicación, así como una concepción nueva de la relación social como fenómeno comunicativo. Sobre la composición reticular de un conjunto de movimientos sociales, estructuras más o menos orgánicas y todo un entramado de recursos puestos en movimiento en estrategias cíclicas de protesta y acción colectiva, los medios de comunicación propios de las redes sociales se irán poniendo en marcha

módems a 2400bps, conectados a menudo mediante carísima conferencia telefónica a Italia, y que daría más o menos forma al actual ideario «hacktivista»— y, a mediados de los noventa, la red completa de BBS —cuatro o cinco nodos en otras tantas ciudades— dieron el salto a Internet, antes de que lo hiciese ningún otro proyecto político europeo de base (las ONGs, en cambio, ya estaban al loro con la vieja APC —no confundir con la ACP—). La historia de la ECN es la historia del hacktivismo político en el sur de Europa (el norte era otro mundo, CCC, los holandeses de xs4all...).

Dando un salto en el tiempo, en 1999, el único apoyo que encontramos para lanzar el proyecto SD vino de fuera del Estado español, precisamente de la ECN (aquí casi nadie veía lo de SD, «ya estaba IPANEX», que por cierto desapareció a los pocos meses). Sin la ayuda y el «modelo» de la ECN, hubiera sido más difícil y, quizá, SD no sería tal como es hoy, y quizá se parecería más a los proyec-

a través de múltiples iniciativas. Se experimentarán diferentes formatos que arrancan con las radios libres (Radio Alice en Padua en 1977, Eguzki Irratia en Euskalherria, la primera Onda Verde en Madrid), las publicaciones autónomas (la revista *Radikal* en Hamburgo, *Molotov* de Madrid o *Ekintza Zuzena* en Euskadi) hasta los servidores de Internet (TAO, Nodo50, ECN 1994), los weblogs antiglobalización (Indymedias, Seattle 1999) y la radio y televisión global (Proyecto Global Radio y Global TV, otra vez en Italia, en los primeros años de este siglo).

Son los medios de comunicación propios de los movimientos sociales, en parte herramienta «a su servicio», en parte estructura central de las redes sociales, un cruce de planos en el que suelen tomar cuerpo buena parte de las dinámicas que determinan la vida (y también la muerte) de los movimientos: su despegue, los debates identitarios, su desarrollo político, sus crisis de crecimiento, las fracturas e incluso su transformación o disolución. Así, la dimensión y la relevancia de *lo comunicativo*, de las prácticas políticas de las redes sociales y la protesta organizada en las metrópolis occidentales, colocan a la acción colectiva contemporánea en un nivel de máxima relevancia social. Es el nivel de la interacción simbólica, o acción comunicativa, que define y sobre la que toman cuerpo modelos sociales articulados sobre consensos que derivan del conflicto, frente al blindaje tecnocrático de los modelos políticos postindustriales.

tos que había por aquí, más de «servicios», tipo pangea o nodo50. De alguna manera, sinDominio fue como nos *imaginábamos* que era la ECN (realmente, luego descubrimos que no funcionaban exactamente como creíamos, pero ya daba igual). La ECN fue sin duda el proyecto que más nos influyó al principio, en positivo (cómo queríamos hacer las cosas), al igual que el nodo50 fue lo que más influyó, en negativo (en el sentido de cómo NO se debían hacer las cosas).

En fin, esperemos que la ECN pueda finalmente resolver sus problemas (de su mensaje se deduce que están intentando reagruparse los que quedan en una sola asamblea y tuvieron una asamblea presencial en Milán la semana pasada), sería una pena que un proyecto así desapareciese. En todo caso, yo he intentado ahora transmitir el significado de ese proyecto, que no se pierda la memoria de su larga historia (ahora que algunos se están dedicando a «reescribir» la historia, aprovechándo-

Contrainformación: modelo de comunicación activista

Partiremos de tres elementos para entender la contrainformación: *las agendas, el estilo de trabajo y la posición del medio en la producción informativa.*

La agenda de la protesta y el conflicto organizado

En relación a la agenda de la protesta o de la acción colectiva, el modelo contrainformativo se define en la medida que construye un conjunto coherente de los actores, causas, problemas sociales que no existen en los MCM. No es un modelo puro, no hay una taxonomía rígida. Cómo mucho podemos hablar de dos etapas. Una de *rigidez* en la que ubicamos la primera época de experiencias como *Molotov, Sabotaje*, fanzines, las primeras radios libres, el movimiento anarko-punk, o la primera «autonomía» que limita el repertorio de acción y la agenda a acontecimientos centrados en un entorno geográfica, personal y políticamente cercano, en clave de denuncia (muchas veces interna, doméstica) y de *autoafirmación*. Con la apertura de un ciclo de movilización y ampliación del campo de intervención e influencia de las redes sociales del activismo anticapitalista, a mediados de la década de los noventa se inicia una segunda *etapa de ampliación* que se define en el desarrollo de una temática propia, de *una agenda de la protesta y de los conflictos*. Si bien ésta estaba ya planteada con la aparición de los Nuevos Movimientos Sociales en los sesenta/setenta, la irrupción de medios de difusión con vocación expansiva en términos de audiencia potencial y contenidos, facilita la puesta en conexión de propuestas aisladas que articulan una agenda sólida en cada área temática. Internet es fundamental para eso y, como veremos más adelante, se convierte en *el medio* de comunicación de las redes sociales. Antimilitarismo, género, derechos humanos, trabajo, okupación, ecología, renta básica, derechos de ciuda-

se de la mala transmisión que suele haber de las experiencias pasadas) y la gran influencia que tuvo en los orígenes de SD (desde aspectos de estructuración interna, el housing, crear asociación, lista asamblea/admin, y mil detalles más que no menciono para no alargarme más de la cuenta).

saludetes

danía, software libre, solidaridad internacional, resistencia global. Al tiempo y como resultado de la ampliación del espacio de conflicto y la capacidad de respuesta política de las redes de activistas, se empieza a dar de manera más o menos sistemática una visión (o una toma de posición) de una agenda informativa desde los movimientos sociales. No sólo se tratan los temas propios, en ocasiones recogen posicionamientos concretos ante la agenda política institucional; en cualquier caso, suponen la apertura de la posibilidad de expresar perspectivas diferentes desde actores sin derecho de acceso a la comunicación convencional. Lo demuestra el debate lanzado por *Molotov* (le dedica seis números al tema) en relación al conflicto vasco y la violencia política. Un tema tradicionalmente secuestrado para la criminalización maniquea por los MCM, rescatado para la reflexión y el debate por los activistas y las redes sociales.

Estilos y organización del trabajo

Mientras que la información convencional se suele organizar sobre un modelo empresarial jerárquico (selección temática y enfoques desde la dirección, redacciones profesionales, subvención por medios propios de la empresa y publicidad), las redes sociales incorporan a sus experiencias comunicativas las pautas de relación/organización que le son propias. Se soporta en su base social (los movimientos sociales), sobre un modelo de cogestión económica no empresarial, gestión colectiva y responsabilidades compartidas: asambleas, flujos horizontales de información y autogestión que cambia el mundo de la direccion/redacción por el de la organización colectiva no jerárquica. Antes de la irrupción de las redes telemáticas como territorio de acción comunicativa de las redes sociales, la precariedad es un denominador común, dada la desproporción que imponen medios como la radio, la TV o la prensa entre la capacidad colectiva de generar discurso y la posibilidad real de difundirlos en los diferentes formatos disponibles.

DEL NARROWCASTING AL NETCASTING*

Net.radio es un término extraordinariamente inadecuado para el conjunto híbrido de tecnologías y estéticas novedosas que configuran la realidad actual del sonido en la red. Por un lado, existe una multitud de directorios de sonido *on-line*, que se asemejan más a bases de datos que a una experiencia digital de radiofonía, y su discutible calidad no aporta mucho en sentido contrario. Por otro lado, si bien los *live-streams* (formatos de sonido de alta compresión que se reproducen a medida que se descargan) introducen una cierta calidad a la radio en la web, no es suficiente para acallar la crítica más radical: la radio digital carece del carácter esencial de la radiofonía, su democrática masividad.

* Basado en un texto original de Gisela di Marco.

Los canales y las direcciones

Al mismo tiempo, encontramos que la pretensión de visibilizar discursos insurgentes, silenciados o demasiado precarios como para salir a la luz, va acompañada en algunos casos por la intención de provocar un «cambio en la estructura» general que caracteriza a los procesos informativos: con el propósito de abolir la mediación en el proceso que arranca en *la emisión* y termina en *la recepción*, se da forma a la figura del *activista reportero* que construye *la información* mediante su actividad política. Sin embargo, esta declaración de intenciones se cruza en su propia argumentación con una paradoja: se pretende el fin de la mediación entre la noticia y el lector final, desmontando así la base de la manipulación periodística convencional; el medio dejará de ser un obstáculo en el camino hacia la verdad parcial, en una pequeña concesión de sinceridad al público afín, que sin embargo debe seguir percibiendo determinados filtros ideológicos a partir de los cuales es fiel a la línea editorial de *su* medio. Al mismo tiempo, se reclama el fin de la objetividad periodística (por falaz), entendiendo que el medio es político (subjetivo por definición) y de ello se debe dejar constancia. La tautología está servida: si eliminando la mediación nos acercamos a la objetividad y de la misma manera rechazamos la objetividad en tanto que defendemos el compromiso político del medio, este discurso (ideal) de algún proyecto contrainformativo se hace impracticable, mera abstracción teórica o modelo irrealizable.

Internet y la bomba contrainformativa

Ya hemos sugerido que Internet es el medio paradigmático de la contrainformación. Hasta su irrupción podríamos hablar de su prehistoria, del *underground* del que ha salido para convertirse en el medio y el mensaje de las redes sociales. Desde las redes telemáticas la contrainformación se dignifica (rompe el estigma de la marginalidad), se hace visible (uno de los objetivos de los movimientos sociales) y redimensiona su relación con los medios de comunicación de masas con los que convive en la red en igualdad de condiciones técnicas.

En este sentido, se ha aplicado a las experiencias de radiodifusión *on-line* la denominación de «narrowcasting», en oposición al término «broadcasting» con el que las naciones de habla inglesa se refieren a la prensa escrita y a las transmisiones por aire de radio y televisión. Con este neologismo se pretende demostrar que la naturaleza elitista de la Internet actual, orientada a la personalización y a los mercados de nicho, es fundamentalmente incompatible con la esencia universalista de la radiodifusión.

Hacia un espacio propio: el netcasting

Estas discusiones revelan que el nuevo espacio no está aún bien definido y que son más los interrogantes que genera que las respuestas que ofrece. Es necesario encontrar la naturaleza específica de la radiodifusión digital, para no configurarla solamente como una versión alternativa a la radiodifu-

Universos soñados

Los primeros discursos sobre el ciberespacio lo presentaban como un lugar de ausencia de control, donde el Estado podría apagar máquinas o desmontar redes, pero en el que sería técnicamente imposible la regulación, la monitorización de identidades y el control de la administración. En el imaginario de los primeros hackers y sobre todo en el imaginario de los primeros (ciber)activistas, este discurso —que se consolida como el que define el ideal técnico y a la vez social con el que trabajan la mayoría de los movimientos sociales en la red— cruzaba elementos a medio camino entre lo deseado y lo real. Es una construcción ideal cuyas referencias reales se soportan sobre el diseño de la Red95[4] de la Universidad de Chicago allá por 1996: una red que permite la libertad de acceso y garantiza el anonimato en todo el proceso de comunicación. La realidad demuestra que el ciberespacio «es como es» y no necesariamente como nos gustaría que fuese. El carácter irregulable o no de la Red depende de su arquitectura y de su

4. El modelo de Red95 de la Universidad de Chicago se caracteriza por:
   – *Inexistencia de credenciales obligatorias.* Es lo mismo que garantizar el anonimato total de las personas que acceden a la red.
   – *Inexistencia de cabeceras en el texto de las aplicaciones de red que permitan control sobre el tráfico de datos.* Se desconoce qué tipo de información circula por la red, con lo que se impide la zonificación o delimitación de áreas de la red en relación a los contenidos que circulen o de las identidades que accedan.
   – El punto primero y el segundo son el resultado de la utilización de protocolos de red en estado puro, es decir, tal como fueron definidos políticamente por los hackers creadores de Internet en la década de los setenta. Es *TCP/IP en estado puro*, es la Internet diseñada en el mundo académico y que se mantiene congelada como tipo ideal de red en el imaginario *hacker* y libertario de mediados de los noventa.

   La Red95+ es el modelo de Red de la Universidad de Harvard. El contramodelo de Chicago. Es la pila TCP/IP más un nivel superior de protocolos que hacen posible:
   – Control de identidades.
   – Control de encabezados de aplicaciones de red.
   – Delimitación de la red por zonas accesibles en función de identidad/contenidos.
   – Posibilidad de regulación del acceso/uso de la red.

   Hay, pues, una arquitectura de control superpuesta a la Red95, protocolos que se añaden al TCP/IP. Como vemos, la arquitectura de Harvard estaba pensada para controlar el acceso y la de Chicago para facilitarlo. Son dos modelos que se diferencian en función de su capacidad reguladora de la conducta. La diferencia entre ambas arquitecturas se basa en las diferencias de código. Por eso no se puede hablar de una naturaleza esencial de la Red, sino del software que la hace posible.
   (Lessig, L.: *El código y otras leyes del ciberespacio*. Madrid, Taurus Digital, 2001).

sión *on-air*. Londres ha sido especialmente activa en este nuevo campo de acción. Las experiencias están enfocadas principalmente al underground, y abarcan una gran cantidad de proyectos y productos culturales que circulan por los canales no oficiales, y que se han demostrado decisivos en la difusión de las tendencias musicales más recientes.

Uno de los popes de esta corriente es Heath Bunting, fundador del portal Irational, desde el cual se puede acceder a la plataforma Pirate Scanner. Se trata de una estación celular que rastrea las frecuencias de las radiotransmisiones «pirata» londinenses y las acerca a la comunidad global. Está vinculada con alrededor de 75 radios «pirata», activas principalmente en la noche y los fines de semana, especializadas en tipos de música muy específicos: desde los productos de la nueva cultura DJ digital hasta el reggae o el revival.

código[5]. Su evolución parte de un modelo ideal «irregulable», en movimiento hacia uno cada vez más sometido a controles y monitorización.

El medio paradigmático de la contrainformación

Con independencia de ello, la red es hoy, tal como ha evolucionado en los últimos 25 años, el territorio por excelencia para las prácticas comunicativas y el activismo mediático de las redes sociales. La amplitud y flexibilidad de su soporte técnico, su independencia respecto a los sistemas operativos y su universalidad creciente, en tanto que producto de consumo y acceso de masas, la coloca en el centro de todos *los medios* y la convierte en *el medio* sobre el que comienzan a superponerse las técnicas predigitales. El mundo de la publicación sucumbe o se recicla en la red y la radio, sin dejar el ámbito de las frecuencias tradicionales, se lanza a la emisión digital que le garantiza a un coste mínimo una cobertura planetaria en la que por primera vez se hace efectivo el eslogan político de la mundialización: *acción local de dimensión global*. El proyecto Red con Voz[6] es un ejemplo singular que encarna esta dinámica de superposición de medios tradicionales y redes digitales. En un sentido mínimo podríamos decir que Red con Voz es un conjunto o repositorio de ficheros de audio que contiene entrevistas, reportajes y programas periodísticos que un colectivo de activistas elabora a diario y coloca en la red. La práctica y su uso cotidiano lo redefine y nos da una dimensión mucho más interesante. Los ficheros de audio son descargados por decenas de radios libres, locales o comunitarias que los reproducen en su entrono radiofónico local y analógico. Su ámbito de influencia es todo el Estado español y buena parte de Latinoamérica, habiendo conseguido poner en funcionamiento una retícula comunicativa en la que articulan técnicas y concepciones mixtas sobre la información y la comunicación popular.

5. Lessig, L. (2001).
6. http://www.redconvoz.org.

Ésta y otras experiencias similares sitúan a la radiodifusión digital en un espacio nuevo y propio, denominado netcasting. Fuera de la dicotomía broadcasting/narrowcasting, traslada el circuito underground local a la telaraña de la globalización, en un proceso de universalización que trasciende incluso los logros de la radiofonía tradicional.

En la misma línea, la comunidad artística ha comenzado a experimentar con las posibilidades del medio, y ha integrado esa exploración en el contexto de especulación filosófica más general. Alimentada por los discursos de la ciencia, el arte y la filosofía, se intenta dilucidar las propiedades aparentemente monádicas del dato sensorial, pero con un interés especial en la convergencia entre formato y estética. Su objetivo es la integración de las prácticas de radiodifusión digital con los discursos especulativos sobre el arte, que con demasiada frecuencia tienden hacia la mistificación de lo abstracto.

Un medio globalizado

Podríamos quedarnos en la superficie y defender las evidencias democratizadoras del medio en la línea legitimadora del nuevo capitalismo postindustrial abanderada por Castells. Cierto es que la propia estrategia del capitalismo marca un línea de penetración y crecimiento de las redes telemáticas y del acceso a Internet que avanza en una dirección clara: hacer de la Red y todo lo que ella trae consigo un fenómeno de consumo masivo y un nuevo territorio para el mercado y la legitimación ideológica de la *sociedad red*. Además, y a pesar de la tendencia global y el espectacular crecimiento (se calcula que en diciembre de 1995 los habitantes del planeta con acceso a Internet apenas llegaban a 16 millones; en mayo del 2002 llegaban a los 580[7]), el acceso, el uso y la actividad política y comercial en Internet no dejan de ser un fenómeno técnica, cultural y políticamente eurocéntrico, occidental y urbano (dejando de lado los polos «desarrollados» del Norte y el Sur del continente, sólo 1 africano de cada 250 tiene acceso a la red; en Europa 1 individuo de cada 2[8]), como lo son las categorías burguesas de las que nacen la Declaración Universal de los Derechos del Hombre, el marxismo, la propiedad intelectual o el Estado del bienestar. La hegemonía global del capital que atraviesa todas las dimensiones de la vida los convertirá en paradigmas universales, de la mano del mercado y el poder militar global. En esa dimensión, en ese contexto, entendemos la irrupción de las redes sociales sobre las redes telemáticas y la adopción de Internet como terreno para la acción comunicativa de los movimientos anticapitalistas a nivel mundial. Con independencia de la desproporción en el grado de desarrollo regional de las tecnologías de la comunicación, éstas se imponen como modelo global, de la misma manera que el capital lo ha hecho por encima de las resistencias económicas, políticas y culturales en los últimos 200 años.

7. NUA y Atlas de *Le Monde Diplomatique*: http://www.nua.com/surveys/how_many_on-line/world.html.
8. NUA: http://www.nua.com/surveys.

Esta empresa está originando una nueva forma de performance colectiva en vivo, cuyas raíces se encuentran en experiencias estéticas y técnicas con tecnologías arcaicas.

HACIA LA CONFORMACIÓN DE UNA COMUNIDAD VIRTUAL

El amplio espectro de productos de net.radio, que abarca desde las actividades independientes del aficionado y la radio «pirata», hasta las prácticas ya institucionalizadas de las emisoras comerciales y las instituciones políticas y artísticas, se está cuestionando su organización.

Partiendo de la idea de que el intercambio de experiencias permitiría el desarrollo y la difusión de métodos de organización y financiamiento, dos agrupaciones alemanas organizaron en 1998 el Primer

Un medio que redefine el modelo

No decimos nada nuevo, pues, si definimos Internet como un medio facilitador y democratizante, dado su diseño técnico (y político) actual, que garantiza el acceso masivo a muy bajos costes, la visibilidad sin apenas recursos técnicos y una relación mucho más desproporcionada (por una vez a favor de lo social frente al modelo clásico de los medios de comunicación unidirecciones y empresariales, como son la prensa, la radio y la televisión) entre la necesidad de inversión (mínima) y la rentabilidad mediática que se obtiene de ella (alta). En este sentido, la red funciona entre las plataformas sociales como una de las herramientas que facilitan un proceso de generación de agendas. El peso cada vez más relativo de lo territorial refuerza la conexión de realidades y resistencias (similares o no), redimensiona la relación tiempo/espacio (y con ello la noción de *frontera*) y sienta las bases para un nuevo modelo comunicativo definido por la horizontalidad y bidireccionalidad del flujo de datos (y, por lo tanto, la democratización del proceso de comunicación): la red telemática y sus dispositivos técnicos diseñados en su momento con una clara intencionalidad política, no sólo atrae a las redes sociales, sino que genera dinámicas reticulares, refuerza las ya existentes y crea las condiciones para el nacimiento de nuevos sujetos sociales que superen los modelos organizativos y de toma de decisiones clásicos, como son el modelo partido, modelo empresa, modelo sindicato o e incluso el modelo (ya clásico) de los movimientos sociales.

Encuentro Internacional sobre Proyectos Experimentales de Radio en Internet, denominado Net.radio Days. Se trata de la agrupación Mikrov, abocada al desarrollo de culturas mediáticas en Berlín, en colaboración con Convex.tv, otro grupo local dedicado a la net.radio. Los miembros de más de 20 agrupaciones similares internacionales se reunieron *on-line* en una transmisión ininterrumpida durante seis días. A éstos se sumaron otras actividades como talleres, presentaciones y discusiones públicas, y parte del encuentro se transmitió también *on-air* (a través de estaciones radiofónicas públicas). La intención era complementar los espacios radiofónicos tradicional y digital, y vislumbrar cómo debe ser la net.radio, cómo puede enriquecer a la radiofonía tradicional y cuáles son sus expectativas para el futuro.

Referencias:
The Pirate Scanner, Londres: http://www.irational.org
Radioqualia, Sydney: http://www.radioqualia.net
Mikro e.v., Berlín: http://www.mikro.org
Convex.tv, Berlín: http://www.art-bag.net/convextv
Otros proyectos: http://xchange.re-lab.net/urlf.html

Microhistoria de la contrainformación en el Estado español

Este apartado no desarrolla una cronología de la contrainformación en el Estado español; no es un apartado exhaustivo y no recoge todos los eventos que podrían ser dignos de mención. Nos limitaremos a constatar la existencia de al menos dos grandes fases en el desarrollo de los medios de información y comunicación al servicio de los movimientos sociales, en torno a lógicas estéticas, económicas, políticas y sociales concretas. No se trata de una síntesis descriptiva de casos, sino de modelos comunicativos representados por hitos, que son los que aquí recogemos.

• **Los medios escritos** son posiblemente los más significativos de la primera etapa. El modelo fanzine, sujeto a una fidelidad estética casi tan precaria como las condiciones económicas en que se edita, será el protagonista indiscutible de esta fase preliminar.

En este período encontramos varios títulos[9]: *Penetración*, que surge en 1985 como el germen del mítico *Sabotaje*, o *El fuego y la piedra* en Madrid, y, en líneas similares, *Resiste* en Vitoria, *Ekintza Zuzena* en Bilbao o *La Lletra A* en Barcelona, en la categoría de pequeñas publicaciones que llegaron a editarse como revistas.

Como modelo de transición entre este primer grupo de fanzines y lo que denominaremos el salto a las redes, encontramos *El Acratador*[10] de Zaragoza, que nace en 1989 y en marzo de 1995 ya tienen espacio web en Internet, desde el que se vuelca el boletín que editaban sobre papel. Al mismo tiempo, emiten dos programas de radio semanales en Radio La Granja y Radio Topo y efectúan intercambios de material, información y publicaciones con cerca de 300 colectivos del Estado español, Europa y América[11].

9. Citado en Casanova, G. (2002): *Armarse sobre las ruinas*. Madrid, Potencial Hardcore.
10. http://www.geocities.com/CapitolHill/4858/acrata.html.
11. http://www.geocities.com/CapitolHill/4858/48/acralc.html.

SINDOMINIO.NET: POR UN DOMINIO ANTAGONISTA EN LA RED

La idea del proyecto sindominio es tener una máquina conectada las 24 horas del día a Internet, y visible por tanto desde cualquier lugar del mundo con acceso a la red de redes. La máquina albergará un dominio virtual —sindominio.net—. Un dominio es una dirección fija en Internet representada por un nombre que cualquier máquina desde cualquier parte del mundo puede localizar, por ejemplo para enviar un correo electrónico o para solicitar ver el contenido de una página web.

Esa máquina tendrá instalado GNU/Linux, que es un sistema operativo libre desarrollado de manera cooperativa y no mercantil en los últimos seis años por miles de programadores y usuarios que lo ponen a prueba, lo traducen a diferentes lenguas, escriben ficheros de ayuda o desarrollan

En todo el tránsito entre las dos fases de las que hablamos, pero no en todos los niveles de proyección posible (no en radios, no completamente en Internet), *Molotov* nace, en 1986, como un fanzine a cargo del colectivo KAOS en la Facultad de Ciencias Políticas y Sociología de la UCM. En 1988, el proyecto lo retoman gentes vinculadas a la Asamblea de Okupas de Madrid, con un producto gratuito de pocas páginas que, con el apoyo de la AOM, se distribuye en Barcelona, Vitoria y Bilbao. El salto al formato periódico lo darán en 1992, en un intento de abandonar la estética punk de los primeros números. En 1994 se fusiona con la agencia de noticias UPA, que nace en 1988 en Madrid, tras lo cual el proyecto se diversifica en varios frentes: una agencia de noticias, el periódico *Molotov*, que se mantiene como tal hasta 2003; y un colectivo político que funciona, entre otras cosas, como gabinete de prensa de Lucha Autónoma (1990-1997)[12].

Molotov será pionero en la elaboración del concepto político de contrainformación, que se convierte en el paradigma de las herramientas políticas de la era pre-Internet, aunque acabe permeando el trabajo de numerosos proyectos actuales. Así, en doble sentido —herramienta (supuesta desaparición de la mediación social entre emisor y receptor, que se funden en uno) política (en la medida en que desaparece la pretendida objetividad del periodista y se acota el proyecto en parámetros ideológicos identificables)— la contrainformación sirve, a la vez, para legitimar discursos insurgentes ocultados por la dinámica de los grandes medios y para remover las «estructuras» con un periódico no convencional en las formas y en los contenidos, que pretende ser progresivamente expansivo, siguiendo la metáfora de las capas de una cebolla.

– *La contrainformación debe dar voz a los sin voz. [...]*
– *[...] debe buscar una globalización así como una contextualización de la información [...].*

12. Wilhelmi, G. (1998): *Lucha Autónoma*. Madrid, Traficantes de Sueños.

«paquetes» (Debian) para facilitar su instalación. El sistema operativo es fundamental (sin él un ordenador es como una caja de zapatos, no puede ni arrancar), porque de él depende que se puedan usar herramientas libres o no. Sobre nuestro Linux funcionarán toda una serie de servicios: servidor de páginas web, servidor de correo electrónico, de listas de correo, de news, buscadores, agencia de noticias, mirrors... No hay más límite que el de nuestro conocimiento, que el de nuestra imaginación y ganas de aprovechar esos recursos: quien participe en sindominio tendrá plena disponibilidad de la máquina.

Linux permite una administración remota completa y hace completamente indiferente la localización física de la máquina. La máquina será administrada remotamente, por el momento desde Barcelona y desde Madrid a través de SSH (Telnet seguro).

– *La información como bien de uso y no de cambio. [...].*
– *La contrainformación debe estar posicionada y dotada de contenido. Frente a la ideología del poder, no podemos pretender ser neutrales ni objetivamente imparciales.*[13]

Durante el período 2003-2004, *Molotov* emprende el «Gran Salto Adelante»: un año de reflexión en torno al proyecto, del que surge en otoño de 2004 la propuesta de un nuevo periódico: *Diagonal*. Un quincenal con una tirada arriesgada (15.000 ejemplares) y un formato algo más alejado de los vínculos identitarios previos, en busca de públicos cercanos, pero más amplios:

> *Nuestro modelo comunicativo tiene como rasgo fundamental la búsqueda de la horizontalidad, que entendemos como intercambio permanente, construcción colectiva o comunicación realmente participativa. Ser un periódico «desde los movimientos sociales» implica establecer con los colectivos y sujetos que los componen esos mecanismos. [...] Esta red se ampliará a los medios de comunicación alternativos y contrainformativos del Estado y poco a poco a los de otros países, apostando por la creación de infraestructuras comunes que faciliten el trabajo y permitan acercar realidades lejanas expresadas por quienes las viven.*[14]

En la actualidad, consolidados como revistas y periódicos los viejos fanzines de la contrainformación inicial, nos veremos obligados a reconocer cierto declive del fenómeno, en gran medida atribuible a Internet: desde el punto de vista del editor, la Red abarata costes en la emisión de boletines, con un soporte ahora unitario en el que no se invierte en distribución. La visibilidad y el alcance redimensionan como con-

13. Casanova, G. (2002): *Armarse sobre las ruinas*. Madrid, Potencial Hardcore, p. 137.
14. http://www.diagonalperiodico.net/2.htm.

PARA QUÉ SINDOMINIO

Como se sabe, existen en el Estado español cuatro nodos —Nodo50, Pangea, Xarxaneta y Eusnet— que han apostado desde el primer momento por ofrecerse como proveedores de conexiones a Internet para los colectivos, organizaciones y personas del ámbito de la izquierda social y política, que pueden así publicar sus contenidos sin depender de un servidor comercial o institucional. En ese terreno han hecho un gran trabajo, dando acceso a Internet y permitiendo su visibilidad a multitud de organizaciones y colectivos, fundamentalmente del ámbito de las ONG. Apostar por ofrecer conectividad es una opción: pero no es la única opción. Porque, a nuestro parecer, la tecnología Internet tiene una potencia que sobrepasa en mucho la posibilidad de publicar contenidos más o menos alternativos o críticos, y nos ofrece de lleno la posibilidad de la comunicación horizontal y de inter-

ceptos, en el momento en que se anulan las trabas espacio-temporales cruciales para procesos militantes cada vez más descentralizados. Desde el punto de vista del receptor, encontramos una generación que recibe información y se educa políticamente en la Red, en cuanto que la contrainformación se vuelve cada vez más telemática.

• Por lo que respecta a las radios libres y comunitarias, nuevamente distinguiremos una etapa inicial, en los primeros ochenta, en la que encontramos ejemplos históricos, como Eguzki Irratia en Euskadi, la primera Onda Verde en Madrid o la mítica Radio Vallekas (nace en 1985, de mano de una asociación radiodifusora y estrechamente vinculada al movimiento vecinal vallekano), Radio Topo (Onda Vorde en sus orígenes, 1986-1989; en 1993 resurge como tal, después del cierre gubernativo de la primera, con parte del equipo personal y material) en Zaragoza o Radio Klara Lliure i Llibertària (en el invierno de 1980 se forma el primer núcleo promotor de lo que en 1982 será la primera emisión de la radio, cercana al movimiento libertario de Valencia), por citar algunas.

Se rigen, en la primera fase, por el «Manifiesto de Villaverde», de 1983, que define a las radios libres por:

– su funcionamiento no profesional y no lucrativo;
– su funcionamiento autogestionario;
– autonomía frente a los grupos políticos, económicos, publicitarios...;
– su funcionamiento al servicio de una comunidad local;
– la lucha contra el monopolio y la centralización de la comunicación.[15]

Con hitos centrales en torno a la campaña anti-OTAN, la guerra del Golfo en 1991 y las huelgas generales de diciembre de 1988 y enero de 1994.

15. http://sindominio.net/radiotopo/toporadioslibres003.html.

conectar redes, proyectos, luchas, deseos y realidades. Es decir, no sólo es un medio, una herramienta para difundir nuestros mensajes que en otros medios son totalmente silenciados, sino que en sí misma permite llevar a cabo prácticas políticas que hasta ahora sólo precariamente y a nivel local era posible. La red elimina el factor tiempo y espacio a la hora de coordinarse o de impulsar debates, campañas o acciones conjuntas, por ejemplo. Nos permite poner en concierto la diversidad y experimentar formas de cooperación totalmente inéditas hasta ahora.

¿QUÉ PRETENDE SINDOMINIO?

Sindominio pretende sumergirse en todo ese multiverso que se mueve por la red, aportar lo que pueda a ese espacio de cooperación y de comunicación, y también de conflictos y luchas, donde ya

Será en la última época, ya en los noventa y primeros años de este siglo, cuando nos encontremos con la adopción de nuevas fórmulas organizativas, en paralelo a la incorporación de nuevas tecnologías. La Unión de Radios Culturales de Madrid (URCM) incorpora desde 1995 a diez radios[16] federadas y tres asociadas y mantiene todavía una agencia de noticias (ANIA[17]), ahora ya bajo soporte digital. De su mano se empieza a extender el uso de K-Jabata, un software (libre) que permite a las radios la planificación de las parrillas informativas y compartir ficheros de audio.

Por su parte, la Red con Voz[18] trabaja desde 2003 en la articulación de un proyecto europeo que ha puesto en sus manos un satélite con capacidad para emitir veinticuatro horas en parte de Europa y América Latina, y en el que tratan de integrar, a través de los Consejos Mancomunados de Redacción (COMADREs), a actores sociales representativos de cada área temática abordada, a fin de que sienten las prioridades informativas.

También el salto a Internet lo han protagonizado algunos históricos de las radios libres, como Radio Klara[19] desde Valencia, que no sólo emite en soporte digital, sino también vía satélite.

• **Finalmente, Internet.** Mantendremos una distinción un tanto forzada, pero de cierta utilidad analítica, a la hora de describir la secuencia de la implantación de los usos políticosociales de las NTIC en el Estado español. Diferenciamos entre:

a) Contrainformación y, dentro de la misma, entre *webs de colectivos* y *colectivos de contrainformación*. Para ser rigurosos, la propia dinámica de implantación de Internet y los costes de conexión favorecieron desde el principio la aparición de los

16. Almenara, Cigüeña, Enlace, Fuga, Jabato, Paloma, Ritmo, Vallekas, Alternativa y Merlin.
17. Agencia de Noticias de Información Alternativa: http://ania.eurosur.org.
18. http://www.redconvoz.org. Depende del Centro Comunicación y Democracia, que lleva operando desde 1998: http://www.redconvoz.org/que.php#que_red.
19. http://www.radioklara.org.

hay puestos en pie proyectos autogestionados de unas dimensiones extraordinarias, como es por ejemplo el que ha dado lugar al sistema operativo GNU/Linux. Necesitamos una máquina Linux donde probar con herramientas libres y cooperar, investigar e intercambiar conocimientos con la comunidad linuxera, una verdadera anomalía en el estratégico campo del software.

Sindominio también pretende coordinarse y cooperar a fondo con proyectos similares al nuestro, como es el caso de la ECN, donde la relación y la implicación entre el proyecto telemático y las realidades que se coordinan en él es total y donde la cuestión de competir con otros servidores en servicios, tarifas, etc., es superflua porque no ofrecen conectividad: necesitamos que quien participe en sindominio no sea un cliente o un simple usuario a quien hay que dar un servicio a cambio de su dinero. Sindominio es un proyecto militante y debe sostenerse con aportaciones, sin asalariados o

grandes proyectos contrainformativos, antes que las pequeñas webs individuales de ciertos grupos: la precariedad económica y técnica de los mismos les lleva a delegar parte del trabajo informativo en medios estructurados.

Por orden cronológico, encontramos:

– Nodo50[20]: nace en 1994 como una BBS para el Foro «Las Otras Voces del Planeta»; permanecerá dentro de SODEPAZ, como un área telemática propia hasta 1999, año en que se independiza como proyecto autónomo. Es un proveedor de servicios de Internet para organizaciones políticas de izquierda y, a la vez, un colectivo de contrainformación. En la actualidad aglutina a 850 organizaciones. Entre sus *momentos estelares* podemos citar el cierre de la web de la Asociación contra la Tortura[21] por la Agencia de Protección de Datos, en marzo de 2000. Durante el semestre de 2002, el informe *Vigilando a los Vigilantes* [22] evidencia el espionaje policial al que son diariamente sometidas las webs de Nodo50 y, con él, la posibilidad de establecer mecanismos de contraespionaje.

– Sindominio[23]: se forma en 1999 tras la salida de parte de sus miembros de la asamblea de Nodo50. Se plantea como un intento de facilitar el acceso general a procesos de inteligencia colectiva, como una apuesta decidida por el software libre y parte de la ruptura con la idea de «dar servicios»[24], todo ello en torno al objetivo último de constituirse en un referente telemático de la autonomía y de los centros sociales okupados. Una de sus primeras apuestas será la Agencia en Construcción Permanente (ACP): «un servicio de noticias en tiempo real, con la peculiaridad de que no sólo se pueden colocar y leer noticias, sino que se pueden comentar, ampliar, debatir»[25]. Tras algunos problemas es cerrada. En enero

20. http://www.nodo50.org.
21. http://www.nodo50.org/actortura.
22. http://losvigilantes.nodo50.org.
23. http://sindominio.net.
24. Padilla, M. (1999): «Por qué Nodo50 ha dejado de interesarme», en http://sindominio.net/biblioweb/telematica/nonodo50.html.
25. FAQ de Sindominio: http://sindominio.net/faq.php3.

personas que deban dedicarse a tiempo completo. Ello obliga a generar una cultura diferente, menos pasiva, en el uso de los ordenadores entre la gente que se mueve con criterios alternativos en otras cuestiones, romper con la idea de «dar servicios», dotar de elementos de juicio para situarse críticamente ante los usos banales, comerciales o despolitizados de Internet y aprender todo lo bueno de las comunidades virtuales, pero sin quedarnos en el ciberespacio.

Pero sobre todo sindominio sólo es viable e interesante si se utiliza como un recurso del movimiento antagonista. O sea, como herramienta de la comunicación alternativa y para la coordinación y cooperación de aquellos colectivos y personas que luchan por la autogestión y promueven la autonomía de lo social en los ámbitos más diversos.

Para entrar en contacto con sindominio.net, podéis hacerlo a través de la Kasa de la Muntanya,

de 2002 se abre IndyACP[26], el nodo de Madrid dentro del proyecto Indymedia, con algunas particularidades dentro del modelo, entre otras, la polémica figura de un colectivo editorial, más cercano en su dinámica a lo que es una redacción «convencional», y que choca con la concepción horizontal de la contrainformación que cuestiona la figura de consejos de redacción o similares.

> *Indymedia Madrid se reserva el derecho a orientar ese caos que entra por la ventana de publicación abierta, a filtrarlo, a extraer lo que su comunidad de usuarios juzga relevante, a separar en fin, la señal del ruido. [...] quiere salir del gueto, romper las casillas, superar las discusiones estériles que lo pueblan y entretienen, evitar los vanos ejercicios ideológicos (en el sentido de «falsa conciencia»).*[27]

– La Haine[28]: *«Proyecto de desobediencia informativa»*. Destacado precisamente por el carácter semiclandestino de su estructura organizativa, de la que no se manejan demasiados datos, se desglosa en varias entidades agrupadas en dos niveles:

- Los nodos territoriales de La Haine Red: Barcelona (agosto de 2002), Madrid (octubre de 2002), Euskal Herria (julio 2003), Valencia (septiembre 2003), Sevilla (octubre 2003), León (marzo 2004) y Granada (marzo 2004). Fuera del Estado, México (octubre 2003).
- Los nodos virtuales, con Cartelera Libertaria[29] (que se crea a finales de 2001, se disuelve tras la creación de Contrainfos Valencia y vuelve a aparecer integrándose en La Haine en octubre de 2003), Jotake[30] (Kontrainformazio Abertzale

26. http://acp.sindominio.net.
27. http://acp.sindominio.net/about.shtml.
28. http://www.lahaine.org.
29. http://www.carteleralibertaria.org.
30. http://www.jotake-lahaine.org.

del Ateneu de Cornellà, del Ateneu de Viladecans, de InfoUsurpa, de Contr@infos, de Zitzània, de UPA-Molotov [reconvertido en el actual *Diagonal*; N. del ed.] o del Área Telemática del CSOA El Laboratorio. También a través de la siguiente dirección de correo electrónico: sindominio@ecn.org.

Iraultzailea, creada en septiembre de 2003) y Clajadep[31] (Coordinadora Latinoamericana y Africana de Juristas, Cientistas Sociales y Grupos Marginados por una Alternativa Democrática y Popular, que existe desde 1987 y que se integra en La Haine en 2003).

- Rebelión[32]: más volcado sobre América Latina, mantiene un formato propio de periódico electrónico de alto nivel, que le reporta cuantiosas entradas diarias; se mantiene alejado de la fórmula contrainfomativa clásica, haciendo énfasis en las colaboraciones de grandes firmas alternativas. Nace en septiembre de 1996 en Madrid.
- Otros igualmente relevantes, a los que mencionaremos brevemente: Kaosenlared[33] (surge en julio de 2001, en torno a las actividades de Barcelona 2001 contra el BM, dentro de Radio Kaos, que nace en 1987 en Terrassa), Alasbarricadas.net[34], Poesía Salvaje[35] (aunque vinculada a aspectos culturales, fue todo un dinamizador en el mundo de la contrainformación), A-infos[36] (un proyecto integrado por activistas internacionales de carácter anarquista) y un largo etcétera.

Entre las experiencias de coordinación de estos medios, destacaremos las Jornades sobre Mitjans de Comunicació i Contrainformació de Terrassa, en noviembre de 2002 (de carácter regional y local, en las que participan entre otros Anta.info, Kaosenlared.net, Radio Kaos y Radio Tsé-tsé, y la distribuidora I Love Pili). También señalaremos el Tercer Encuentro Estatal de mayo de 1998 en Zaragoza o el cuarto, que tiene lugar entre el 16 y el 18 de abril de 1999 en Madrid[37].

Con la intención de articular una propuesta de trabajo conjunto durante el semestre de enero a junio de 2002, encontramos la creación de una

31. http://clajadep.lahaine.org.
32. http://www.rebelion.org.
33. http://www.esfazil.com/kaos.
34. http://www.alasbarricadas.org.
35. http://www.poesiasalvaje.com Se integró dentro de Barriodelcarmen.net: http://www.barriodelcarmen.net/poesiasalvaje.
36. http://www.ainfos.ca/ca.
37. http://www.nodo50.org/contrainfos.

¿QUÉ ES NODO50?

Somos un proyecto autónomo de contrainformación telemática orientado a los movimientos sociales, una asamblea independiente que proporciona servicios informáticos y comunicativos a personas, grupos y organizaciones de izquierda, un servidor de Internet en el que confluyen voces antagonistas y alternativas desde un amplio espectro político; un centro de encuentro, difusión y contrainformación para l@s sin voz, disidentes, subversiv@s, utópic@s y desencantad@s... nada más y nada menos.

¿CÓMO NACIÓ NODO50?

Una brevísima biografía. Vinimos al mundo como instrumento de comunicación del «Foro 50 años

Coordinadora de Medios Telemáticos, con motivo de la campaña «Contra la Europa del Capital y la Guerra». Ésta integra a varios colectivos, como Nodo50, La Haine, Indymedia Barcelona, Rebelión, Pangea[38] o Griesca[39], entre otros, que crean una web (http://www.antiue.net)[40] destinada a concentrar, mediante un sistema de sindicación de los titulares de cada una de esas páginas relacionados con el semestre, toda la información de las protestas. Aunque el proyecto no termina de arrancar, se crea un anillo (un sistema de enlaces a todos los proyectos en cada una de las páginas) que en muchos casos todavía se mantiene.

Otros proyectos se han concretado bajo la forma de propuestas de debate, como el que organizan La Haine y UPA-Molotov en la página web de la primera, bajo el título de «Los límites de la contrainformación y la comunicación de masas»[41], en el que participaron activistas de quince colectivos entre diciembre de 2003 y los días en que se escribió este artículo, en septiembre de 2004.

Por último, se convocan las Primeras Jornadas de Análisis y Reflexión del Colectivo de Contrainformación Kaosenlared[42], que tuvieron lugar en Terrassa en julio de 2004. Al mismo tiempo, y como encuentros concretos de los nodos del Estado de la Red Indymedia, señalaremos el encuentro de Indymedias que se desarrolló en Iruña con motivo del cuarto hackmeeting[43].

Finalmente, y aunque con carácter más específico, mencionaremos las áreas de comunicación de las campañas regionales constituidas con motivo de las contracumbres durante la presidencia española de la UE, en 2002. El área de comunicación del Foro Social de Sevilla[44] fue un importante nodo dinamizador de

38. http://www.pangea.org, Un proveedor de servicios de Internet que opera en el ámbito catalán; da «servicio a organizaciones y personas que trabajan por el cambio y la justicia social» desde hace diez años.
39. Con bajo nivel de actividad en la actualidad, antes en http://www.griesca.org.
40. Ahora no operativa; se puede consultar en http://www.nodo50.org/antiue.
41. http://www.lahaine.org/b2/articulo.php?p=1805&more=1&c=1.
42. http://www.esfazil.com/kaos/noticia.php?id_noticia=3140.
43. Los hackmeetings han sido cinco: CSO Les Naus (Barcelona), octubre de 2000; Leioa (Bilbao), septiembre 2001; CSO Laboratorio III, en octubre de 2002; Iruña (Navarra), octubre 2003, y Sevilla, en octubre de 2004.
44. http://www.forosocialsevilla.org.

bastan», un encuentro contra la macabra celebración que las instituciones de Bretton Woods (FMI y Banco Mundial) realizaban en Madrid en 1994. En aquellos tiempos éramos una simple BBS (Bulletin Board System) que proporcionaba pequeñas ayudas telemáticas para las organizaciones que intentaban denunciar la lógica de estas poderosas instituciones. En el año 1996 dimos el salto a Internet y nos convertimos en proveedor de acceso. Desde entonces hemos venido trabajando ininterrumpidamente en diversas campañas, acciones, proyectos, congresos junto a diversos movimientos sociales y organizaciones políticas.

¿QUÉ ORGANIZACIONES ESTÁN EN NODO50?

En Nodo50 cabe y está representado un amplio espectro de la izquierda política y social, de los

actividades; muchos de sus miembros están en el origen de Indymedia Estrecho y colaboran activamente en la preparación del quinto hackmeeting[45], el Hackandalus, en octubre de 2004.

Aunque con una vida cotidiana fuera de las campañas más intensa, también están implicados en la cobertura de la campaña Barcelona 2002 contra la Europa del Capital y la Guerra, junto con Indymedia Barcelona, Liberinfo.net[46]; además de facilitar las relaciones de los movimientos sociales catalanes con los medios de comunicación convencionales, posee una útil herramienta que permite el envío de notas de prensa a los mismos desde la Red. Cabe destacar igualmente el Infospai[47], que provee servicios de Internet a movimientos sociales, y moviments.info[48] y moviments.net[49] que están vinculados al proyecto.

b) Dentro de lo que entendemos por publicación abierta, propia de los weblogs, nos centraremos en *la Red Indymedia*. La distinción planteada respecto de la contrainformación parte de la mera gestión de los contenidos en sus páginas: en la primera está moderada por el colectivo editorial, mientras que en la publicación abierta sólo permanece, teóricamente, en manos de los editores la columna central, existiendo un espacio para la publicación libre, anónima, sólo regulada por orden cronológico.

Mantendremos la pequeña hipótesis de que la vinculación entre redes sociales y redes virtuales es más acuciante en la red Indymedia, precisamente al quedar su funcionamiento como «herramienta» a merced de las contribuciones de los usuarios. La caída del ciclo de movilización «antiglobalización» tras los sangrientos sucesos de Génova, en julio de 2001, se traslada a las herramientas telemáticas, que se ven obligadas a sustentar la línea argumental en procesos más cotidianos, alejados

45. http://www.sindominio.net/hackmeeting/index.pl?FAQes.
46. http://liberinfo.net.
47. http://infoespai.org.
48. http://www.moviments.info.
49. http://moviments.net.

movimientos de transformación y contestatarios: desde el ecologismo al feminismo, desde el sindicalismo de clase hasta las radios libres y la solidaridad internacional, desde la teología de la liberación a los centros sociales, desde la cooperación al desarrollo a familiares de desaparecidos, del anticapitalismo militante a la democratización de la educación, desde grupos teóricos a colectivos de acción directa, desde la liberación animal a las luchas contra la globalización. Como colectivo apostamos por superar la fragmentación de los movimientos en islotes atomizados trabajando en la construcción de un archipiélago interconectado de resistencias y acciones colectivas.

¿QUÉ PODEMOS ESPERAR DE LA INFORMÁTICA?
La informática no debería ser coto privado de expertos y dominio de especialistas y multinacionales.

de las grandes contracumbres. En el caso del Estado español, sólo los Indymedias ubicados en áreas geográficas donde hay niveles de conflictividad interna y movimientos sociales capaces de mantener una tensión informativa constante, precisamente aquellos dos donde el nacionalismo actúa como elemento de dinamización social, el fenómeno Indymedia no acusa la caída del ciclo. En los demás casos, se ven obligados a optar o bien por una dispersión territorial de nodos, descentralizando la gestión en pequeños grupos con autonomía y menor carga de trabajo; o bien por cerrar filas en torno al proyecto, perfilando de manera más estrecha la línea editorial y combatiendo consecuentemente la disidencia interna.

Resulta difícil evaluar el futuro de la Red Indy en el Estado español al margen de sus correspondientes bases sociales, siendo éstas las que determinan el sentido último de cada proyecto:

- Indymedia Barcelona[50]: nace en diciembre de 2000, de la mano de activistas catalanes y europeos que habían participado en la contracumbre de Praga y que estaban preparando el trabajo del área de prensa de la campaña Barcelona 2001; concretamente, se funda tras el hackmeeting de Barcelona, en octubre de 2000, en el transcurso de la reunión convocada para este fin en el Espai Obert. Es el único Indymedia que se crea antes de la contracumbre de Génova en el Estado, y se trata, posiblemente, del nodo más activo.
- Indymedia Euskal Herria[51]: surge en junio de 2002, de mano de activistas vascos que asisten a la contracumbre de Génova (julio 2001) y, más concretamente, gracias al trabajo del Centro de Medios de la Escuela Díaz. Tras una intensa ronda de trabajo político interno (Desobedientzia Eguna en octubre de 2001, etc.), se constituye técnicamente gracias al impulso recibido por el grupo promotor en la Reunión Regional de Indymedias en Berlín. Mantiene importantes niveles de actividad, en una clave nacionalista algo más pronunciada que en el caso catalán.

50. http://barcelona.indymedia.org.
51. http://euskalherria.indymedia.org.

Aquellos quienes tienen la competencia necesaria para apropiarse de las ventajas de un uso intensivo de la red son precisamente aquellos que se sitúan normalmente del lado de la dominación. Los instrumentos que permiten el acercamiento al mundo telemático no están universalmente distribuidos (ni en hardware ni en software) y la posibilidad de su disfrute debería ser un derecho garantizado. Facilitar y garantizar la accesibilidad a un recurso como es la información y la actividad en la red es algo prioritario. Debemos poner de relieve los límites que se imponen al uso social de las nuevas tecnologías determinados por la desigualdad social y la mercantilización del conocimiento.

¿Qué entendemos por contrainformación?

Contrainformar es trabajar por legitimar los discursos insurgentes frente al pensamiento único neoli-

- Indymedia Madrid[52]: como ya dijimos, surge en enero de 2002, dando continuidad a la primera ACP.
- Indymedia Galiza[53]: aunque planteado en clave nacionalista, no logra alcanzar sin embargo niveles espectaculares de actividad en el momento clave de las movilizaciones con motivo del hundimiento del Prestige. Vinculado al CSO A Casa Encantada y a su hacklab, no ha logrado gran resonancia dentro de la red Indy, permaneciendo a niveles muy similares a los dos IMC más recientes.
- Indymedia Estrecho/Madiaq[54]: aunque su asamblea fundacional data de abril de 2003, no empieza a funcionar hasta julio de ese mismo año. Puesto en marcha por activistas andaluces implicados en la contracumbre de Sevilla de junio de 2002, es el primer Indymedia transfronterizo, con la multiculturalidad como principio rector y la vocación de lograr «paridad entre las dos orillas». Consta de numerosos nodos territoriales dentro del IMC Andalucía, como el IMC Jerez, IMC Granada, IMC Málaga o el de Sevilla. El IMC Canarias[55] se independiza de Estrecho y constituye un nodo aparte durante 2004. Con proyección hacia el otro lado del Estrecho de Gibraltar, está el IMC Magreb[56].
- Indymedia La Plana[57] e Indymedia Alacant[58]: los dos más recientes, surgen en 2004 como nodos provinciales en la Comunidad Valenciana. Trabajan en clave nacionalista, con el idioma como reivindicación central. Con el despegue en fase reciente y dada su adscripción territorial marcada por la identidad territorial que manejan, es pronto para evaluar su impacto en la Red.

52. http://madrid.indymedia.org.
53. http://galiza.indymedia.org.
54. http://madiaq.indymedia.org.
55. http://canarias.indymedia.org
56. http://madiaq.indymedia.org/magreb.
57. http://laplana.indymedia.org.
58. http://alacant.indymedia.org.

beral, destruir el mito de la objetividad, servir de vocero de los movimientos sociales, dar la palabra a quienes callan por falta de oportunidades para hablar, combatir el ruido con apariencia de música que emana de los gigantes mediáticos. Contrainformar es también hacerse con herramientas que permitan la difusión horizontal de información, construir puentes que hagan circular contenidos con valor de uso, romper el monopolio de la producción de discursos sobre el mundo social, desbaratar la ilusión de una «opinión pública libre». Contrainformar es también romper la atomización que el capitalismo global está generando, entrelazar realidades sociales transformando la aventura individual en una relación social comunicable y comunicada.

No podemos terminar sin mencionar proyectos pioneros o paradigmáticos en el campo de la comunicación alternativa que surgen fuera de las fronteras del Estado español. Éstos son, entre otros:

– Isole Nella Rete («Islas en la Red») nace en 1996 y progresivamente se convierte en un proveedor de servicios de Internet para movimientos sociales, con una evolución técnica similar a la que siguió Nodo50. Opera en Italia, muy vinculado a los centros sociales okupados, dentro de la esfera ideológica de la Autonomía:

> *«¡Esta es una zona autónoma!» Un lugar que ofrece visibilidad, relaciones y una oportunidad de disfrute para aquellos que se han visto fragmentados y dispersados por los profundos cambios ocurridos en nuestra sociedad —aquellos que no están alineados con el «pensamiento único», todavía no resignados a la marginalidad—, aquellos que todavía sueñan con construir un movimiento REAL capaz de cambiar el actual «estado de cosas».*[59]

En junio de 1998, su servidor (ecn.org) es secuestrado por orden de la Fiscalía de Vincenza, por haber publicado una convocatoria titulada «Solidaridad con el pueblo kurdo. Boicoteemos el turismo en Turquía», firmada por la sección de Vincenza de la Liga por los Derechos y la Liberación de los Pueblos[60]. Nodo50 hizo un *mirror* (espejo) de la web de ecn.org como medida de solidaridad[61] y para garantizar su visibilidad durante todo el secuestro.

Pero la European Counter Network (ECN) había nacido como red de BBS[62], en 1989, como un proyecto en el que están involucrados ciberactivistas italianos, británicos, alemanas y holandeses, y contó en su momento con nueve nodos en Italia: Asti, Bolonia, Brescia, Florencia, Milán, Monselice, Padua, Roma y Turín.

59. http://www.ecn.org.
60. http://www.bufetalmeida.com/free/isole.html.
61. http://www.nodo50.org/ecn.
62. Bulletin Board System.

¿POR QUÉ NUESTROS SERVIDORES CORREN SOBRE EL SISTEMA OPERATIVO GNU/LINUX?
Apostamos por el software libre, es decir, por la producción colectiva de conocimiento al margen de los procesos de mercantilización de las ideas. GNU/Linux, sistema operativo libre, alternativa al monopolio Microsoft y resultado del trabajo colectivo de una comunidad mundial de programadores, es el máximo exponente de este nuevo fenómeno que sólo es posible en Internet y que pone en cuestión los pilares sobre los que se construye la «nueva economía»: la propiedad privada sobre el conocimiento, las patentes sobre todo aquello que genera beneficios, incluyendo la vida. GNU/Linux rompe con eso y nosotr@s apostamos por Linux.

– Autistici[63] es otra iniciativa con sede en Italia, que coordina (y a los que da servicios de Internet) a cerca de cuatrocientos colectivos que trabajan el hacking, la privacidad, la seguridad informática y el acceso libre a la Red. En agosto de 2004, algunas de sus páginas fueron censuradas[64] por criticar satíricamente a Trenitalia por el transporte de armas en territorio italiano destinadas a la guerra de Irak.
– TAO[65] es el proyecto del colectivo anarquista canadiense Organizing for Autonomous Telecomms, que pretende «crear una escuela radical de comunicaciones»[66]. No sólo funciona como proveedor de servicios de Internet. Como proyecto político, se basa en un decálogo[67] inspirado en el programa del Partido de los Panteras Negras[68]. Es un referente para gran parte de los proyectos telemáticos alternativos de la Red.
– Greennet es un proveedor de servicios de Internet que da soporte a todo tipo de iniciativas (individuales y colectivas) que promueven la paz, la defensa del medio ambiente y los derechos humanos a través de la tecnologías de la comunicación. Lo relevante de esta iniciativa es su carácter pionero: nace como BBS en 1986, es decir, mucho tiempo antes del nacimiento de Internet y, ya en 1989, establece vínculos con otros proyectos similares en diversas partes del mundo[69]. A diferencia de Isole Nella Rete o de Nodo50 (ambos con un perfil movimentista claro), se inscribe en lo político y lo organizativo, en el modelo ONG que define a los miembros de la Association for Progressive Communications (APC), la cual contribuye a fundar en 1990 junto a otras 25 plataformas.

63. http://www.autistici.org/it/index.html.
64. http://www.cmaq.net/es/node.php?id=17824.
65. http://www.tao.ca.
66. https://members.tao.ca.
67. Bases of Unity: http://oat.tao.ca/book/view/9.
68. http://lists.village.virginia.edu/sixties/HTML_docs/Resources/Primary/Manifestos/Panther_platform.html.
69. http://www.gn.apc.org/about/index.html.

Mediactivismo, *fase superior* de la contrainformación

Franco Berardi, *Bifo*, nos habla de activismo mediático (*mediactivismo*) como superación del modelo contrainformativo y como acción orientada a romper la pasividad política que se impone a nivel masivo por el bombardeo televisivo sobre una población que ha sido expulsada de cualquier espacio público de expresión[70]. Su crítica a la contrainformación se podría resumir de esta forma:

– En principio el *mediactivismo* pretende desvelar algo que el poder esconde. En esa línea es heredero de la contrainformación clásica. Para Bifo la contrainformación expresa cierta ingenuidad en relación a lo que entiende por información. Su oposición a la mentira o al vacío lleva a la contrainformación a defender la idea de que existe una verdad no revelada, sin reparar en que la información es una construcción política, un elemento en el conflicto cargado de intención. El *mediactivismo*, fase superior de la contrainformación, no trabaja sobre la premisa de una verdad objetiva.

– Por otra parte, Bifo aclara que en los términos técnicos del enfrentamiento existe una desproporción inmensa entre las guerrillas contrainformativas y los medios de comunicación de masas. Combatir *la verdad del poder* con *la verdad del movimiento* en un embate frontal no tiene ningún sentido como estrategia de acción política, salvo que se asuma la recreación en la derrota o la marginalidad como posición permanente en el conflicto. «La invasión de la *infosfera* por los flujos mediáticos emitidos por el poder es asfixiante, omnipresente e ineludible».

– El flujo mediático no se dirige a la atención consciente y no trabaja sobre los contenidos. Trata de influir de modo subliminal modelando reacciones cognitivas, formando hábitos mentales que reduzcan la capacidad de reacción crítica y nos predispongan a una asimilación pasiva e irreflexiva de lo real-mediático. Por eso, los mensajes contrainformativos dirigidos a la racionalidad del receptor no tienen un lugar en el *mediactivismo*. «El público no tiene tiempo de examinar racionalmente el contenido de los mensajes: tiende más bien a ser orientado por flujos infoestimulantes».

- El *activismo mediático* se pone en marcha, en un primer momento, como *hacking* o interferencia técnica de los medios empresariales para pasar a una estrategia de *brain hacking o subvertising*. Es el arte de la resistencia cultural y consiste en modificar el mensaje del anuncio o del discurso político («Al flan Ibarretxe le faltan huevos», leemos en *Ekintza Zuzena*) mediante la *tergiversación semántica*. El *subvertising* trabaja en el terreno indefinido situado entre el *mediascape* y el *mindscape*[71], en donde se define el espacio del discurso público, se delimita lo que se puede y no se puede ver y se establecen las jerarquías de prioridad (criterios de selección) de la atención colectiva. El modelo teórico de Bifo reduce la

70. Bifo (Franco Berardi) (2004): «Dictadura mediàtica y activismo mediàtico en Italia«. *Archipiélago*, 60.
71. *Mediascape* de la industria cultural, el ámbito de la producción de discursos *massmediáticos*. El *mindscape* es el plano de la aprehensión y procesamiento individual de los datos recibidos (Bifo: 2003, 2004).

esfera de lo comunicativo a estos dos planos, sin entrar en mayores detalles: uno social en sentido amplio (*mediascape*) y otro psíquico e individual (el *mindscape*, la estructura cognitiva que procesa lo percibido). La *infosfera* es la interfaz que media, hacia la que se emite y desde la que se recibe.

Si bien Bifo no deja de señalar que la capacidad de producción de datos del *mediascape* está dominada por el trabajo de las máquinas, los automatismos y la explosión digital, no hay en su trabajo un sólo intento de aproximación empírica al concepto en tanto que estructura social: no sabemos *dónde* localizarla, cuáles son sus componentes, la relación jerárquica entre ellos, las relaciones de propiedad que la atraviesan y su posición en relación a la estructura de poder global o local o estatal, en caso de que estuviera sujeta a algunas de estas referencias políticas y espaciales[72]. Sabemos pues lo que hace, pero no *qué* es, *de quién* es, *cómo* y *por qué*[73]. Así de complejo y de simple al mismo tiempo. La intervención organizada en el *campo infosférico* (seguimos en Bifo) da forma y arrima las primeras piedras de lo que pueda llegar a ser *un nuevo espacio público* que se constituye en el *éxodo del espacio privatizado* de comunicación que se ha impuesto desde los *massmedia mercantilizados y militarizados por el Estado*. Lo conformarían núcleos de producción cultural autónoma que entran en conflicto, pugnan y se redefinen en relación a los campos de comunicación del Estado-mercado (redes telemáticas de activismo, netart, hackmeetings, hacklabs, redes de consumo, redes wireless, sin tierra, piqueteros, estudiantes, en otros años la universidad, precari@s del espectáculo, los centros sociales o las distribuidoras contraculturales); es decir, un proyecto, un deseo: el archipiélago de resistencias culturales que conforman el imaginario político de la *autonomía política italiana*, de la que Bifo es parte y desde la que construye un modelo.

En otro plano, algunas referencias que hace Bifo a la contrainformación no son del todo precisas. Hace tiempo ya, y una vez superada la primera etapa de rigidez de los proyectos contrainformativos, que se ha dejado de trabajar (si es que en algún momento se asumió) sobre las premisas de la comunicación como un ejercicio de imposición de verdades reveladas y de relatos objetivos acerca de *lo real*. Desde un medio que puede pensarse «clásico», como *Ekintza Zuzena*, se toca el tema en mayo de 2004: «*Los mass media, y en especial la televisión, se venden a sí mismos como no ideológicos y no selectivos. Los medios de comunica-*

72. El nivel de aproximación de Bifo a los conceptos que maneja es de este estilo: «El *mediascape* es el sistema mediático en continua evolución, el universo de los emisores que envían a nuestro cerebro señales en los más variados formatos. La *infosfera* es el interfaz entre el sistema de los medios y la mente que recibe sus señales; es la ecosfera mental, esa esfera inmaterial en la que los flujos semióticos interactúan con las antenas receptoras de las mentes diseminadas por el planeta. La *mente* es el universo de los receptores, que no se limitan, como es natural, a recibir, sino que elaboran, crean y a su vez ponen en movimiento nuevos procesos de emisión y producen la continua evolución de *mediascape*» (Bifo: 2003).

73. Bourdieu se aproxima desde una posición un tanto más materialista a la realidad en su definición de «campo periodístico». «Un campo es un espacio social estructurado, un campo de fuerzas —hay dominantes y dominados, hay relaciones constantes, permanentes, de desigualdad que se desarrollan dentro de este espacio— que es también un campo de luchas para transformar o conservar ese campo de fuerzas. Cada cual, dentro de ese universo, compromete en su competencia con los demás la fuerza (relativa) que posee y que define su posición dentro del campo y, consecuentemente, sus estrategias» (Bourdieu, P.: 1997).

ción alternativos, por su parte, se declaran abiertamente como no objetivos, puesto que parten de una propuesta de cambio social y la defienden, es decir, no ocultan sus intenciones y el grado de su fiabilidad viene determinada por valores como la honestidad, la transparencia y la independencia»[74]. En la misma línea, desde un servidor telemático comprometido en la contrainformación desde hace diez años se puede leer esto otro en su declaración de intenciones:

> *Contrainformar es trabajar por legitimar los discursos insurgentes frente al pensamiento único neoliberal, destruir el mito de la objetividad, servir de vocero de los movimientos sociales, dar la palabra a quienes callan por falta de oportunidades para hablar, combatir el ruido con apariencia de música que emana de los gigantes mediáticos. Contrainformar es también hacerse con herramientas que permitan la difusión horizontal de información, construir puentes que hagan circular contenidos con valor de uso, romper el monopolio de la producción de discursos sobre el mundo social, desbaratar la ilusión de una «opinión publica libre». Contrainformar es también romper la atomización que el capitalismo global está generando, entrelazar realidades sociales transformando la aventura individual en una relación social comunicable y comunicada.*[75]

Nada que ver con la idea de un ejército de inofensivos liliputienses inmolándose en nombre de su verdad ante ese par de gigantes (el mercado y el Estado en acción comunicativa) en alianza. La contrainformación como modelo de comunicación tiene más que ver con el empeño por estructurar medios *desde y para* los movimientos, medios de coordinación, espacios para el intercambio simbólico, para la puesta en común, terreno en el que los agentes de la movilización miden fuerzas, establecen alianzas, diseñan su estrategia. Ése fue el papel de las herramientas comunicativas del movimiento durante el ciclo de movilizaciones que arranca en Seattle en 1999 y se cierra en Génova en el 2001, aplastado por la represión y emplazado a gestionar políticamente su demostrada capacidad de movilización y respuesta.

Algunos sectores de la comunicación movimentista iniciaron en cierto momento un proceso de debate interno en el que pretendían encontrar las claves que permitieran dar el salto de lo que es el ámbito de influencia de las redes sociales hacia *el gran público*. El debate penduló entre aquellas posiciones que defienden la laxitud del discurso, las que analizan la acción comunicativa en relación al movimiento social que las sustenta y las que anticipando el asalto a la opinión publica, advierten sobre el peligro de un cambio de tal naturaleza que, guste o no, convertiría a la contrainformación en algo distinto a lo que es, cambiaría su

74. Colectivo Ekintza Zuzena Contrainformación. (2004): «Algunos planteamientos sobre la contrainformación». *Ekintza Zuzena*, 31.
75. «¿Qué entendemos por contrainformación? FAQ de Nodo50». http://www.nodo50.org/faq.htm#contrainformacion.

objeto, su objetivo, su medio técnico y el juego de discursos que la define. Las cuestiones sobre las que fluctuó el debate fueron cuatro:

– ¿Por qué si en las últimas movilizaciones estatales (huelga general, estudiantiles, contra la guerra...) han participado miles de personas, ahora desde los colectivos de información alternativa no logramos comunicarnos con ellas?
– ¿Cómo lograr el objetivo de trasladar nuestros mensajes más allá del círculo de activistas?, ¿rompemos realmente el cerco comunicativo con nuestros proyectos actuales?
– ¿En qué medida es importante poner en marcha un medio de masas desde los movimientos sociales?
– ¿Qué pasos efectivos podemos dar en esa dirección?

El resultado fue un tanto decepcionante y puso sobre la mesa las limitaciones analíticas y autorreflexivas de parte de los movimientos sociales, atrapados a medias entre esquemas mentales acartonados y retóricos (con clichés del estilo «la necesidad de construcción de un medio de comunicación de masas»), y una superficialidad y banalidad fuera de lugar en un debate serio. Se centró en una búsqueda de «responsables» y no de causas de estas limitaciones, que fueron encontrados en la ciudadanía que los ignora, en los medios de comunicación convencionales que los ocultan, en los militantes que no se comprometen o en los tics de un discurso politizado que fragmentan. Se obvia, por otra parte, la pregunta crucial que parece sobrevolar todo el debate, y que se centra en torno a su propia posición en los procesos políticos y sociales: ¿son herramientas al servicio de lo social, son movimientos sociales? Todo ello sin la más mínima mención del terreno donde realmente se resuelve esta dicotomía: la necesaria correspondencia entre redes sociales y redes virtuales que dan sentido a un movimiento social donde realmente no lo hay, que justifican una herramienta aparente que los movimientos utilizan.

En este momento, en el que la acción comunicativa de los movimientos se lleva a cabo en un espacio mixto, en el que confluyen redes sociales sobre redes tecnológicas, la contrainformación hace tiempo que se ha liberado de sus primeras limitaciones operativas para convertirse en un instrumento de dinamización y expansión de las redes de activistas a nivel global. Al contrario que el movimiento de las *telestreets* italianas que irrumpen en un espacio comunicativo hostil disputando con el enemigo la *infosfera* (Bifo), el espacio en el que la opinión publica capta *lo real* (paradójicamente, en una competencia con el poder en su terreno, bajo una desproporción de medios impresionante); los proyectos contrainformativos forman parte de la estructura interna de los movimientos y sus terrenos de expansión. Lejos de todo intento ilusorio de abordaje a las audiencias, lo suyo es *la guerrilla*, la irrupción fugaz, la construcción de redes subterráneas de resistencia política y de producción simbólica. En ese terreno y sobre un medio nuevo (la Red), su potencial ha demostrado ser magnífico.

Cierre

Todo actor colectivo en el conflicto político contemporáneo vive con la necesidad de ampliar su espacio de intervención, sobre la base de la visibilidad de su repertorio de acción y la legitimidad de su propuesta. En ese empeño, la *técnica* informativa y la dimensión comunicativa de la intervención política se convierten de forma gradual en centrales, determinantes y, en algunos casos, en la dimensión definitiva de algunos proyectos y organizaciones políticas. Ésta es la dinámica histórica y política donde han de situarse las prácticas y las propuestas que en este trabajo hemos llamado «contrainformación». No siempre es fácil actuar en función de lo que se piensa, de la misma manera que muchas veces el frenesí del activismo cotidiano limita la capacidad de reflexión en tiempo real sobre lo que se hace. Con este artículo, que concebimos como análisis de nuestra propia militancia política, no pretendemos hacer simple cronológica. Nuestra intención ha sido más bien sustraer de ella algunos hechos, determinados proyectos y unos cuantos relatos para explicar las prácticas contrainformativas de la redes sociales y poder abordar la contrainformación como modelo de comunicación.

Bibliografía

BIFO (Berardi, F.) (2004): «Dictadura mediática y activismo mediático en Italia». *Archipiélago*, 60, Barcelona.

— (2003) *La fábrica de la infelicidad. Nuevas formas de trabajo y movimiento global*. Madrid, Traficantes de Sueños.

BOURDIEU, P. (1997): *Sobre la televisión*. Barcelona, Anagrama.

CASANOVA, G.(2002): *Armarse sobre las ruinas*. Madrid, PH.

COLECTIVO EKINTZA ZUZENA DE CONTRAINFORMACIÓN (2004): «Entre lo real y lo virtual». *Ekintza Zuzena*, 31, Bilbao.

— (2004) «Algunos planteamientos sobre la contrainformación». *Ekintza Zuzena*, 31, Bilbao.

HORKHEIMER, M y ADORNO, T. (2003): *Dialéctica de la Ilustración*. Madrid, Editorial Trotta.

LESSIG, L. (2001): *El código y otras leyes del ciberespacio*. Madrid, Taurus Digital.

LÓPEZ, S. (2004): *Distintos medios para distintos fines: movimientos sociales y medios de comunicación propios, España 1999-2003*. Tesina inédita, UCM.

LÓPEZ, S.; ROIG, G. y SÁDABA, I. (2003): «Nuevas tecnologías y participación política en tiempos de globalización». *Hegoa Cuadernos de Trabajo*. Bilbao.

ROIG, G. y SÁDABA, I. (2003): «Internet: nuevos escenarios, nuevos sujetos, nuevos conflictos». En Aparici, R. y Sáez, V.: *Cultura popular, industrias culturales y ciberespacio*. Madrid, UNED.

— (2004): «El movimiento de okupación ante las nuevas tecnologías. Okupas en las redes». En Adell, R. y Martínez, M.: *Dónde están las llaves. El movimiento okupa: prácticas y contextos sociales*. Madrid, Libros de la Catarata.

WILHELMI, G. (1998) *Lucha Autónoma. Una visión de la coordinadora de colectivos (1990-1997)*. Madrid, Traficantes de Sueños.

UNA INTRODUCCIÓN AL SOFTWARE LIBRE

Enrique Matías Sánchez
enrique.matias@hispalinux.es

INTRODUCCIÓN

A día de hoy, mucha gente ha oído hablar de «Linux» y sabe que es una alternativa a Windows, gratuita y libre de virus malignos. A bastantes les suena también la expresión «software libre», pero todavía no saben muy bien de qué se trata. Sin embargo, el software libre es tan antiguo como las propias computadoras, y sus raíces son todavía más profundas, pues se hunden en una tradición secular entre los hombres de ciencia: la de compartir los logros de cada uno con el resto de sus colegas.

A lo largo de la historia, la ciencia se ha desarrollado como búsqueda del conocimiento y de mejora de nuestras condiciones de vida. Desde la antigua Grecia, los científicos han considerado que el conocimiento era patrimonio de la humanidad. Podían ganar dinero de sus descubrimientos, pero no era ésa su principal motivación, sino satisfacer su curiosidad, contribuir a la sociedad y lograr el reconocimiento de sus semejantes. Para ello se apresuraban a publicar sus teorías y experimentos, poniéndolas a disposición de sus colegas, que las podían emplear para profundizar en el tema y hacer nuevos descubrimientos[1].

La filosofía hacker no es sino una actualización de la de los científicos de épocas anteriores. Básicamente, consiste en creer que toda la información útil, que sirva para ayudar a comprender cómo funciona el mundo, debe ser libre y accesible para todos, y que se debe usar el conocimiento ya disponible para crear más conocimiento.

1. Isaac Newton expresó su gratitud hacia los trabajos previos de Copérnico, Tycho Brahe, Galileo y Kepler en su conocida frase *«If I have seen further it is by standing on ye shoulders of giants»*.

Un poco de historia

Los primeros hackers

La cultura hacker tiene su mítico origen en los años cincuenta. El Tech Model Railroad Club era (y sigue siendo) un club de estudiantes del prestigioso Massachusetts Institute of Technology (MIT) aficionados a las maquetas de trenes. Un grupo de miembros del TMRC formaba el subcomité de *Signals and Power*, que se ocupaba de arreglar, mejorar y redistribuir los innumerables cables, interruptores, relés, etc., que hacían funcionar el complicado circuito que tenían, que ocupaba toda una habitación. Dedicaban a esta tarea incontables horas, y con el tiempo fueron desarrollando su propia jerga: por ejemplo, llamaban *hack* a algo que se hacía no sólo por su (in)utilidad, sino también por el simple placer que suponía plantearse retos que exigían cierta innovación, estilo y técnica.

Algunos de aquellos hackers tomaron una asignatura recién creada: programación de computadoras. Su profesor era el matemático John McCarthy, que acuñó el término «inteligencia artificial» e inventó el lenguaje de programación LISP. Inevitablemente, los hackers no tardaron en plantearse desafíos y poner en la programación la misma pasión que habían puesto en perfeccionar el circuito de trenes.

Aquel pequeño grupo de hackers dio inadvertidamente cuerpo a una filosofía y ética propias:

Se debe desconfiar de la autoridad y promover la descentralización. Las burocracias crean reglas para consolidar el poder establecido, y ven el impulso constructivo de los hackers como una amenaza. La mejor manera de promover el libre intercambio de información son los sistemas abiertos, aquellos que no levantan fronteras artificiales entre el hacker y la información que necesita. Esto permite una mayor creatividad en general, y evita tener que reinventar la rueda una y otra vez.

La valía de un hacker debe juzgarse por sus *hacks*, no por criterios estúpidos como calificaciones académicas, edad, raza o posición. Un hacker puede crear arte y belleza con una computadora, pero no sólo en el resultado producido: el propio código de un programa puede ser bello, si está escrito con maestría, es innovador y aprovecha al máximo los recursos disponibles. Además, las computadoras pueden mejorar nuestras vidas, incluso las de quienes no son hackers. Son herramientas poderosas con las que se puede hacer casi cualquier cosa que uno desee.

Para los hackers, el trabajo y el dinero no son fines en sí mismos: el tiempo de ocio es más importante, y el dinero es básicamente un medio para poder dedicarse a actividades más afines a sus intereses personales o inquietudes intelectuales. Cuando trabajan en un hack, no es el dinero su principal motivación, sino la pasión de hacer algo interesante y creativo, y el reconocimiento del mismo por parte de los demás. Los resultados se ponen a libre disposición del resto de la comunidad, para que sean criticados o mejorados en un esfuerzo colectivo de aprendizaje. Defienden la libertad de expresión en la red, la privacidad, la libertad individual y el uso de la red como herramienta de denuncia y lucha contra situaciones de abuso e injusticia producidas en cualquier lugar del mundo. Entienden que las redes

EL SOFTWARE LIBRE EXPLICADO A LAS MARUJAS

El mundo del software se puede explicar fácilmente recurriendo a una comparación sencilla: los programas de computadora se pueden muy bien equiparar a las recetas de cocina. No son más que una serie de instrucciones a realizar: ponga una cucharada de aceite en una sartén, caliéntelo hasta 80ºC, casque un huevo y viértalo sobre la sartén, etc. Entre los programadores, esta receta o conjunto de instrucciones de un programa se denomina «código fuente». Ahora pensemos en la tarta de queso que prepara nuestra tía Mariluz cuando vamos a visitarla. Cada vez que recordamos lo deliciosa que es, pensamos: «tengo que acordarme de pedirle la receta». De algún modo, hemos asumido que no puede negarse a dárnosla. Lo vemos natural, y de hecho nos parecería mal y nos enfadaríamos con

deben ser un elemento de inclusión y entendimiento, y no un instrumento que aumente las brechas sociales provocadas por la exclusión de personas y regiones en función de intereses políticos y económicos.

Origen de la Fundación para el Software Libre

Inicialmente, las computadoras eran herramientas que servían para procesar datos, y los programadores se ayudaban entre sí compartiendo el código que escribían. Sin embargo, poco a poco las empresas decidieron convertir los programas informáticos en un producto comercial y prohibir su libre copia y modificación, lo que llevó al desmembramiento de la comunidad *hacker*.

Richard Matthew Stallman[2], del Laboratorio de Inteligencia Artificial del MIT, veía a principios de los años ochenta como la comunidad hacker que constituía su vida empezaba a disolverse bajo la presión de esta comercialización de la industria de software. En particular, otros hackers del Laboratorio de IA fundaron la empresa Symbolics, que activamente intentaba reemplazar el software libre del Laboratorio con su propio software privativo. Durante dos años, Stallman consiguió duplicar en solitario cada avance que creaba el equipo de programadores de Symbolics, para cuya desesperación Stallman liberaba como software libre, en castigo por haber destruido la comunidad que él amaba.

Por aquel entonces, sin embargo, él era el último de su generación de hackers en el laboratorio. Finalmente se planteó crear una nueva comunidad, en la que compartir y ayudar a los demás no fuera ilegal. Para ello decidió escribir un nuevo sistema operativo completo, compatible con Unix (un potente sistema operativo), pero libre para todos.

El 27 de septiembre de 1983 anunció en Usenet (grupos de discusión de la red) su proyecto, al que bautizó como GNU (*GNU's Not Unix*[3]), aunque

2. También es conocido por sus iniciales RMS. Tiene su página personal en http://www.stallman.org.
3. Es decir, «GNU No es Unix«. Los hackers son aficionados a estos juegos de palabras autorreferenciales.

ella si no lo hiciera, pues a ella no le cuesta nada, y a nosotros nos endulzaría la vida.

Sin embargo, no siempre es así. Algunas empresas, como la Coca Cola, venden alimentos o bebidas misteriosas. Quizá a regañadientes lleguen a decirnos los ingredientes que la componen, pero siempre se niegan en redondo a proporcionarnos la receta, el método de elaboración. No piensan en lo útil que nos podría ser para nuestra próxima fiesta. Como niños egoístas, prefieren guardarse su receta para ellos solos. Parece que han olvidado lo que les enseñaron en la guardería, que se juega más y mejor compartiendo los juguetes con los demás niños.

Comparemos su actitud con lo que nos encontramos en el mercado de nuestro barrio. Con frecuencia vemos un producto nuevo que nos llama la atención. Inmediatamente, le preguntamos a la tendera qué es y cómo se prepara. Antes de que acabe de darnos la receta, inevitablemente habrá

no lo acometería hasta enero de 1984, pues, antes de ponerse manos a la obra, RMS decidió dejar su puesto en el MIT, para evitar que la institución académica pudiese reclamar posteriormente algún tipo de derechos sobre su trabajo.

En 1985, publicó el «Manifiesto GNU», que define y explica sus objetivos y motivaciones, y poco tiempo después fundó la organización sin ánimo de lucro Free Software Foundation para coordinar el proyecto, al que poco a poco se iba uniendo más gente.

Escribir un sistema operativo no es tarea sencilla, y hacerlo tan completo como Unix, la convertía en titánica. RMS empezó escribiendo piezas capaces de funcionar sobre los Unices existentes: un editor de texto (Emacs), herramientas para programar como un compilador (gcc) y un depurador (gdb), etc. Un mérito tan importante o más que sus impresionantes logros como programador fue el inventar el concepto de *copyleft* (izquierdos de autor), que implementó en la Licencia Pública General de GNU (conocida generalmente como «GPL»).

La influencia de Stallman ha sido esencial para establecer el marco de referencia moral, político y legal del movimiento del software libre como alternativa al desarrollo y distribución de software privativo. Ha recibido numerosos premios y reconocimientos por su trabajo, entre ellos el *genius grant* de la MacArthur Foundation, en 1990, un doctorado honorario del Royal Institute of Technology de Suecia, en 1996, y la membresía en la American Academy of Arts and Sciences, en 2003.

Hacia 1990 el sistema GNU estaba casi completo; el único componente esencial que faltaba era lo que se llama núcleo[4], al que denominaron Hurd[5]. La Free Software Foundation decidió (quizás equivocadamente) escribirlo siguiendo

4. El núcleo o kernel es el responsable de la distribución de recursos, interactuar a bajo nivel con el hardware, seguridad, acceso al sistema de ficheros, protocolos de red, etc.
5. Aunque originalmente iba a llamarse Alix, el núcleo del sistema GNU fue bautizado por Thomas Bushnell como Hurd (http://www.gnu.org/software/hurd/hurd.html). «Hurd» significa *Hird of Unix-Replacing Daemons* (Hird de diablillos que reemplazan a Unix), y donde «Hird» significa *Hurd of Interfaces Representing Depth* (es decir: Hurd de interfaces que representan profundidad). ¡Si el nombre del sistema GNU es un acrónimo recursivo, el nombre del núcleo son dos acrónimos mutuamente recursivos!

otras personas en la fila que interrumpirán su explicación y nos ofrecerán sus propias consejos: añadir una pizca de tal especia que le dará toque especial a la salsa, combinarlo con tal otra cosa, etc. Si somos duchos en la cocina, con el tiempo nos atreveremos a experimentar con nuestras propias variaciones, con las que sorprenderemos a nuestros invitados, que nos pedirán a su vez «nuestra» receta.

Como vemos, la posibilidad de distribuir, usar y modificar las recetas permite descubrir y desplegar un abanico de sabores y aromas que ni el propio autor de la receta original sospechaba. Quizá a partir de la receta de nuestra tía podamos idear otro tipo de tartas, además de la de queso: de chocolate, de yogur, de frambuesa... En cambio, nunca podremos elaborar otro refresco a partir de la Coca Cola (en otro color, con sabor a horchata, con el doble de cafeína para las largas noches de estudio...). No es difícil discernir cuál de las dos actitudes es más beneficiosa para el conjunto de la sociedad.

un diseño tan innovador como complejo: en vez de escribir un núcleo monolítico al estilo tradicional de Unix, optaron por implementar el núcleo como una colección de procesos servidores (o «manada de ñus») que se ejecutarían sobre un micronúcleo y se ocuparían de las tareas del núcleo Unix.

Como micronúcleo, tras probar Trix (desarrollado en el MIT), decidieron usar Mach (desarrollado en la Carnegie Mellon University), que ahora es usado también por Mac OS X, el sistema operativo de Apple. El inicio del desarrollo se demoró un tiempo mientras esperaban que Mach se publicase como software libre, tal y como se había prometido.

La implementación de este diseño ha resultado ser mucho más difícil de lo que se esperaba. Sin embargo, y tras algunos años de pocos avances, el desarrollo de Hurd se ha reavivado últimamente, pues muchos programas están siendo adaptados para funcionar sobre él, y un grupo de desarrolladores está trabajando para sustituir al viejo GNU Mach por un micronúcleo más moderno, llamado L4.

A día de hoy, el Hurd es funcional, pero todavía le faltan varios años para alcanzar la madurez necesaria para ser usado en entornos de producción y poderse publicar la versión 1.0. Afortunadamente, no ha hecho falta esperar a la publicación del Hurd para poder disfrutar de un sistema libre, gracias a la aparición de Linux.

Linux, *just for fun*

Unix es una familia de potentes sistemas operativos desarrollada, a partir de 1969, en los Bell Labs de la American Telephone and Telegraph company (AT&T) por Kenneth Thompson y Dennis MacAlistair Ritchie (quien de paso creó el lenguaje de programación C), en un equipo dirigido por Doug McIlroy. Tras varios años de uso interno, AT&T empezó en 1974 a conceder licencias gratuitas o por un pago simbólico a las instituciones académicas, con lo que Unix se convirtió en la base de muchas clases y proyectos de investigación. Poco a poco se iría convirtiendo en un producto comercial y, finalmente, se prohibió el uso de su código fuente con fines educativos, con lo que

Volvamos ahora al mundo del software. Observaremos que la mayoría de las empresas tienen la misma actitud antisocial que la Coca Cola, agravada además por una situación de monopolio, cualquiera que sea el segmento de mercado (sistemas operativos, bases de datos, tratamiento de imágenes, diseño asistido por computadora...). Sin embargo, al igual que en el caso de las recetas, no siempre ha sido así, y no tiene porqué seguir siéndolo: las cosas se pueden hacer de otra manera.

la distribución del libro *A Commentary on the UNIX Operating System* que John Lions había escrito explicando cada fragmento del código fuente pasó a ser clandestina[6].

En la asignatura «Sistemas operativos: diseño e implementación» que se impartía en la Universidad Libre de Amsterdam habían estado usando el sistema Unix como ejemplo, pero ahora necesitaban buscar una alternativa. Para la mayoría de los usuarios, los Macintosh de Apple tenían un precio prohibitivo, y tendían a comprar PC basados en procesadores de la familia x86 de Intel, que funcionaban con el endeble MS-DOS (una copia mediocre del CP/M de Gary Kildall).

El profesor de la asignatura, Andrew Stuart Tanembaum, ante esta situación, decidió escribir desde cero un sistema operativo tipo Unix para los ordenadores domésticos con procesadores x86, al que llamó Minix, y un —hoy clásico— libro de texto explicativo que llevaba el mismo título que la asignatura. A pesar de que su código fuente estaba disponible, Minix no era libre, pues se seguía precisando una licencia y no se podía copiar. Tampoco era un sistema operativo excepcional: su único propósito era ser didáctico, por lo que el sistema era deliberadamente sencillo y con pocas funcionalidades; la claridad tenía más importancia que la potencia y la eficiencia.

El libro de Tanembaum fue devorado por miles de estudiantes de todo el mundo, que querían aprender como se escribía y se hacía funcionar un sistema operativo, ahora que todos los productores de software guardaban su código fuente en secreto. Entre estos estudiantes se encontraba un finlandés llamado Linus Benedict Torvalds.

Como hacker que era, Linus quería sacar el máximo partido posible de su 386, y a falta de otra alternativa (la FSF acababa de empezar a trabajar en el Hurd, que se preveía tardaría un tiempo en salir) decidió aplicar lo que había apren-

6. En agosto de 1996, dos años antes de la muerte de Lions, el libro pudo finalmente ser publicado legalmente. Para entonces, unas fotocopias legibles eran un pequeño tesoro.

dido con el libro y escribir un nuevo núcleo que superase las limitaciones de Minix. Lo hizo por mera diversión y aprovechando las herramientas del proyecto GNU.

Sin embargo, no fue ésta la verdadera genialidad de Linus, sino lo que hizo con lo que en principio no pasaba de ser un entretenimiento privado: lo puso en la red a disposición de todo el que quisiera jugar con él y solicitó la ayuda de quien quisiera colaborar.

El 25 de agosto de 1991, envió un mensaje al grupo de discusión de Usenet comp.os.minix, explicando su proyecto y señalando que ya había hecho funcionar sobre él algunas de las utilidades del proyecto GNU: el intérprete de órdenes bash y el compilador gcc. Aprovechaba para pedir comentarios sobre lo que la gente odiaba o le gustaba de Minix, ya que lo estaba tomando como modelo. Aclaraba que lo hacía por *hobby*, y que aquello no iba a ser un sistema grande y profesional como GNU.

A mediados de septiembre publicó, sin hacer mucho ruido, la versión 0.01. Su intención era que se llamara «Freax» (*free + freak + X*), pero Ari Lemmke, un amigo suyo que le ofreció espacio en su servidor, decidió publicarlo como Linux. El 5 de octubre Linus anunció la versión 0.02 con un histórico mensaje[7] en comp.os.minix, en el que animaba a la gente a descargarlo, probarlo y modificarlo para satisfacer sus necesidades. Para entonces ya era capaz de ejecutar más herramientas de GNU, como make y sed. Durante el resto del año salieron las versiones 0.03, 0.10 y 0.11, todas ellas bajo una licencia que prohibía su uso comercial. La versión 0.12, publicada en enero de 1992, fue la primera bajo la GNU GPL, y también la primera suficientemente estable (tras esta versión se saltó a la 0.95).

Lo revolucionario de Linux no está en su diseño (que no es especialmente innovador) ni en su filosofía (que la Free Software Foundation llevaba años predicando), sino en su metodología. Efectivamente, hasta entonces el software se escribía en grupos cerrados y de carácter vertical, mientras que Linus inauguró un nuevo modelo, distribuido y muy abierto, en el que cualquiera podía participar. A estos métodos tan diferentes se les ha denominado modelo catedral y modelo bazar, respectivamente, y los estudiaremos con más detalle más adelante.

Estos hackers, como el propio Linus, empezaron a trabajar en Linux simplemente por diversión y para aprender. No tenían grandes ambiciones con él, sino que más bien lo consideraban como un juguete hasta que, al cabo de unos pocos años, se lanzara el sistema GNU o una versión libre de BSD (otra familia de sistemas de la que hablaremos después). Sin embargo, ese juguete que era entonces Linux es usado hoy por más de 30 millones de personas de todo el mundo.

7. http://groups.google.com/groups?selm=1991Oct5.054106.4647%40klaava.Helsinki.FI&output=gplain.

GNU/Linux: la unión hace la fuerza

Linux empezó a aparecer en servidores FTP de Finlandia y otras partes del mundo. Los mensajes sobre Linux en el grupo de discusión comp.os.minix eran cada vez más numerosos, y finalmente Tanenbaum, el profesor que había escrito el Minix, intervino, haciendo notar que el diseño monolítico de Linux era obsoleto y que el futuro estaba en los micronúcleos, y criticando que no fuera portable a otros procesadores. A esto siguió una tremenda y encendida discusión[8], tras la que Linux pasó a tener un grupo de discusión propio.

Los usuarios de Minix fueron pasando a utilizar Linux, porque tenía más funcionalidades y porque cuando arreglaban fallos o escribían nuevas funcionalidades que necesitaban, podían enviarle a Linus las modificaciones (llamadas parches) para que las incluyera en la siguiente versión (Tanenbaum no lo hacía para que no se resintiera la sencillez y portabilidad de Minix). Además, no tenían que molestarse en escribir las otras partes del sistema, sino que simplemente adaptaban mutuamente el software GNU ya existente y el nuevo núcleo Linux, hasta que finalmente se obtuvo un sistema operativo libre completo y funcional: el sistema GNU/Linux (al que con frecuencia, y de manera incorrecta, se llama simplemente Linux).

Desgraciadamente, instalar en una computadora este nuevo sistema era un tanto complicado. No bastaba descargar y compilar[9] Linux, sino que había que realizar todo un proceso partiendo de las herramientas de GNU. También había que buscar el software libre de terceras partes que se quisiese usar, como el entorno gráfico X.

Fue Owen LeBlanc, del Manchester Computing Centre, quien, después de tener una réplica del código fuente de Linux en sus servidores, empezó en febrero de 1992 a publicar sus propios disquetes con binarios del núcleo y utilidades extra, con lo que se facilitaba extraordinariamente la instalación del sistema. Nacía así la primera *distribución* de GNU/Linux, llamada MCC Interim Linux. Poco después aparecieron otras distribuciones, como SLS (*Softlanding Linux System*) de Peter MacDonald, TAMU (*Texas A&M University*) e Yggdrasil.

El papel de una distribución es tomar programas de diferentes fuentes, compilarlos y configurarlos para conformar un sistema integrado, estable y fácil de instalar. A lo largo de los años han aparecido decenas de distribuciones, algunas de ellas llegando a ser empresas de notable envergadura (Slackware, SuSE, Red Hat, Mandrake...).

A primera vista, a un observador externo le podría parecer que el mundo del software libre está disgregado y dividido. Sin embargo, la descentralización no implica dispersión: esta variedad resulta muy beneficiosa para los usuarios. La fuerte competencia obliga a las distribuciones a avanzar y mejorar continua-

8. Comparando la evolución de Hurd y de Linux, vemos que si bien la teoría nos dice que un micronúcleo es mucho más potente y flexible, también es mucho más difícil de implementar en la práctica. Hoy en día, Linux ya no está atado al x86, sino que ha sido adaptado a muchas arquitecturas, y tiene un diseño muy modular, por lo que podría decirse que ocupa un espacio intermedio entre los micronúcleos y los núcleos monolíticos.
9. Procesar el código fuente escrito por el programador para generar un programa ejecutable por la computadora.

mente para intentar ser mejor y más atractiva que las demás. Al mismo tiempo, y al tratarse de software libre, cada distribución puede mirar las nuevas funcionalidades y mejoras que han desarrollado sus competidores e incorporarlas a su versión, con lo que al final acaban siendo bastante similares y son los usuarios los principales beneficiados.

En esta carrera por ser la distribución más moderna y atractiva, muchas distribuciones han optado por incluir también algo de software privativo para diferenciarse de las demás. En cualquier caso, tampoco pueden permitirse alejarse mucho del terreno común, pues a los usuarios no les gusta tener que invertir mucho esfuerzo en migrar y aprender un nuevo sistema, y los programadores no están dispuestos a perder tiempo y esfuerzo en solventar pequeñas incompatibilidades estúpidas. En general, un programa libre funcionará indistintamente sobre cualquier distribución de GNU/Linux (así como sobre *BSD).

Una distribución que merece una mención especial es Debian, por varios motivos:

– no es una empresa, sino que está constituida por cientos de voluntarios de todo el mundo y todo el software que incluye es totalmente libre (no obstante se pueden instalar paquetes no oficiales con software privativo);
– es la más completa: contiene varias veces más paquetes que cualquier otra distribución;
– no se limita al núcleo Linux, sino que también está desarrollando distribuciones basadas en Hurd y el núcleo de NetBSD;
– no sólo funciona sobre x86, sino también sobre PowerPC y otros procesadores más esotéricos (alpha, arm, mips, S/390, sparc, hppa...).

Otra distribución que, entre otras particularidades, también es desarrollada por voluntarios, es Gentoo.

Hay también distribuciones capaces de funcionar desde un CD-ROM (llamado *live-CD*), sin necesidad de instalar nada en el disco duro. Resultan útiles tanto para mostrar GNU/Linux a alguien que no lo conozca, así como para poder utilizar nuestras herramientas favoritas en una computadora que tenga instalado otro sistema.

Algunas de estos CD en vivo, como Knoppix, tienen carácter general, mientras que otras están orientadas a un uso particular. Por ejemplo, Pequelín está dirigido a los niños, Movix a la reproducción de vídeo, mientras que X-Evian y dyne:bolic están pensadas para satisfacer las necesidades de activistas y artistas, y son una herramienta práctica para la producción de multimedia.

El lector aguerrido que desee instalar GNU/Linux manualmente, desde cero y sin la ayuda de una distribución, puede visitar las páginas web del proyecto *Linux from scratch*, donde se explica el proceso paso a paso, a lo largo del cual aprenderá mucho sobre el funcionamiento interno del sistema.

La tortuosa historia de BSD

El software libre es un concepto que no se limita al sistema GNU/Linux. El ejemplo más conocido son los BSD, una familia de sistemas muy similares a GNU/Linux en cuanto a su funcionamiento y calidad.

Como se ha explicado, AT&T no consideraba inicialmente Unix como un producto comercial y lo compartía con terceras partes, como la Universidad de California en Berkeley, donde Ken Thompson pasó un año sabático. Allí, estudiantes como William N. Joy y Chuck Haley empezaron a escribir software para él, como un intérprete de Pascal y el editor de texto vi, y a distribuir estos programas en cintas, bajo el nombre de *Berkeley Software Distribution* (BSD)[10].

En 1979, la Defense Advanced Research Projects Agency (DARPA) decidió usar Unix como su sistema operativo estándar. Al enterarse, el catedrático de Berkeley Robert Fabry escribió una propuesta para que la Universidad desarrollara una versión mejorada de BSD que cubriera sus necesidades. Tras conseguir un contrato de 18 meses, se creó para este fin el Computer Systems Research Group (CSRG), con Bill Joy como líder del proyecto. Después de negociar con AT&T unos términos aceptables para todos, en octubre de 1980 publicaron 4BSD. Se vendieron unas 150 cintas, pero la licencia no era por máquina, sino por institución, con lo que el número de sistemas instalados era varias veces mayor.

Las siguientes versiones se numerarían 4.1, 4.2, etc., pues AT&T objetó que 5BSD podría dar lugar a confusión con su propio System V. En junio de 1981 se publicó 4.1BSD que, entre otras mejoras, incluía las que Bill Joy había hecho sobre el núcleo para aumentar su rendimiento. DARPA estaba satisfecha, y les concedió un nuevo contrato por dos años más y casi el quintuple de fondos. Joy acabó yéndose a la empresa Sun Microsystems, pero el desarrollo continuó, y en agosto de 1983 se publicó la 4.2, que añadía un sistema de ficheros más rápido y soporte para los protocolos de red TCP/IP, lo que supuso una importante ventaja sobre el System V de AT&T. A partir de entonces, AT&T incorporaría éstas y otras mejoras desarrolladas por BSD a su System V.

A la versión 4.3 (junio 1986) le siguió 4.3BSD-Tahoe (junio 1988), en la que el núcleo había sido dividido en partes dependientes del procesador y partes portables. Esto facilitaría extraordinariamente la posterior adaptación de BSD a otras arquitecturas. Hasta ese momento, todos los receptores de BSD tenían que adquirir previamente una licencia de código fuente de AT&T, pues Berkeley nunca publicaba su sistema solamente de forma binaria, sino siempre acompañado de su código fuente. A raíz del aumento del coste de estas licencias, Berkeley empezó a recibir peticiones para que publicara las utilidades y el código de red de TCP/IP que había desarrollado en una cinta aparte, que no requiriese dicha licencia.

10. BSD y 2BSD se basaron en Unix versión 6 sobre máquinas PDP-11, y 3BSD en Unix 32/V sobre máquinas VAX. El núcleo de 3BSD incorporaba una funcionalidad de memoria virtual que necesitaba y había desarrollado Ozalp Babaoglu, otro estudiante.

Así, en junio de 1989 se publicó la *Networking Release 1*, el primer código libremente redistribuible de Berkeley. Berkeley cobraba 1.000 dólares por cinta, pero la licencia era muy liberal, pues los usuarios podían modificar y redistribuir el código, incluso de forma binaria y bajo otra licencia. Las únicas exigencias eran que se mantuvieran las notas de copyright en los ficheros de código y que se añadiera una nota de reconocimiento a la Universidad y sus contribuidores en la documentación. A pesar de que el código no tardó en estar disponible de forma gratuita en servidores FTP, cientos de instituciones compraron copias, ayudando así a financiar futuros desarrollos.

Constatado este éxito, Keith Bostic propuso al CSRG reimplementar todas las utilidades, bibliotecas y el núcleo para poder publicar una versión de BSD libremente distribuible. En eventos públicos como Usenix, Bostic empezó a pedir a la gente que reescribiera las utilidades de Unix desde cero, basándose únicamente en su descripción pública. La única recompensa sería que su nombre aparecería en la lista de contribuidores junto a la utilidad que había reescrito. 18 meses después, prácticamente todas las utilidades y bibliotecas importantes habían sido reescritas. Bostic, Michael J. Karels y Marshall Kirk McKusick dedicaron los siguientes meses a examinar uno a uno todos los ficheros de la distribución, eliminando el código procedente del sistema 32/V de AT&T. Finalmente, les quedaron seis ficheros que no eran fáciles de reescribir y, tras pedir autorización a la Universidad, en junio de 1991 publicaban la *Networking Release 2*, bajo los mismos términos que la anterior.

Seis meses después, William Frederick Jolitz había conseguido reescribir estos seis ficheros, y compiló y publicó en la red una versión para PC, llamada 386/BSD. Bill Jolitz no tenía tiempo para atender todos los fallos y mejoras que aparecían, y al cabo de unos meses, un grupo de usuarios formó el proyecto NetBSD para mantener y mejorar el sistema. Una de sus prioridades fue la de que su distribución funcionara sobre el mayor número de plataformas posible. NetBSD no se limita a funcionar sobre los procesadores Intel o los PPC de los Apple, sino que es capaz de comportarse exactamente igual sobre una vertiginosa lista de máquinas menos frecuentes.

Unos meses más tarde, se formaba el grupo FreeBSD, que prefirió concentrarse en los procesadores x86 para así obtener un sistema operativo sólido como una roca y tremendamente eficiente, que obtuviese el máximo rendimiento de la máquina. También pretendían hacerlo más accesible a usuarios menos técnicos, como estaba haciendo GNU/Linux.

Más adelante, a mediados de los noventa, surgió de NetBSD otro grupo llamado OpenBSD, que, liderado por Theo de Raadt, decidió enfocar su trabajo en la seguridad[11], pero incorporando también la idea de facilidad de FreeBSD.

Por otra parte, se formó una empresa llamada Berkeley Software Design, Incorporated (BSDI) para desarrollar una versión del código con soporte comercial.

11. OpenBSD presume de ser el sistema operativo más seguro del mundo.

Sin embargo, las cosas se complicaron: Unix System Laboratories (la filial que tras USG había creado AT&T para desarrollar y comercializar Unix) interpuso una demanda contra BSDI y la Universidad de California por violación de copyright y divulgación de secretos comerciales. La Universidad de California contraatacó con otra demanda, argumentando que a su vez USL estaba usando el código de BSD sin respetar la licencia (la nota de reconocimiento a la universidad en la documentación y publicidad).

Poco después Novell compró USL, y su directivo, Raymond J. Noorda, prefirió negociar a seguir un proceso judicial de resultados impredecibles. En enero de 1994 llegaron a un acuerdo: la universidad aceptó retirar 3 de los 18.000 ficheros que componían la *Networking Release 2*, hacer algunos cambios menores y añadir notas de copyright de USL a otros 70 ficheros. El resultado se publicó en junio de 1994 como *4.4BSD-Lite*, y USL se comprometió a no demandar a nadie que lo usara como base. Así, los otros proyectos (referidos en conjunto como *BSD) tuvieron que desandar lo que habían hecho durante esos tres años y volver a empezar a partir de esta versión. En junio de 1995 se publicó *4.4BSD-Lite*, Release 2, y el CSRG se disolvió, dejando el desarrollo en manos de los demás proyectos.

Los diferentes *BSD eran y son unos sistemas maduros, estables y muy eficientes, pero para cuando se aclaró su situación legal, GNU/Linux ya era el sistema libre más popular. Por otra parte, la filosofía BSD, si bien apuesta firmemente por el software libre, no se opone al software privativo como hace la FSF. Esto se refleja en su licencia (que muchos encuentran demasiado permisiva) y en que sus desarrolladores y usuarios no hacen tanto *ruido* como los de GNU/Linux.

Las definiciones de software libre

Como hemos visto, al principio los hackers se intercambiaban sus programas y el código circulaba libremente. No existía una noción de software libre, pues todo el software lo era. El concepto de software libre no empezó a tomar forma hasta que las empresas comenzaron a restringir el acceso al código fuente, a prohibir la copia de los programas y a cobrar por licencias de uso.

Definición de software libre de la FSF

Stallman fue el primero en presentar un análisis de la situación, dar cuerpo a una filosofía y formular una definición de software libre. La Free Software Foundation entiende por software libre aquel que concede cuatro libertades a sus usuarios:

Libertad 0[12].- La libertad de usar el programa con cualquier propósito.

Libertad 1.- La libertad de estudiar cómo funciona el programa y adaptarlo a sus necesidades.

Libertad 2.- La libertad de distribuir copias.

12. Por extraño que pueda parecer, las computadoras no empiezan a contar por uno, sino por cero. Muchos hackers hacen lo mismo.

Libertad 3.- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie.

La libertad 0 garantiza que podamos usar el programa donde y para lo que queramos. Esta libertad no es obvia, pues el software privativo suele poner limitaciones a donde podemos usarlo (normalmente una única computadora y tras el pago de una licencia) y cómo podemos usarlo. Hay quien ha impuesto limitaciones de uso a sus programas, no permitiendo que sean usados comercialmente, o en determinados países, o por los que ejercen ciertas profesiones u otras singularidades. Esta práctica presenta serios inconvenientes a la hora de combinar dos o más programas, y estos programas no se consideran libres, pues el software libre ha de serlo para todos.

La libertad 1 nos permite modificar el programa o, si no tenemos conocimientos técnicos para hacerlo, pagar a alguien para que nos lo haga. No tenemos que negociar con el productor original del programa, sino que podemos contratar a quien más confianza y mejor precio y servicio nos dé. Mientras la posibilidad de adaptar un programa a sus necesidades es importante para las empresas, los usuarios quizás estén más interesados en saber que puede ser traducido a su idioma, por minoritario que sea.

Con la libertad 2, el autor nos da su permiso para hacer copias del programa y dárselas a quien queramos. Y no sólo podemos regalarlo o intercambiarlo por otro programa, sino incluso venderlo, si encontramos a alguien que nos pague por él. En el caso del software libre esto no es ilegal, pues el autor no sólo lo autoriza, sino que además anima a ello. Al difundir el programa estaremos ayudando no sólo a otras personas, sino también al autor: su programa llegará a más gente sin ningún esfuerzo por su parte, y al haber más gente usándolo, recibirá más sugerencias para mejorarlo y surgirá más gente dispuesta a ayudarle a desarrollarlo.

La última libertad nos permite redistribuir el programa con las modificaciones que hayamos hecho. Si lo hemos traducido a nuestro lenguaje, posiblemente queramos que nuestros paisanos puedan beneficiarse también de nuestro trabajo. Generalmente, lo más recomendable es enviar nuestras mejoras a los autores originales, para que las incorporen al programa y así no tengamos que volver a hacer nuestras modificaciones en futuras versiones. Pero quizás queramos usar parte del código de ese programa en un programa propio, o hacerle cambios importantes y crear un programa nuevo.

Hay veces que un grupo de usuarios o desarrolladores no está de acuerdo con el rumbo que está tomando un programa y decide emprender un *fork* o bifurcación: partir del código ya existente pero darle una orientación diferente. Por lo general, esto no es negativo, sino que proporciona una mayor diversidad y cubre necesidades que un sólo programa no podría cubrir.

Estas cuatro libertades son las que definen el modelo del software libre, y todas sus demás características son consecuencia de ellas. Para que un programa sea considerado software libre, debe facilitar todas y cada una de estas liber-

tades. Por ejemplo, hay software privativo que nos permite ver su código fuente y así comprobar que no hace nada malicioso, pero sin concedernos las demás libertades mencionadas. El *freeware* o software gratuito normalmente tampoco es libre, pues aunque nos permita usarlo y distribuirlo, no nos permite modificarlo. El shareware no es más que una forma de distribución de software privativo: normalmente se nos permite copiarlo, pero no usarlo más allá de un periodo de evaluación.

Por otra parte, el software libre no tiene porqué ser gratuito. La empresa productora o distribuidora puede cobrar la cantidad que estime oportuna por proporcionar una copia. Sin embargo, la propia naturaleza del modelo tiende a la gratuidad, pues una vez que un usuario tiene el programa, goza de todas las libertades del software libre, y tiene perfecto derecho a revenderlo más barato, copiárselo a sus amigos o publicarlo en Internet para cualquiera que lo necesite.

Directrices de software libre de Debian

Debian fue iniciada por Ian A. Murdock en agosto de 1993 y es la distribución de GNU/Linux más antigua que sigue viva. En abril de 1996 pasó a ser coordinada por Bruce Perens, y después por otros. Debian incluye únicamente software libre, por lo que fue patrocinada por la FSF durante un año (de noviembre de 1994 a noviembre de 1995).

Sin embargo, Debian tenía algunas dificultades para determinar si un determinado programa era libre. Había que interpretar cuidadosamente la definición de la FSF y considerar las restricciones de la licencia del programa para ver si encajaban tanto en el espíritu como en la letra. Finalmente, en junio de 1997 Bruce elaboró una serie de características precisas que debía tener un programa para ser considerado libre y poder formar parte de Debian. Las directrices fueron discutidas y refinadas durante un mes, y en julio de 1997 se publicaron las *Debian Free Software Guidelines*. Las DFSG facilitan la clasificación de un programa como libre o privativo comparando su licencia con estas directrices.

Definición de *open source* de la OSI

Con el tiempo, el software libre empezó a suponer una alternativa de bajo coste y alta calidad al software privativo. Sin embargo, el discurso filosófico y moral de la FSF no era del agrado de todos. Para algunos, el software libre simplemente suponía un sistema más eficiente de desarrollo y uso del software, y proporcionaba una serie de interesantes ventajas que estudiaremos un poco más adelante. También estaba el problema de que, en inglés, *free software* puede significar tanto software libre como software gratuito.

Con estos argumentos, Eric Steven Raymond (conocido por ser autor del artículo «La catedral y el bazar» y otros textos y programas), Bruce Perens y algunas otras personas idearon un nuevo concepto: el *open source* o software de código abierto. Con esta nueva denominación pretendían ganar la atención del mundo empresarial, en el que la palabra «libertad» y el ideario de la FSF no despertaba entusiasmos.

Para este fin fundaron la *Open Source Initiative* (OSI). Tras eliminar las referencias a Debian de las DFSG y realizar algún otro cambio menor, publicaron la definición del software de código abierto. Además, registraron una marca de certificación (*OSI Certified*) que un programa puede ostentar si su licencia ha sido aprobada por la OSI como conforme con la definición de software de código abierto.

En la práctica, el software libre y el *open source* son lo mismo, pero mientras un término hace énfasis en los valores éticos de beneficio de la comunidad, libertad, cooperación, etc., el otro recalca las ventajas prácticas, que son, en definitiva, económicas.

Aunque es difícil determinar la importancia que tuvo la nueva denominación, lo cierto es que ese año el software libre empezó a despertar el interés de las empresas, y podemos asumir que no fue por los motivos éticos, sino por las ventajas que proporcionaba. En febrero de 1999, Bruce Perens anunciaba[13] que abandonaba la dirección de la *Open Source Initiative*, pues consideraba que ya habían conseguido la atención del mundo no-hacker y que había llegado el momento de volver a hablar de software libre y de la importancia de la libertad.

Licencias

¿Propiedad? intelectual: copyright, patentes y marcas

Todos conocemos el concepto de «propiedad». Sabemos que, si alguien se cuela subrepticiamente en nuestra casa y se come la tarta que tenemos en la nevera, nos está causando un perjuicio, pues él la disfrutará y nosotros no. También sabemos que podemos ver y tocar nuestras posesiones, pero que, desafortunadamente, la mayoría de las veces no podremos duplicarlas (con la notable excepción de los panes y los peces en manos de Jesús de Nazaret).

En cambio, compartir la receta de nuestra tarta no nos provocaría ninguna pérdida (al contrario, nos proporcionará la gratitud de muchos golosos). Aun después de dar nuestra receta a todas nuestras amistades, la seguiremos teniendo y podremos continuar usándola, mejorándola y compartiéndola durante toda nuestra vida. Observamos, además, que la podemos reproducir de manera indefinida, sin más coste que un poco de saliva (¡y sin necesidad de ser una divinidad!).

Cabe preguntarse, pues, si tiene sentido hablar de «propiedad» en estas condiciones. Evidentemente no se trata de algo inherente a las ideas, sino de un concepto artificial de reciente creación.

Es indiscutible que, aunque determinados trabajos sean inmateriales, sus creadores deben ser recompensados por él, como lo son otros profesionales. En la búsqueda de un mecanismo para estimular a los autores a que aporten nuevas creaciones, la sociedad decidió concederles determinados derechos sobre su obra, durante un tiempo limitado. Sin embargo, hoy se nos quiere hacer creer que no se trata de algo formal, sino que el autor ostenta una propiedad absoluta, equiparable

13. http://slashdot.org/articles/99/02/18/0927202.shtml.

a los objetos físicos, y se utiliza una expresión tan confusa como «propiedad intelectual». En realidad, la mal llamada «propiedad intelectual» agrupa varios tipos de derechos sobre lo intangible que poco tienen que ver entre sí. Confundir copyright, patentes y marcas registradas nos puede llevar a suposiciones incorrectas.

El copyright, tal y como hoy lo conocemos, nació en Estados Unidos en el año 1790, con el fin de impulsar el desarrollo de las artes y las ciencias. El copyright protege las obras literarias, artísticas e intelectuales en su forma, pero no protege las ideas contenidas en esas obras. Consiste en conceder en exclusividad, y durante un tiempo limitado, ciertos derechos de control al autor: copia de la obra, hacer obras derivadas, distribución de la obra, ejecución de la obra...

Diferentes países fueron adoptando legislaciones similares, que desde la convención de Berna en 1881, se han ido uniformando paulatinamente. Hoy el copyright se aplica automáticamente y, si no se indica lo contrario, se entiende que el autor se reserva todos los derechos.

Estos derechos, por otra parte, están sometidos a ciertas limitaciones, como los derechos de «uso justo». Este derecho permite usar una obra con propósitos de crítica, comentario, información de novedades, investigación, etc. Pasado el tiempo legislado, la obra pasa a ser «de dominio público» y ya no hay ninguna restricción respecto a cómo se puede usar, modificar o distribuir la obra.

En Estados Unidos este tiempo era inicialmente de 14 años, pero se ha ido alargando progresivamente. Actualmente es la vida del autor más 70 años, o 95 años si se trata de una empresa. Si bien el propósito original del copyright era recompensar al autor, ahora no sólo le recompensa de por vida, sino también a sus nietos y hasta a los nietos de sus nietos[14]. Se dice que Disney, que no quiere conceder la jubilación a Mickey Mouse, tiene algo que ver con esto.

Otra forma de protección es la «propiedad industrial», entre las que se incluyen las patentes y los signos distintivos. Las patentes tienen por propósito el fomento de la investigación y el desarrollo tecnológico, y protegen una invención particular, que debe cumplir con ciertos requisitos como originalidad, no trivialidad y aplicación industrial.

Una patente reconoce el derecho de explotar en exclusiva la invención patentada, impidiendo a otros su fabricación, venta o utilización sin consentimiento del titular. Mientras el secreto industrial hace que los competidores tengan que *inventar* por segunda vez los aparatos que ya existen (una forma ineficiente de usar los recursos), con las patentes el inventor tiene un incentivo económico para hacer públicos sus descubrimientos. Al cabo del plazo de validez de una patente (20 años), la sociedad dispone de las especificaciones del invento que puede usar libremente.

Presentan el inconveniente de que si dos personas desarrollan de forma independiente el mismo invento, sólo una podrá patentarlo, y la otra ni

14. Stephen Joyce, el ya septuagenario nieto de James Joyce, defiende agresivamente los derechos que ha heredado, hasta el punto de prohibir varios actos del 100 aniversario de la novela *Ulises*, que se celebró en Dublín en junio de 2004. Finalmente, para evitar sus desaforadas exigencias y poder exhibir los manuscritos originales, el Parlamento irlandés tuvo que modificar la ley con carácter de urgencia.

siquiera tendrá derecho a usarlo sin el pago que le exija la otra. Tampoco es raro que las pequeñas empresas no dispongan de los recursos necesarios para patentar y hacer valer sus invenciones[15].

Los signos distintivos (marcas y nombres comerciales) son un nombre o signo único que identifica a un producto, servicio o empresa y evita que se pueda confundir con otro. Ocasionalmente esta protección puede dar lugar a abusos, aunque no es frecuente[16].

Curiosamente, ésta es la razón por la que GNU/Linux y *BSD no son Unix. Como dicen en NetBSD: si algo parece un pato, camina como un pato y hace cuac como un pato, ¿qué es? ¡La respuesta depende de si la palabra «pato» es una marca registrada! Si lo es, a lo más que podemos acercarnos, sin permiso del propietario de la marca, es a que «es como un pato». Unix es una marca registrada de The Open Group, y para poder usarla en un producto, además de pasar unas pruebas, hay que pagar una importante cantidad de dinero. Por eso se les llama «sistemas de tipo Unix».

La licencia BSD: libertad sin control

La propiedad de los objetos físicos la conocemos bien. Cuando compramos una silla, sabemos que podemos usarla para sentarnos, pero también subirnos sobre ella para alcanzar los estantes más altos, regalársela a un amigo, destrozarla si nos cansamos de ella o, mejor, pintarla de otro color. En definitiva podemos hacer lo que queramos con ella, pues es nuestra y para eso la hemos pagado.

En cambio, cuando vamos a una tienda y pagamos por un CD de música, no pasamos a ser los dueños de esas canciones: únicamente estamos adquiriendo un soporte físico, un pequeño libreto (eso si tenemos suerte) y unos determinados derechos de uso no exclusivo. Dicho de otra manera: a cambio de nuestro dinero, aparte de un poco de plástico y papel, lo que obtenemos es un permiso para usar de cierto modo y bajo ciertas condiciones el contenido del CD.

Los programas informáticos, al igual que la música, se protegen mediante el copyright. Al igual que el cantautor Lluís Llach pudo prohibir en marzo de 2002 que la policía cantara su canción *L'estaca*, el propietario del copyright de un programa tiene el control legal de quién y cómo puede usar dicho programa.

Una licencia es un documento por el cual el propietario de la obra concede (frecuentemente tras el abono de cierta cantidad de dinero) ciertos derechos bajo determinadas limitaciones. Por ejemplo, puede disponer que el licencia-

15. El caso del teléfono es paradigmático: lo inventó el inmigrante italiano Antonio Meucci, quien no tenía los 250 dólares necesarios para obtener una patente definitiva, así que el 28 de diciembre de 1871 se limitó a pagar la solicitud preliminar, renovable anualmente por 10 dólares. Tres años después, ni siquiera disponía de los 10 dólares necesarios para renovarla. Así, Alexander Graham Bell pudo conseguir la patente en 1876 y amasar una fortuna. La disputa entre Meucci y Bell llegó a los tribunales, pero Meucci murió durante el proceso.

16. Por ejemplo, en noviembre de 2002 la Hermandad de Nuestro Padre Jesús del Gran Poder consiguió que la Guardia Civil detuviera a un programador y se incautara de cientos de CD por violar su propiedad industrial: la cofradía había registrado como marca la imagen del Jesús del Gran Poder (tallada en 1620) que el informático había usado en un videojuego. Hacia las mismas fechas, la Sociedad General de Autores y Editores consiguió clausurar el dominio putaSGAE.com, una web crítica con sus prácticas.

BELL Y LOS PHREAKS

Alexander Graham Bell, profesor de fisiología vocal y electricista aficionado, fue oficialmente el inventor del teléfono. En marzo de 1874, A. G. Bell se convirtió en la primera persona que logró transmitir eléctricamente voz humana comprensible cuando el Sr. Watson, elementalmente su ayudante, oyó a través del audiotelégrafo experimental los aullidos y tacos del Profesor al derramársele, no se sabe dónde, una botella de Ácido.

Como todo invento que promete, éste necesitaba de dinero para seguir desarrollándose, por lo cual Bell decidió hacer una gira con su dispositivo como atracción de feria. Parece ser que la prensa de la época decía que el debut del teléfono provocó una mezcla de asombro y miedo en la gente.

tario sólo lo puede usar en una computadora, que sólo puede hacer una copia de seguridad y que no puede redistribuirlo a otras personas.

Naturalmente, también se pueden conceder licencias más permisivas, como son las del software libre. Como hemos visto, el sistema BSD se publicó bajo una licencia muy sencilla[17] por la que se concedía a los licenciatarios libertad para usarlo, copiarlo, modificarlo y distribuirlo como quisieran, con lo que podían incluso usarlo para crear binarios bajo una licencia privativa.

Básicamente, la única restricción era que cualquier tipo de publicidad que explicitara funcionalidades o uso de ese software debía hacer mención de la Universidad de California y sus colaboradores. Inicialmente, esto no era un problema, pero otros desarrolladores usaron esta misma licencia reemplazando el nombre de la universidad por el suyo propio o el de su institución.

Sin embargo, al combinar varios de estos trabajos (en una distribución, por ejemplo) podía resultar que hiciera falta una página entera de reconocimientos. Esto no es una exageración: en 1997, NetBSD incluía 75 de estas frases. La Universidad de California derogó[18] esta cláusula, con efectos retroactivos, el 22 de julio de 1999. Muchos otros autores, como los de FreeBSD, también lo han hecho, pero todavía hay trabajos que mantienen esta pequeña pero molesta restricción.

GPL: nace el copyleft

La FSF tuvo que enfrentarse a una situación paradójica. Si publicaban su software como de dominio público o bajo una licencia muy permisiva, como la BSD modificada, corrían el riesgo de que alguna empresa lo tomara, modificara y redistribuyera como software privativo. Ya había pasado con el sistema de ventanas X, que aunque había sido desarrollado en el MIT como software libre, normalmente llegaba a los usuarios bajo una licencia privativa.

17. http://www.freebsd.org/copyright/license.html.
18. http://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change.

En un principio Bell tenía la idea de convertir el teléfono en un medio de masas, es decir, sería a traves del teléfono que se transmitiría música, discursos, etc. Esta idea cuajó pues parecía que sonaba bien, de hecho en Hungría se utilizó el teléfono de esta forma diariamente y con éxito. En Budapest, desde 1893 hasta después de la Primera Guerra Mundial, había un servicio de información pertenenciente al gobierno llamado «Telefon Hirmondo1/2», una fuente centralizada de noticias, entretenimiento y cultura, incluyendo información bursátil, obras de teatro, conciertos y lecturas de novelas.

Este concepto del teléfono no está muy lejos de los inicios de los servicios informáticos de datos a través de línea telefónica, como Compuserve o Prodigy. Compuserve, fundada en 1969, fue la primera en poner en marcha una industria de servicios *on-line*. En 1979, Compuserve se convirtió en el primer servicio en ofrecer correo electrónico y servicio técnico destinado a los usuarios, en 1980 se

El objetivo de la licencia BSD era promover el desarrollo de la industria y el uso de estándares abiertos. Sin embargo, la meta del proyecto GNU no era ser popular y tener muchos usuarios, sino proporcionar libertad a los usuarios. Por tanto, idearon unos términos de distribución que impidieran que el software GNU pudiera ser convertido en software privativo. Haciendo un nuevo juego de palabras, bautizaron al método como *copyleft* o izquierdos de autor, un término que había sido acuñado por Don Hopkins en oposición al *copyright* o derechos de autor tradicionales.

El copyleft es un *hack* de las leyes internacionales del copyright. Se basa en ellas, pero las usa de tal modo que, en vez de servir para mantener un software privativo, sirven para mantenerlo libre. La idea central del copyleft es autorizar a cualquiera para usar el programa, copiarlo, modificarlo y distribuir versiones modificadas, pero con la restricción de que no se permite añadir más restricciones a dichas versiones. De esta manera, las libertades concedidas por el autor original se convierten en inalienables, y ese código ya no puede ser mutado a privativo. Hay quien objeta que este tipo de licencias son menos libres, pues tienen una restricción importante (prohibido prohibir), pero para la mayoría esto no es un problema, sino una atractiva funcionalidad.

Al principio, la FSF implementó esta idea en una licencia individual para cada programa. Esto tenía el inconveniente de que había que adaptarla para cada paquete (una para Emacs, otra para NetHack, etc.), y hacer todavía más modificaciones para que otros programadores pudieran emplearla en sus propios programas.

Finalmente, en febrero de 1989 publicaron la primera versión de la Licencia Pública General de GNU[19], o GNU GPL. Esta licencia, escrita en un intrincado lenguaje legal, puede emplearse en cualquier programa sin necesidad de modificaciones, sin importar quien lo publique. Sólo hace falta una breve nota en el propio programa, indicando que se publica bajo dicha licencia.

19. http://www.gnu.org/copyleft/copying-1.0.html.

ofreció el primer chat *on-line* y en 1982 la compañía amplió sus servicios de redes a empresas. Prodigy, fundada en 1984, fue el primer proveedor de servicios de Internet en América.

Bell y sus patrocinadores tuvieron que enfrentarse, como suele suceder, al escepticismo y competencias de otras industrias, donde el telégrafo era considerado el medio «serio», mientras que el teléfono era un mero «juguete eléctrico».

Así que para hacer del invento algo productivo y mostrárselo al mundo, el concepto original del teléfono dio un giro. Bell y sus patrocinadores concluyen que una música procedente del ciberespacio del siglo XIX no era lo que iba a vender el invento. El teléfono encontraría su lugar con la voz personal e individual, conversación e interacción humana, de manera que se convierte en una tecnología personal e íntima.

En junio de 1991 se publicó la versión 2 de la GPL, que muchos consideran una auténtica obra de arte o de ingeniería legal, para la que no ahorran elogios. El sistema GNU oficial se compone de unos pocos cientos de paquetes, pero hay miles de programas libres que funcionan sobre él, y la inmensa mayoría de ellos están publicados bajo esta licencia, al igual que el núcleo Linux.

Redactada por el abogado Eben Moglen, su solidez ha levantado airadas críticas de empresas como Microsoft, que han arremetido contra ella calificándola de «antiamericana», «comunista», «cáncer para la industria», etc. El caso es que el copyleft les impide llevar a cabo una de sus prácticas favoritas: la de comprar las empresas competidoras.

Otras licencias

Hay muchas otras licencias de software libre, tanto con copyleft (*Affero General Public License, GNU Lesser General Public License, IBM Public License, Mozilla Public License*, etc.) como sin él (*Apache Software License, Eiffel Forum License, Q Public License, Sun Industry Standards Source License*, etc.). Algunas de ellas son muy sencillas, mientras que otras pueden ser bastante complicadas, pero todas proporcionan las cuatro libertades básicas del software libre. La FSF mantiene en su web una lista de licencias que cumplen la definición de software libre, y la OSI otra de las que cumplen la definición de *Open Source*.

Más allá del software

El espíritu del software libre se puede llevar a otros tipos de información, pues ésta siempre se puede duplicar a un coste prácticamente nulo. La FSF constató que, además de software libre, también hacía falta documentación libre que explicara cómo funciona ese software. Para ello creó la *GNU Free Documentation License*, que está pensada para documentación técnica (aunque no necesariamente de software). Además de la GNU FDL, existen otras licencias libres de

A partir de 1890, la red telefónica se empieza a expandir a gran velocidad y hacia 1904 se extendía por todo el continente norteamericano.

Bell era el prototipo de empresario dedicado a la alta tecnología y, como tal, no sólo desempeñará un papel importante en los ámbitos técnicos sino que, también como pionero de la frontera electrónica, podrá partir el bacalao en la arena política y social. Bell defendió con uñas y dientes la exclusiva de sus patentes; en los 18 años que duraron dichas patentes se enfrentó a 600 causas, ganándolas todas. Después de que expiraran sus patentes, las compañías telefónicas empezaron a expandirse. AT&T (American Telephone and Telegraph) se adueñó de Bell, estando al frente de aquélla Theodore Vail. Tanto la política de empresa de Bell como la de Vail se basaba en los principios democráticos del «acceso universal». El teléfono americano no iba a convertirse en un

documentación como la *FreeBSD Documentation License* y la *Apple's Common Documentation License*.

La FDL sirve igualmente para libros de texto o diccionarios. Así, numerosos voluntarios han creado a través de Internet Wikipedia, una completa enciclopedia bajo esta licencia. Se basa en el uso de un tipo de programa llamado wiki, que permite a cualquiera editar cualquier artículo de manera sencilla. En caso de que alguien hiciera modificaciones malintencionadas, es posible deshacer los cambios y devolver el artículo a su estado anterior.

A pesar de que hoy el mundo avanza mucho más rápido que en 1790, el periodo de protección del copyright se ha multiplicado increíblemente. Deberíamos plantearnos si hay un equilibrio entre lo que el autor aporta a la sociedad y lo que ésta cede: no parece normal que algunos artistas se hagan multimillonarios por poco más de media hora de música.

Por otra parte, lo más frecuente actualmente es que el copyright, más que recompensar a los autores (ya sean éstos músicos, escritores o programadores), sirva para generar pingües beneficios a las empresas intermediarias, a las que los autores se ven obligados a ceder sus derechos.

Son estas empresas las que han presionado a los gobiernos y logrado que las leyes sean cada vez más extensivas, empezando a afectar gravemente nuestra vida cotidiana. La imprenta fue un vehículo extraordinario para la expansión de la cultura, pero ahora, cuando más fácil y económico es acceder a ella, no hacen sino poner trabas, llegando al extremo de gravar con un canón el préstamo de libros en las bibliotecas públicas. Cada vez que un avance tecnológico amenaza su imperio, intentan detenerlo. En su momento pretendieron ilegalizar los aparatos domésticos de vídeo, y ahora intentan criminalizar el uso de Internet, la grabación de CD-ROM, etc. Últimamente están desarrollando e intentando imponer unas tecnologías llamadas DRM (*Digital Rights Management*), que podrían hacernos perder el control de nuestras computadoras. Básicamente pretenden someter el mundo de

herramienta especializada del gobierno ni del mundo empresarial, sino en un bien público.

Los teléfonos estaban valorados especialmente por pertenecer al ámbito doméstico, permitían la relación social; la gente perdió el miedo a esta alta tecnología cuando empezó a oír a sus familiares, amigos, en sus propias casas. El teléfono pasó a ser una pieza clave en la vida cotidiana de la comunidad humana.

Las comunidades electrónicas que fueron surgiendo en los años ochenta cobraron conciencia de su existencia, cuando en 1990 se desencadenó la primera caza de hackers; a quien se estaba atacando no era a individuos aislados que se encontraban en sus casas, sino a toda una comunidad. No se trataba de niños haciendo trastadas con un juguete, sino que se convertía en la lucha por la supervivencia de una comunidad y la lucha por un nuevo espacio, el ciberespacio.

la cultura a sus intereses comerciales, polarizarlo de modo que haya unos pocos creadores bajo su control y que el resto seamos consumidores pasivos de su cultura.

Por todo esto, otros colectivos han llevado la filosofía del software libre a diversos tipos de manifestaciones artísticas (literatura, música, fotografía, cine, etc.), para lo que han creado licencias específicas. El sitio web Creative Commons[20] es un importante punto de encuentro para artistas con estas inquietudes, que prefieren usar las nuevas tecnologías para dar a conocer su obra al mayor público posible.

Praxis: cómo y por qué se desarrolla el software libre

Por qué: valores éticos y motivos prácticos

Cuando RMS inició el proyecto GNU, no pensaba que el software libre iba a contar con millones de usuarios y sería empleado en la mayoría de las empresas. Lo que ha pasado es que, con el tiempo, ha resultado que el software libre no sólo es mejor desde una perspectiva filosófica, sino también práctica, que es la que publicitan los seguidores del *open source*.

Desde hace algunos años se nos viene enseñando que «copiar es malo», sin más; quien lo hace es un «pirata», un delincuente de la peor calaña. Pero si prestamos atención a nuestro entorno o si nos remontamos atrás en el tiempo, comprobaremos que no es cierto. Constantemente redistribuimos chistes, noticias, rumores, etc. En tiempos pasados también los libros se copiaban (entonces era una labor tediosa, pues se tenía que hacer a mano). En cambio, hoy en día la biblioteca de Alejandría sería considerada la sede de una mafia o red de malhechores, y sería objeto de intervención policial, y los fantásticos conocimientos que albergaba serían destruidos en nombre de la propiedad *intelectual*.

No cabe duda de que ayudar y colaborar con nuestros amigos y vecinos es bueno para la sociedad, de lo que se deduce que publicar, copiar, mejo-

20. http://creativecommons.org.

En el transcurso de la operación «Sundevil», la actuación de las fuerzas de la ley y el orden contra «las actividades ilegales de hacking», se detiene a tres personas. Se estimaban unas pérdidas en los ingresos de compañías telefónicas de millones de dólares debido a las actuaciones criminales del «*underground*», según el comunicado de prensa que ofrecieron las autoridades.

En estos momentos los grupos *underground* se comunicaban a través de sistemas de mensajería entre ordenadores conocidos como BBS (Bolletin Board Systems), que usaban las líneas telefónicas para conectarse. Los *phreaks*, pioneros pobladores del *underground*, fueron quienes las pusieron en marcha y las mantuvieron. Fue interesante su relación con el movimiento yippie, por donde andaban Abbie Hoffman y Jerry Rubin, que acabó siendo un broker de Wall Street, mientras que Hoffman era buscado por las autoridades federales y tuvo que permanecer escondido siete años de

rar o traducir programas informáticos es lo correcto, mientras que guardárnoslos para nosotros es antiético.

Por ello el software libre no precisa necesariamente de financiación: muchos programadores lo escriben en su tiempo libre, simplemente por el placer de programar y colaborar con otros hackers o bien para satisfacer una necesidad personal; y después lo publican para ayudar a quien le pueda ser útil, pues no pierden nada al hacerlo. Asimismo, hay mucha gente que, sin saber programar, colabora haciendo traducciones, dibujando iconos o escribiendo documentación, en agradecimiento por haber recibido como software libre un programa que les resulta particularmente útil. Estas maneras de contribuir están al alcance de cualquiera que disponga de un poco de tiempo. Quien no lo tenga, aún puede ayudar usando software libre, difundiéndolo, informando de fallos, aportando sugerencias o haciendo una aportación económica.

Tampoco todos lo hacen por altruismo. Las motivaciones no directamente económicas son muchas: pueden hacerlo por aprender, practicar y adquirir experiencia, darse a conocer[21], etc., o simplemente mejorar un programa que también ellos utilizan, por lo que se unen al grupo de desarrollo. Se habla entonces de *colaboración egoísta*.

Es sabido que el principal objetivo de cualquier empresa es ganar dinero, y que algunas de las empresas de informática más grandes del mundo (IBM, Novell, Sun, etc.) están invirtiendo enormes sumas de dinero en el software libre. En general, podemos descartar la filantropía, así que ¿por qué lo hacen?, ¿por qué cada vez más empresas usan y desarrollan software libre?

Los mecanismos económicos del software libre todavía están en estudio, y no será aquí donde se explique cómo ganar dinero con él, pero sí se intentará explicar algunas de sus ventajas y posibles modelos de negocio.

21. En ocasiones, cuando un proyecto destaca por ser especialmente interesante, alguna empresa contrata a su principal desarrollador y le paga para que siga trabajando, ahora a tiempo completo, en su proyecto.

nada. Continuó escribiendo y publicando con la ayuda del *underground* americano hasta que se entregó. Podéis ver el cacho dedicado a los Yippies en el *Manual de la Guerrilla de la comunicación* o también en *El asalto a la Cultura* de Stewart Home, ambos publicados, mira tú por donde, en esta misma editorial.

Abbie Hoffman era considerado una amenaza pública. Publicista con talento, utilizaba los medios electrónicos como un juego y como un arma. Le gustaba participar en la manipulación de la televisión por cable y otros medios ansiosos de imágenes, generaba rumores, mentiras, suplantaciones y todo tipo de distorsiones del medio.

Rubin escribió un libro llamado *Roba este libro* —ilustre precedente del *Libro Rojo* y el *Libro Morao* de Yomango—, donde divulgaba todo tipos de métodos para que los diferentes agitadores se

Las prácticas de las empresas de software privativo han conducido a situaciones de monopolio en las que no hay competencia, y en las que por tanto las empresas líderes aplican márgenes abusivos y no necesitan trabajar para mejorar la calidad de su producto ni atender a las peticiones y quejas de sus clientes, pues éstos no tienen ninguna alternativa viable.

De hecho, la mayoría de las pequeñas empresas de software se dedican a escribir software a medida, por encargo, y no intentan comercializar programas, pues es prácticamente imposible que una empresa consiga vender un programa alternativo al dominante (sea éste un procesador de textos, un maquetador o cualquier otro), aunque sea mejor y más barato, pues generalmente los usuarios prefieren comprar el programa que usa todo el mundo y no el que les ofrece una pequeña empresa local. De intentarlo, esta empresa tendría además que invertir previamente una importante cantidad de dinero en *marketing* para lograr introducirse en los principales canales de distribución. Lo más probable es que acabe arruinada o, si consigue tener cierto éxito, sea absorbida por sus grandes rivales. Esto provoca que el software privativo avance lentamente y sea caro de producir.

En cambio, en el caso del software libre la situación es más equilibrada, y se compite en una cierta igualdad de oportunidades. Para empezar, un nuevo proyecto puede apoyarse en la miríada de bibliotecas y funciones ya existentes, ahorrándose la necesidad de volver a programar lo que otros ya han hecho antes. Además, cada proyecto puede tomar ideas e incluso el código de los programas rivales, basarse en otro ya existente, etc., con lo que todos se benefician y desarrollar un programa es más rápido y más económico.

El software libre no tiene porqué ser gratuito, aunque con frecuencia lo sea. En general, las empresas desarrolladoras no obtienen sus ingresos de la venta de licencias, sino de servicios como implantación, soporte, mantenimiento, cursos de formación, certificación de profesionales, consultorías, adaptación del programa a casos particulares e incluso *merchandising*.

buscaran la vida sin dinero. Hizo extensivo el uso de teléfonos de pago usando chapas baratas de metal como monedas falsas.

Durante la guerra del Vietnam, había un impuesto sobre el servicio telefónico. Hoffman y compañía robaban a la compañía telefónica como una forma de desobediencia civil, como forma de negar el pago para financiar la guerra. Ya en esas, a principios de los años setenta, Abbie Hoffman y All Bell publicaron un boletín de noticias conocido como *Party Line de la Juventud Internacional*, dedicado a reunir y divulgar las técnicas yippies de destripar sobre todo los teléfonos. Como táctica política, el robo de servicio telefónico garantizaba a los defensores de los yippies acceso a llamadas de larga distancia.

All Bell, unos años más tarde, dejó el movimiento yippie y rebautizó al boletín con el nombre de *TAP* (Technical Assitance Program). Poco a poco, la gente que se movía entorno al *TAP* alcanzaron un

El hecho de que cualquiera pueda acceder al código fuente de un programa hace que los programadores sean más cuidadosos[22] con su código y eviten hacer chapuzas de las que podrían avergonzarse después. Esto no significa que todos y cada uno de los programas libres sean de mayor calidad que los privativos, pero sí que tienen un mayor potencial. Para una empresa de este tipo esto significa un importante ahorro de costes en su modelo de negocio.

Para las empresas usuarias de software, además del menor o ningún coste de las licencias, el software libre tiene la ventaja de que pueden elegir quién le proporcionará los servicios de mantenimiento y soporte, pues las opciones ya NO se limitarán a la empresa productora. Una vez más, esto redunda en un mejor precio y servicio, pues la mayor proximidad de los programadores y la existencia de competencia implica que sus quejas y sugerencias sean atendidas. En consecuencia, los programas libres se adaptan mejor a las necesidades de los usuarios y tienen menos fallos que sus contrapartidas privativas. Por todo ello, el software libre ofrece generalmente a las empresas usuarias unos índices de coste total de propiedad y de retorno de inversión más atractivos que el software privativo.

Algunas empresas ofrecen sus productos bajo dos licencias, una libre y otra privativa[23]. Gracias a la primera pueden ser empleados por usuarios y desarrolladores de software libre, mientras que la segunda exige el pago de una licencia a los desarrolladores de software privativo. Cuando alguien contribuye con un parche a un proyecto de este tipo, para que entre en la rama principal se le pide que acepte que se pueda publicar también bajo la licencia privativa.

También muchas empresas de hardware están interesadas en el software libre. Hoy en día, el coste de las licencias de los programas instalados en una

22. Un estudio de la empresa Reasoning de diciembre de 2003 analizó la calidad del código de varias bases de datos, y concluía que el del proyecto libre MySQL era seis veces superior al de los productos privativos (http://www.reasoning.com/newsevents/pr/12_15_03.html).

23. El ejemplo más conocido es la empresa noruega Troll Tech. Sus bibliotecas Qt están disponibles bajo dos licencias libres (GPL y QPL), por lo pueden ser empleadas por proyectos como KDE, pero también lo están bajo una licencia privativa, que muchas empresas de desarrollo de software cerrado adquieren por su altísima calidad.

alto nivel técnico. A finales de los setenta, All Bell dejó el boletín cuando los lectores de *TAP* eran unos 1.400 y los sistemas de ordenadores iban creciendo.

Mientras tanto, en la calle las cabinas telefónicas eran reventadas y estudiadas con detenimiento para ver cómo podían burlarse los sistemas de pago, ya sea con pedazos de hielo con forma de moneda, palancas, imanes, ganzúas, petardos...

Y eso se hacía extensible al empleo de trucos en las líneas para que las llamadas salieran más baratas, a precio de llamada local. Eran los *phone phreaks* los que se dedicaban a estas lindezas. El primero de los *phone phreaks* fue John Draper, luego conocido como *Capitán Crunch*, porque conseguía hacer llamadas gratuitas con el silbato de juguete que venía en los cereales Captain Crunch y una *blue box* o «caja azul». Las «cajas azules» eran ingenios capaces de abrir la línea, enviar un tono de 2600 hz

computadora suele ser muy superior al coste de la propia máquina. Estas empresas apoyan el software libre porque si se reduce el coste del software, las empresas usuarias podrán permitirse comprarles más y mejores máquinas.

Lo cierto es que durante los últimos 25 años se ha invertido muchísimo dinero en software privativo y poquísimo en software libre, y lo cierto es que, a día de hoy, el software libre es comparable al privativo (si bien es muy superior en algunas áreas, todavía está a la zaga en otras), de lo que se concluye que, económicamente, el modelo del software privativo es muy ineficiente, en comparación con el del software libre.

Cómo: la catedral y el bazar

El software libre, además de sus valores éticos, ha supuesto un nuevo sistema de desarrollo de software. Siguiendo la ingeniería del software tradicional, los programas se desarrollaban de manera muy estructurada por grupos cerrados de gente liderados por un analista. Cuando la FSF inició el desarrollo del sistema GNU, si bien invitaba a los voluntarios a entrar en el círculo, siguió prácticamente el mismo modelo, y a cada persona se le asignaba una tarea muy específica. Fue el joven Linus Torvalds quien tuvo la genial intuición de lanzar su mensaje a USENET y dejar que la gente aportase lo que considerase oportuno en vez de seguir un plan preestablecido. Prácticamente todos los proyectos de software libre han adoptado esta misma metodología. Eric S. Raymond estudió este fenómeno, denominando al método centralizado «catedral» y al distribuido «bazar».

Examinemos rápidamente las características del modelo bazar. Lo primero que llama la atención es que los proyectos suelen estar desarrollados por grupos de hackers distribuidos por todo el mundo, que no se conocen entre sí, sino que simplemente comparten un interés común, de modo que forman una comunidad más o menos difusa. Cualquier persona con los mismos intereses puede cola-

—que era el tono de control que usaban los operarios de las compañías de teléfono— y acceder a controlar la operadora con las teclas de tono u otros pitidos, para luego decirle que se quería llamar «de prueba» a tal teléfono, obteniendo como resultado llamadas gratuitas a larga distancia. Luego salieron otras «cajas», como las «cajas negras» o *black box*, que eran una resistencia que anulaba el envío de la señal eléctrica que indicaba a la centralita que se había recibido la llamada y que hacía que el tarificador echase a andar; y, por tanto, las llamadas que recibían los receptores eran gratis.

Steve Jobs y Steve Wozniak, los fundadores de Apple Computer Inc., se dedicaron a vender cajas azules en los colegios mayores de California. En esos momentos el uso de dichas cajas no era considerado un delito. Si estaban las líneas ahí, no se usaba toda su capacidad y no se producía ningún daño, ¿por qué no se iban a usar?

borar e incorporarse al equipo de desarrollo. Sin duda, el hecho de trabajar en algo que les gusta les lleva a poner más esmero e incluso cariño en lo que hacen.

Para coordinarse utilizan listas de distribución de correo electrónico. Mediante ellas intercambian sus objetivos, puntos de vista, críticas, etc. En cada proyecto suele haber un *dictador benevolente* (normalmente el fundador del proyecto) que debe coordinar y motivar a los demás desarrolladores, así como buscar consensos. En proyectos grandes no suele haber un único líder, sino un grupo de ellos elegidos por los demás desarrolladores en base a sus méritos (cuánto contribuyen al proyecto). En casos de desacuerdo irreconciliable, el coordinador tiene la última palabra, pero nadie está sometido a ella, sino que puede iniciar su propio proyecto a partir de lo hecho hasta el momento (lo que se denomina *fork* o bifurcación). Cuando un líder no puede o sabe cumplir adecuadamente su papel, debe ceder el testigo a otro desarrollador, para que el proyecto continúe con vigor.

Para poder trabajar varias personas a la vez sobre el código de un programa se han desarrollado sistemas de versiones concurrentes a través de Internet, como CVS, Subversion o Arch, que al tiempo que permiten que cualquier desarrollador pueda añadir sus aportaciones, permiten retirarla y volver al estado anterior en caso de que contuviera algún error. Es bien sabido que un sistema libre como GNU/Linux o *BSD tiene muchos menos fallos de seguridad y peligro de ser atacado por un virus informático que otro privativo como Microsoft Windows. Esto se debe también al carácter colaborativo del desarrollo. Por una parte, se discuten y analizan las ventajas e inconvenientes de los distintos diseños posibles, y por otra, si un programador comete un fallo, es muy probable que haya otro que lo detecte y solucione.

Además, los programas no son publicados cuando las exigencias del *marketing* indiquen, sino cuando se considera que los programas están preparados. Es frecuente que haya dos ramas en paralelo del programa: una estable, apta para su uso en entornos productivos, y otra de desarrollo, para quienes quieran estar a la última. El ciclo de publicación de las versiones de desarrollo suele ser muy rápido, y es habitual

El dominio del funcionamiento de las líneas y, sobre todo, poder disponer de los «mejores precios» de conexión hizo que la comunicación a través de las BBS (Bulletin Board System) se incrementara rápidamente, y con ello comenzaron a surgir las comunidades de personas que trabajaban conjuntamente pese a estar en distintos puntos del planeta.

Las BBS son el punto de encuentro del mundo *underground*, miles de personas crean BBS para intercambiar todo tipo de conocimiento. Al ser conocedores de sistemas de telefonía, consiguen conexiones gratuitas, se intercambian códigos, programas, textos, recetas para crackear líneas, entrar en compañías, etc. Un BBS es un ordenador al que uno se puede conectar para intercambiar mensajes y archivos con otras personas que se conecten a él. Los BBS se conectan entre sí para formar redes de intercambio de mensajes (por ejemplo FidoNet). Así se tiene el equivalente al e-mail, el

que cada año se publiquen varias versiones del programa. Esto permite que los usuarios adopten rápidamente las nuevas versiones, encuentren los inevitables fallos y sugieran nuevas mejoras, que serán atendidas por los desarrolladores, y que se repita el ciclo. Cuando la versión de desarrollo tiene cierta cantidad de nuevas funcionalidades y es estable, pasa a ser la versión de producción y se crea una nueva rama de desarrollo.

Aun así, el desarrollador de Linux, Alan Cox, ha hecho notar que este modelo tampoco está exento de problemas. En concreto ha descrito lo que ha denominado el «consejo municipal»[24], que se produce cuando en un proyecto hay muchas personas que dan ideas y críticas, pero pocas o ninguna realmente hace algo. Este efecto *opinódromo* puede afectar especialmente a proyectos que empiezan de cero, sin un código base del cual partir, por lo que es importante empezar a publicar código cuanto antes, aunque todavía no sea muy funcional.

Poul-Henning Kamp, de FreeBSD, describió un fenómeno similar que denominó «discutir por el color del cobertizo para bicicletas»[25]. Explica que las cosas grandes y complicadas se llevarán a cabo sin mucha discusión, precisamente por su complejidad, mientras que las cosas sencillas recibirán un montón de atención por parte de gente que querrá hacerse notar y discutirá sus más insignificantes detalles, provocando finalmente una discusión recurrente en la que nunca se alcanzará un consenso.

Otro obstáculo es que con demasiada frecuencia el diseño del programa no está documentado, lo que supone un cierto esfuerzo de familiarización para el programador que entra en un proyecto ya avanzado.

A pesar de estos posibles inconvenientes, el modelo bazar ha demostrado ser extraordinariamente eficiente y capaz de producir programas de mayor calidad con menos recursos. Los partidarios del término «*open source*» esgrimen esto como su principal motivación, mientras que los seguidores de la filosofía

24. http://slashdot.org/features/98/10/13/1423253.shtml.
25. http://www.freebsd.org/doc/en_US.ISO8859-1/books/faq/misc.html#BIKESHED-PAINTING.

netmail, y el equivalente a los grupos de noticias, el echomail. Pero la diferencia más importante con Internet no es la tecnología, es la filosofía. La mayoría de los BBS son amateurs, y el administrador (el sysop, SYStem OPerator) se mantiene pagando los gastos de su bolsillo. Así pues, el correo comercial está prohibido. En el echomail se encuentra la segunda diferencia. Las áreas de echomail, equivalente a los diferentes grupos de noticias, están moderadas, con lo que se elimina el «correo basura» y la mayoría de los off-topics.

La gente que se agrupa entorno a las BBS son de todas las edades, sexos, condiciones sociales; así los phreaks no tienen el perfil de chicos jóvenes adolescentes, de color blanco espectral, que nunca salen de sus habitaciones, imagen que se asociará a los hackers informáticos.

A día de hoy, el *phreaking* sigue estando de plena actualidad. Objetivos vulnerables son los telé-

del software libre explican que no es el objetivo final, sino simplemente una consecuencia de la libertad del software, que es lo realmente importante.

Apto para todos los públicos

Inicialmente, el software libre estaba escrito por y para informáticos. La mayoría de los programas se usaban desde la línea de órdenes y los entornos gráficos eran francamente espartanos. Sin embargo, esto hace ya años que empezó a cambiar, y hoy en día hay magníficos entornos de escritorio como KDE y GNOME, y programas para llevar a cabo todas las tareas corrientes: procesadores de textos, hojas de cálculo, grabación de CD, visualización de DVD, escucha de MP3 y Ogg, fotografía digital, etc.

La manera más simple de asomarse al software libre es quizá empezar a usarlo sobre Windows. En efecto: también hay programas libres para Windows. Sobre esta cuestión hay un debate abierto en la comunidad: unos piensan que crear software libre para Windows es contraproducente, argumentando que disponer de software libre para Windows reduce los alicientes de cambiar de sistema operativo, mientras que otros afirman que esto les permitirá saborear el software libre fácilmente y les motivará a dar el salto.

Otra posibilidad más interesante es probar un *live-CD* como Knoppix o X-Evian, que nos permitirá usar GNU/Linux en nuestro PC sin necesidad de instalar nada en él.

Instalar una distribución de GNU/Linux o *BSD no es especialmente complicado, pero si no tenemos mucha confianza en nuestras habilidades informáticas, lo más sencillo y cómodo es invitar a merendar a un amigo *friki* y pedirle que traiga unos CD para instalarlos en nuestro ordenador. La facilidad de uso de los entornos KDE y GNOME es tal hoy en día que una vez instalado probablemente no necesitemos ninguna ayuda para manejarnos con ellos.

fonos móviles, pues se puede mostrar un identificador falso y llamar gratis, hacer un *diverting* o acceso a compañías locales, conseguir sus claves y hacer llamadas internacionales a coste suyo, reventar sistemas de correo de voz, monitorizar llamadas, interceptarlas... vaya que los phreakers siguen teniendo muchos juguetes con los que jugar y aprender.

Obstáculos en el camino

Hace unos años, las empresas de software privativo menospreciaban el software libre y no lo percibían como una amenaza. Sin embargo, cada vez hay más y mejor software libre, que cuenta hoy con millones de usuarios. Muchas de las empresas y gobiernos más importantes del mundo se han rendido a la evidencia y han empezado también a emplearlo e incluso potenciarlo.

Hay que reconocer, no obstante, que todavía no ha llegado a absolutamente todas las parcelas posibles, y que hay algunas necesidades que no están debidamente cubiertas. La falta de madurez de las aplicaciones libres en algunos campos muy especializados (diseño asistido por computadora, por ejemplo) puede impedir que algunos profesionales puedan migrar completamente. La percepción general es que es simplemente una cuestión de tiempo.

Las empresas de software privativo están viendo así como el mundo del software está cambiando, por lo que han empezado a reaccionar en diferentes frentes. Algunas están adaptándose en mayor o menor medida a los nuevos tiempos, mientras que otras han preferido el combate en diferentes frentes.

El primer obstáculo para la migración es, en realidad, un defecto del software privativo, donde cada programa usa un formato propio no documentado, con lo que una aplicación, como un procesador de textos, no entiende y tiene problemas para abrir un documento creado por otra (o incluso por otra versión de ella misma). A la hora de cambiar a otro programa, es probable encontrarse con que los datos y documentos que se han acumulado durante años están en un formato cerrado, que el nuevo programa no conoce. Con demasiada frecuencia, el viejo programa se negará incluso a exportar nuestros documentos a un formato común de intercambio.

Evidentemente, esta política es una estrategia deliberada de las casas de software, destinada a atrapar a los sufridos usuarios en su programa, impedirles que puedan migrar a otro programa de la competencia, pues el coste de

hacerlo subiría extraordinariamente. La situación es especialmente grave en caso de que dicha empresa cierre y el programa desaparezca.

En cambio, en el mundo del software libre se presta gran atención al uso de estándares, y todos los formatos están bien documentados, de modo que es imposible que nuestro trabajo quede atrapado en manos de una única empresa.

Otra dificultad similar es que algunas empresas usan aplicaciones hechas a medida que fueron escritas sin pensar en la portabilidad, de modo que solamente funcionan sobre Microsoft Windows, por lo que para migrar tendrían que reescribir el programa o usar un emulador de este sistema.

Otro arma que emplean son las técnicas FUD (*Fear, Uncertainty and Doubt*): consiste en sembrar miedo, incertidumbre y duda mediante campañas de desinformación plagadas de medias verdades y datos obsoletos que confundan a la gente con menores conocimientos técnicos y les hagan desconfiar de la posibilidad de migrar al software libre.

Así, nos dirán que el software libre es una cosa de *rojos* o de aficionados, que no tiene garantías y no se puede utilizar en entornos profesionales. O, por el contrario, pretenderán convencernos de que es muy difícil y que sólo sirve para expertos. Muchas veces estos ataques se camuflan como informes o artículos supuestamente imparciales, pero que están financiados por la empresa atacante. Algunos de estos FUD consiguen arraigar entre la gente y convertirse en auténticos mitos difíciles de desterrar, por más que se presenten pruebas que demuestren su falsedad.

Pero el mayor peligro que acecha al desarrollo del software libre es el de las patentes de software. Recordemos que, mientras el copyright controla la reproducción de una expresión concreta, las patentes otorgan durante un tiempo limitado la exclusividad para la explotación de una invención. Esto tenía cierto sentido cuando se inventó, pues se aplicaba a invenciones mecánicas. Pero aplicar el mismo concepto a ideas, como son los algoritmos matemáticos y, por tanto, los programas informáticos, lleva a situaciones absurdas. Por poner una analogía, el copyright controla la letra de la canción *Happy birthday to you*, pero no impide que la cantemos con otra letra. En cambio, una patente controlaría la idea misma de felicitar un cumpleaños, como quiera que lo hagamos.

Si bien hasta el momento no se permiten en Europa este tipo de patentes, algunos lobbies están presionando para que se adopte una legislación similar a la estadounidense. Esta adopción sería catastrófica no sólo para el software libre, sino también para la pequeña y mediana empresa informática europea. El proceso legislativo está ya en marcha, y numerosos profesionales y usuarios se han movilizado y están intentando hacer ver a los poderes políticos las consecuencias que tendría ceder a estas presiones.

El último peligro es interno, y es olvidar la importancia de la libertad y aceptar el uso de software privativo sobre sistemas libres, como hacen algunas distribuciones de GNU/Linux.

Conclusiones

Como hemos visto, la competencia salvaje de la industria del software privativo había llevado a una situación de monopolios, precios desorbitados, falta de innovación, abusos como documentos cautivos en formatos cerrados, etc.

Afortunadamente Stallman no fue el último hacker. En parte por la difusión de las computadoras personales, y en parte por su propio trabajo al crear el proyecto GNU y difundir su filosofía, han aparecido nuevas generaciones de hackers que han adoptado la ética del hacker y dedican su talento a escribir software y documentación libre.

En la actualidad, el software libre ha alcanzado tal grado de desarrollo que ya no es necesario convencer a nadie de que es posible. Ya no es una cuestión de fe, la existencia de productos de altísima calidad como el sistema GNU/Linux y programas como Mozilla, OpenOffice, Apache, Perl, Python, PHP, MySQL, PostgreSQL, etc., es indiscutible. La filosofía de apoyo mutuo del modelo colaborativo del software libre ha demostrado así que lo que es mejor éticamente, también lo es en la práctica, y que compartir la información y el conocimiento nos beneficia a todos: un magnífico ejemplo para la educación en valores.

Como se ha explicado, el modo de funcionamiento del modelo bazar es muy asambleario; por las listas de distribución de correo electrónico se discuten todas las ideas, se estudian sus ventajas y fallos, y se busca el consenso sobre cuál es la mejor: una suerte de democracia directa. Gente procedente de entornos técnicos, sin opiniones políticas, ha saboreado de este modo la experiencia de la libertad, y ahora quiere llevarla a otras facetas de su vida. Así, apoyan a los movimientos sociales, son firmes defensores de las libertades civiles, de la solidaridad, etc.

El software libre también está produciendo cambios en la economía. No deja de ser sorprendente que Bill Gates se haya convertido en una de las personas más ricas del mundo vendiendo algo inmaterial desarrollado por trabajadores asalariados anónimos. El software libre está trayendo una mayor equidad al sector y está permitiendo que los programadores recuperen el control de su trabajo. Quizás ya no sea posible hacerse rico repentinamente, pero sin duda el conjunto de la sociedad sale ganando. Para los países en vías de desarrollo el software libre supone también una oportunidad tecnológica que no necesita de grandes inversiones.

Si bien hace unos años un sistema GNU/Linux o *BSD podía resultar de difícil manejo para un usuario final, el software libre ha ampliado sus horizontes y proporciona ahora programas de excelente calidad que satisfacen las necesidades de la mayoría de los usuarios.

Para la mayoría de los usuarios ya es posible llevar a cabo todas sus tareas usando únicamente software libre, y solamente es cuestión de querer dar el salto y aprender algunas cosas nuevas. En cambio, a un usuario sin conocimientos informáticos le supondrá el mismo esfuerzo aprender a manejarse en un entorno libre que en uno privativo.

Para muchos usuarios, las nuevas libertades que les da este software les abre un nuevo campo en el que jugar y aprender, con lo que acaba convirtiéndose en una pasión. En cualquier caso, y aunque sólo sea como curiosidad, es un mundo que merece la pena explorar. *¡Happy hacking!*

Bibliografía y referencias para saber más

FREE SOFTWARE FOUNDATION: http://www.gnu.org.

GONZÁLEZ BARAHONA, Jesús (2002) *¿Qué es el software libre?* (conferencia). En: http://sinetgy.org/~jgb/presentaciones/soft-libre-palma-2002.ogg.

HIMANEN, Pekka (2002) *La ética del hacker y el espíritu de la era de la información*. Barcelona, Destino.

LESSIG, Lawrence (2004) *Free Culture*. Londres, Penguin Books. También disponible en castellano en: http://www.elastico.net/archives/001222.html

LEVY, Steven (2001) *Hackers: Heroes of the Computer Revolution*. Londres, Penguin Books.

MOINEAU, Laurent y PAPATHÉODOROU, Aris (2000) *Cooperación y producción inmaterial en el software libre. Elementos para una lectura política del fenómeno GNU/Linux*. También disponible en: http://www.sindominio.net/biblioweb/telematica/cooperacion.html.

SEOANE PASCUAL, Joaquín; GONZÁLEZ BARAHONA, Jesús y ROBLES, Gregorio (2003) *Introducción al software libre*. En http://curso-sobre.berlios.de/introsobre.

STALLMAN, Richard M. (2004) *Software libre para una sociedad libre,*. Madrid, Traficantes de sueños. También disponible en: http://www.nodo50.org/ts/editorial/librospdf/free_software.pdf

STEPHENSON, Neal (2003) *En el principio... fue la línea de comandos*. Madrid, Traficantes de sueños.

VARIOS AUTORES (1999) *Open Sources: Voices of the Open Source Revolution*. O'Reilly. También disponible en: http://www.oreilly.com/catalog/opensources/book/toc.html.

VARIOS AUTORES (2004) *Sobre software libre. Compilación de ensayos sobre software libre*. Dykinson. También disponible en http://gsyc.escet.urjc.es/~grex/sobre-libre.

2600

2600 es una publicación que nació en 1984 cuando se vio la necesidad de establecer algún tipo de comunicación entre aquellas personas que realmente valoran lo que significa comunicación. Se las podría llamar entusiastas de la tecnología, aunque también se las podría calificar de hackers, phreaks, criminales o anarquistas. El propósito de la revista no era establecer un juicio. *2600* existe para proporcionar información e ideas a individuos que viven para ambas cosas.

Cuando nace *2600* se acababan de producir un gran número de redadas, el FBI había confiscado numerosos equipos de unos 15 sitios de todo EEUU, y de esta manera se habían perdido los contactos, la gente temía las posibles consecuencias de seguir adelante, BBS legendarias habían sido desconectadas, al menos una temporada. Lo que *2600* pretendía era continuar esa comunicación, y resultó que las ganas, necesidad y aprobación del proyecto estaban ahí, los servicios secretos no habían destruido una comunidad, sino que la habían fortalecido y, a día de hoy, *2600* sigue publicándose.

Desde *2600* se han llevado a cabo campañas contra grandes compañías (en algunos casos sólo por diversión en otros con mayor intencionalidad), registrando dominios de grandes compañías como general motors (www.fuckgeneralmotors.com), microsoft (www.fuckmicrosoft.org); en contra del racismo (www.fuckracism.com) o contra los medios de comunicación (www.fuckthemassmedia.com). Esos dominios luego eran redirigidos a otras páginas web, en el caso de www.fuckracism.com el dominio apuntaba a una página donde se vigilaban las acciones del KKK; mientras que en el caso de www.fuckthemassmedia se redireccionaba a varias páginas donde se hablaba de la corrupción de los grandes medios de comunicación.

Podemos tomar como ejemplo la campaña contra Ford, pero para entender qué tiene que ver Ford en todo esto, pues al fin y al cabo en un principio ninguno de los dominios que se compraron estaban relacionados con la Ford. Todo empezó con el caso de www.fuckgeneralmotors.org, cuando al recibir amenazas de la compañía General Motors, que decía que estaban violando los derechos de su marca, desde *2600* se pasó a redirigir el dominio a las páginas web de sus competidores y, entre ellos, a la Ford.

La General Motors, pese a haberles amenazado, no llegó a poner una demanda, pero en cambio la Ford sí que puso una demanda judicial a *2600* aduciendo a que dicho redireccionamiento ensuciaba su imagen de marca.

Así que de una forma un tanto inesperada, lo que empezó siendo un juego más o menos provocador, resulta que iba a los tribunales bajo la acusación de que establecer un enlace entre el nombre de un dominio y una IP causaba un daño irreparable.

Desde *2600* se veía que, si Ford ganaba este juicio, podía sentarse un precedente que perjudicaría gravemente las libertades en Internet, pues establecer un simple enlace que no conllevaba ninguna ambigüedad entre un dominio y una IP se convertiría en un crimen. Después de varios meses, *2600* ganó el juicio a la Ford el 20 de diciembre de 2001.

PENÉLOPE: TEJIENDO Y DESTEJIENDO LA RED

Raquel Mezquita
(mezrakel@terra.es,
http://perso.wanadoo.es/rakelm)

Margarita Padilla
(mpadilla@sindominio.net,
http://www.sindominio.net/~mpadilla)

«Patriarcado: sistema de relaciones que institucionaliza y legitima la dominación de un género/sexo sobre otro.»
Ana de Miguel Álvarez[1]

«El aparente divorcio de las mujeres y la tecnología tiene sus raíces en una doble división del trabajo, por una parte la división sexual que hizo que las mujeres, a medida que la organización social avanzaba hacia el modelo actual, quedaran como especialistas de la reproducción y, por otra, la división entre trabajo manual e intelectual, que alejó a las pocas mujeres que tuvieron acceso a la cultura de un tipo de desarrollo como es el técnico, resultado de la articulación de los conocimientos prácticos con los científicos.»
Laura Tremosa[2]

SUPERAR LOS LÍMITES IMPUESTOS

El siglo XIX parece ser el momento en que comienza a desarrollarse un pensamiento propiamente feminista. Kate Millet, en su conocida obra *Sexual Politics* (publicada en 1971), sitúa entre los años 1830 y 1930 la primera fase de lo que ella denomina la «revolución sexual». ¿En qué sentido puede hablar Millet de una «revolución»?

Novecento y El profesor chiflado

Es preciso dejar claro que el campo de batalla de la revolución sexual abarca en mayor grado la conciencia humana que las instituciones sociales. El patriarcado se halla tan firmemente enraizado, que la estructura característica que ha creado en ambos sexos no constituye solamente un sistema político, sino también, y sobre todo, un hábito mental y una forma de vida. La primera fase [de la revolución sexual] atacó tanto los hábitos mentales como las estructuras políticas, pero tuvo mayor éxito con estas y, por ello, flaqueó ante las primeras acometidas de la reacción, sin llegar a alcanzar su objetivo revolucionario. Sin embargo, ya que su meta era lograr una modificación de las formas de vida mucho más radical que la conseguida por la mayoría de las revoluciones políticas, esta renovación, básicamente cultural, cobró el aspecto de una transformación lenta más parecida a la gradual pero profunda metamorfosis originada por la Revolución Industrial o el desarrollo de la burguesía, que a las rebeliones espasmódicas a que dio lugar la Revolución Francesa.[3]

1. De Miguel Álvarez, Ana (1994) «Deconstruyendo la ideología patriarcal», en VV AA: *Historia de la teoría feminista*. Dirección General de la Mujer de la Comunidad de Madrid, Madrid.
2. Tremosa, Laura (1986) *La mujer ante el desafío tecnológico*. Icaria Editorial, Barcelona.
3. Millet, Kate (1995) *Política sexual*, colección Feminismos, Cátedra. Madrid.

Durante esos cien años en los que, según Millet, tuvo lugar la primera fase de la revolución sexual, otra revolución, si es que así podemos llamarla, se estaba gestando. Nos referimos, claro está, a la revolución tecnológica.

En 1852 murió, a causa de un doloroso cáncer de útero, Ada Lovelace, la primera programadora de la historia, que dedicó gran parte de su trabajo a perfeccionar la máquina analítica de Babbage e inventó, entre otras cosas, estructuras ahora tan familiares en programación como son el bucle y la subrutina. Tenía 37 años y había parido tres hijos.

Cincuenta y tres años más tarde, Christabel Pankhurst se convirtió en la primera mujer que fue a la cárcel por reclamar públicamente en un mitin liberal, en Inglaterra, el derecho al voto femenino, justo cuando Georg Cantor tenía 60 años, Gottlob Frege 57 y Bertran Russell 33. No conocemos ningún testimonio sobre cuál fue el efecto que el encarcelamiento de Christabel Pankhurst, y las acciones de las sufragistas en general, produjeron en la generación de matemáticos y filósofos que sentaron las bases lógico-matemáticas de la revolución tecnológica.

Mientras las sufragistas inglesas incendiaban casas, rompían escaparates, asaltaban a miembros del Parlamento, colocaban bombas y saboteaban las comunicaciones, sufriendo una dura represión policial que llegó incluso a provocar algunas muertes, en Viena los filósofos Wittgenstein y Carnap trabajaban en el uso de las nociones de apareamiento de elementos de un conjunto y de autorreferencia para poner en evidencia los alcances de un pensamiento libre de contradicciones que permitiera una construcción lógica del mundo, libre de paradojas.

Estas nociones, poderosos instrumentos de análisis lógico, influyeron en todas las ciencias y técnicas, pero especialmente en las tecnologías de la computación, en las que era imprescindible que los algoritmos estuvieran libres de paradojas (del tipo «si cierto entonces falso y si falso entonces cierto») para evitar que su computación volviera continuamente a recalcularse sobre sí misma sin alcanzar un resultado efectivo.

Cuando, en 1928, las mujeres inglesas consiguieron el derecho al voto, el genial matemático Kurt Gödel tenía ya 22 años, estudiaba en la Universidad de Viena y trabajaba en la tesis doctoral que presentaría al año siguiente: «La completitud de los axiomas del cálculo funcional de primer orden». Estaba preocupado por averiguar los límites de lo lógicamente posible, e intentaba responder a preguntas del tipo: ¿es cierto que sentencias tales como 0 = 1 no pueden demostrarse por métodos válidos?

En 1931 presentó su famoso Teorema de Incompletitud que viene a decir que la verdad matemática no es algorítmica, situando los límites de la computación y mostrando la imposibilidad de diseñar algoritmos eficientes para muchos problemas aparentemente sencillos (los denominados NP-completos). Aunque los resultados de Gödel supusieron un trallazo a la racionalidad, la práctica de la computación sigue presentándose ante «la opinión pública» omitiendo sus limitaciones. La racionalidad, ese atributo tan masculino que concilia los discursos prescriptivos

LA CHICA DE LA PELÍCULA

La película *Gaslight* conocida en España como *Luz que agoniza* (1944) refleja, en un marco de intriga narrativa, el dominio psicológico de un marido sobre su esposa. El título hace referencia a las antiguas lámparas de gas que generaban un peculiar ambiente de luces y sombras, que en la cinta sirven al protagonista (Charles Boyer) para ir debilitando la firmeza síquica del personaje femenino (Ingrid Bergman), convenciéndola de que lo que ve no es real sino imaginado. La férrea sociedad victoriana es el marco de esta historia: un contexto en el que la autoridad del marido es incuestionable, lo que explica que la mujer vaya perdiendo paulatinamente la razón sin poner en duda las afirmaciones de su perverso compañero. De hecho, no podrá escapar sola de esta situación, sino que necesitará de la

con los normativos y que impulsa al hombre a hacer lo que debe, apenas sufrió ningún cuestionamiento.

Indiferente al avance del nazismo, Kurt se casó contra la voluntad de su familia, en 1938, con Adele Porkert, una bailarina de cabaret divorciada y seis años mayor que él, y se cuenta que no dejaron de amarse.

La costilla de Adán y Jules y Jim

Cuando estalló la Segunda Guerra Mundial, muchos años de luchas de mujeres por el derecho al voto femenino habían producido notables cambios sociales de diferente índole:

- Se cuestionaron los roles sexuales que identifican como valores masculinos, orientados hacia la vida pública y social, la agresividad, la inteligencia, la fuerza y la eficacia, y como valores femeninos, orientados hacia la vida privada y doméstica, la pasividad, la ignorancia, la docilidad y la virtud; y también se cuestionó el principio fisiológico sobre el que se legitiman estos roles: la fuerza física del macho.
- Se alteró el orden político, con la irrupción de las mujeres en los espacios públicos, la obtención del derecho al voto femenino y la presencia de grupos de mujeres organizadas.
- Se criticó el sistema educativo, erosionando los modelos de una educación para niñas basada en actividades domésticas y otra para niños basada en la ciencia y la tecnología.
- Se reformó el sistema jurídico y legislativo, reconociendo el derecho al divorcio y aboliendo los privilegios que permitían al marido el sometimiento de su esposa.
- Muchas mujeres accedieron al mundo laboral, con lo que consiguieron independencia económica y se pudieron negar a desempeñar sus roles tradicionales en el ámbito doméstico.
- Se liberó la sexualidad femenina, se ampliaron y divulgaron los conocimientos fisiológicos sobre el cuerpo femenino, y se atenuó la férrea inhibición patriarcal.

ayuda de un galante caballero enamorado (Josep Cotten).

Ejemplo cinematográfico de lo que Millet llama la contrarrevolución sexual son algunos films realizados durante los años cuarenta en EE UU y que abordaban, generalmente en tono de comedia paródica, el tema de la liberación de la mujer, destacando las interpretadas por Katherine Hephurn y Spencer Tracy. Tanto *La costilla de Adán* (1949) como *La mujer del año* (1942) nos muestran un estereotipo de mujer liberada: independiente, soltera o casada sin hijos, atractiva, segura de sí misma y a la que, sin embargo, le resulta imprescindible la compañía de un varón para sentirse completa. En estas películas encontramos reflejos de los rasgos con los que Freud describía la personalidad femenina: masoquismo, pasividad, narcisismo y el complejo que denominó «envidia del pene». Es una época de profunda influencia del psicoanálisis.

Sin embargo, aunque todas estas reformas empezaron a ofrecer un contexto político y jurídico más igualitario, los objetivos de la revolución sexual, una radical modificación de las formas de vida, quedaban inalcanzados.

En 1949, Simone de Beauvoir publicaba, con gran escándalo, *El segundo sexo*, en el que se analizaba el porqué de la existencia de la mujer como «lo otro», lo negativo, la alteridad, que sólo «es» en la medida en que el macho la cualifica.

Cinco años más tarde, Alan Turing se suicidó tomando una manzana envenenada con cianuro. El que fuera considerado como el padre de la inteligencia artificial, que cuenta nada menos que con un test, una tesis y una máquina que llevan su nombre, fue juzgado por homosexual y condenado a un tratamiento hormonal a base de estrógenos, a fin de que su homosexualidad fuera «curada» y de este modo no volviera a «delinquir». Los estrógenos deformarían su cuerpo, hasta entonces atlético, hasta el punto de que Alan decía no reconocerse a sí mismo al mirarse en un espejo. Su deterioro físico y la impotencia sexual le llevaron, tras dos años de «tratamiento», a una profunda depresión. El genial matemático que sentara, junto con Von Neumann, las bases teóricas de la computación murió en la soledad de su alcoba, dejando una gran pila de notas manuscritas cuyo valor, al cabo de tantos años, todavía no ha sido totalmente desentrañado.

De poco le sirvió haber contribuido a la democracia trabajando, junto con los servicios de inteligencia británica, en el desciframiento de los códigos secretos utilizados por el ejército alemán, ni que la mismísima reina Isabel le otorgara en 1946, en el más completo de los secretos, el máximo galardón del momento: la Orden del Imperio Británico. De nada le valió su extraordinaria contribución a la revolución informática, cuando el patriarcado le impuso un ajuste de cuentas por haber desertado de su rol de macho.

Claro que todo esto ocurría entre los años treinta y sesenta del siglo XX, periodo en el que Kate Millet sitúa una fase de «retroceso» o «contrarrevolución»

Muchos años más tarde, el director de cine Ridley Scott todavía supo valerse del inconsciente para recrear un claustro materno en los interiores deliberadamente viscosos de la nave en la que viajaba *Alien, el octavo pasajero* (1979). Pero, claro, para entonces las cosas habían cambiado. Ahora, la protagonista femenina ya no será, como analizó Simone de Beauvoir en *El segundo sexo*, lo Otro del sexo masculino. Todo lo contrario, la teniente Ripley, personaje interpretado por Sigourney Weaver, representa lo Mismo, que deberá enfrentarse a vida o muerte a lo Otro, el Alien, lo extraño, lo ajeno que hay que dominar porque en ello se juega la supervivencia del Mismo.

¿Por qué lo Mismo es ahora una mujer? Porque lo que está en liza, en esta lucha, es el propio futuro de la especie y, en definitiva, la vida colectiva. Scott presenta en esta película un Mismo que se siente amenazado (idea foucaultiana) por el agotamiento de los recursos naturales y la insosteni-

en la revolución sexual y que coincide con los años del nazismo, de la Segunda Guerra Mundial, de la caza de brujas anticomunista en EE UU, de la dictadura en España...

Querelle y La cortina rasgada

A partir de los sesenta se abre un periodo de auténtica revolución sexual, en la que las palabras y los cuerpos se encuentran, sin otra finalidad más que aquella gratuita de conocerse, y socavan profundamente las bases de la estructura patriarcal: la familia, el matrimonio y la maternidad tradicional. Muchas mujeres se atreven a vivir la maternidad despreciando la paternidad biológica, las lesbianas hacen públicas sus relaciones, se extienden las experiencias de sexualidad colectiva como alternativa a la familia tradicional, se practica el amor libre, la promiscuidad, la crítica del vínculo idealista entre «sexo» y «amor», las parejas son provisionales, «abiertas», se impone el derecho al aborto y a la anticoncepción, y las relaciones con los hijos dejan de ser autoritarias... El cuerpo mujer «templo sagrado» sometido a una sexualidad orientada a la reproducción y no al placer o, en el opuesto, mercado de fantasías masculinas extraconyugales, comienza a estallar en un cuerpo mujer liberado, que desea el goce más que cualquier otra cosa. Las mujeres difunden el conocimiento de su anatomía, su fisiología y su sexualidad y cuestionan la medicina como institución opresiva e instrumento del discurso patriarcal. Lo deseable ya no es mimetizarse con los hombres, sino investigar las posibilidades del ser mujer.

Muchas mujeres creen que la batalla no debe librarse en contra de la estructura económica sino en la esfera sexual, y viven dolorosamente la militancia política junto a «compañeros» que conservan herencias y hábitos patriarcales.

Se impone una autonomía en las ideas que permita la libre producción de pensamiento femenino al margen de la cultura masculina. Estallan feminismos de diferencia que quieren «nombrar el mundo en femenino». Proliferan los gru-

bilidad del actual modelo de desarrollo —amenaza puesta en evidencia por la crítica ecologista—, pero que también está amenazado por la crisis que las nuevas técnicas de reproducción plantean sobre los roles sexuales. En definitiva, ese Mismo amenazado no es más que la vida biológica como fundamento de la vida social.

La extinción de la vida biológica será planteada por el mismo director en *Blade Runner* (1982), donde los replicantes, hijos bastardos del militarismo y del capitalismo, tienen una enorme similitud con los cyborgs de Donna Haraway. Una película tan rica en simbolismos no elimina, sin embargo, los estereotipos. Las replicantes Zhora y Pris, adultas, fuertes y combativas, morirán como animales,

pos exclusivamente de mujeres: la política de sentido masculino pierde sentido. Como señala Luisa Muraro, se presenta una nueva apuesta: poner fin al dualismo por el cual la política de las mujeres sería una política al lado de la otra, llamada masculina o neutra, y poner en el centro de la política la política de las mujeres.

La primavera del 68 en París mostró que no es preciso consumar una revolución para sentir sus efectos: la irrupción del feminismo, del homosexualismo, de la ecología, del movimiento comunitario, antiautoritario, biopolítico, el resquebrajamiento del estalinismo internacional, el surgimiento de nuevas alternativas, de nuevas necesidades, de nuevas subjetividades, son los efectos, las ondas de ese inmenso wireless que fue Mayo del 68, el otoño caliente italiano, el Tlatelolco mexicano, los *sit-in* californianos, la Primavera de Praga...

Pero 1968 no fue sólo el año de una revolución. Ese mismo año se definió la estructura y especificaciones de ARPANET, la red de área extensa de la agencia federal estadounidense ARPA. Según la leyenda, el Departamento de Defensa de los EE UU, preocupado por su vulnerabilidad ante un hipotético ataque soviético, a través de la agencia ARPA asumió como un problema de carácter estratégico la interconexión entre las distintas redes de ordenadores, interesando en la solución de este problema a investigadores tanto industriales como académicos, y animándolos a discutir sus hallazgos y poner en común sus problemas. El proyecto auspiciado por ARPA comenzó a llamarse Internetwork (interredes), uno de los prototipos fue denominado Internet (con la inicial en mayúscula), y de ahí el nombre de la red de redes.

Por esas fechas, los grandes ordenadores ya disponían de suficiente memoria y velocidad de proceso como para ejecutar aplicaciones civiles en tiempo real, tales como el control de flujo de pasajeros en las grandes líneas aéreas. Hacía unos años que, en las redes de ordenadores, la conmutación de paquetes se estaba imponiendo sobre la de circuitos, faltaba sólo un año para que el sistema operativo UNIX empezara a ser desarrollado y cuatro para que Ray Tomlinson introdujera algo que ahora parece tan imprescindible como el correo electrónico.

mientras que Rachel, enamorada del que debería ser su ejecutor, presenta una evidente humanización física. Roy, el replicante más perfecto que su propio creador, se autoinmolará en favor de Deckard rodeado de muchos de los elementos de la simbología cristiana (herida en la sien, clavo en la mano, paloma).[1]

1. Algunas de estas ideas están tomadas de Moreno López, Esther: «Con-fusiones corporales. Personas, máquinas y animales», http://www.caminosdepakistan.com/pdf/4/cyborg.pdf.

Aunque, si de simbología cristiana queremos hablar, será *Matrix* (1999), la mesiánica película propiedad de Warner Bros y Roadshow Pictures, quien se lleva la palma. Y es que no entendemos cómo esta obra cinematográfica de los hermanos Andy y Larry Wachowsky ha despertado tanto entusiasmo, incluso entre nuestros amigos hackers. Un elegido que liberará a la humanidad, algo que desde fuera entrará en tu vida y te sacará del tedio, la dualidad entre el mundo real y el apa-

Los veteranos lenguajes de programación FORTRAN y COBOL habían visto el nacimiento del lenguaje BASIC, que, en 1968, con tan sólo cuatro años de edad, a causa de su sencillez y accesibilidad había producido una revolución en el tipo de usuarios de ordenadores, posibilitando el surgimiento de grupos de aficionados no expertos ni profesionales, que a su vez constituirían la base social sobre la que abrir el mercado de consumo de los ordenadores personales y masificar el uso comercial de la informática.

Messidor y La red

En 1982, IBM incorporó una versión económica del procesador Intel 8086, conocida como 8088, dentro de su primer ordenador personal. Un año más tarde, Richard M. Stallman empezaba a darle vueltas al proyecto GNU, con el que quería recuperar el espíritu hacker dominante entre los programadores que trabajaban en el MIT en los años sesenta.

Al mismo tiempo, Donna Haraway escribía *The Ironic Dream of a Common Language for Women in the Integrated Circuit: Science, Technology, and Socialist Feminism in the 1980s or A Socialist Feminist Manifesto for Cyborgs*, anticipando lo que posteriormente sería uno de sus ensayos más conocidos: el *Manifiesto para cyborgs*.

Por esas fechas, los ordenadores personales empiezan a llegar a los consumidores, y la posibilidad de creación de tecnología fuera del marco académico o empresarial permite el nacimiento de la imagen del hacker aficionado trasteando en el garaje de su casa. Las nuevas posibilidades de negocio abiertas por la masificación del mercado de la informática personal empiezan a valorar como bueno lo accesible (lenguajes sencillos, aplicaciones para el ocio, interfaces agradables, entornos gráficos, funcionalismo...) pero oculto (software propietario, pago por licencias, sistemas cerrados imposibles de trastear, secretismo...), valores sobre los que se establece la informática de ocio y consumo.

rente, el sacrificio propio como necesidad para la liberación de los demás o la posibilidad de alcanzar una vida auténtica y con sentido nos parecen metáforas muy poco sugerentes, por no decir que reintroducen ideas que harían sonreír al más viejo de los cyborgs.

En general, tanto el cine como la literatura han mantenido la tradición patriarcal que relaciona a la mujer con el cuerpo, lo orgánico y los flujos (sentir), y al hombre con la mente, lo maquínico y las prótesis (actuar). Ni siquiera las grandes obras del ciberpunk han sido innovadoras en su tratamiento de las relaciones entre los sexos, reproduciendo, en el fondo, las dualidades clásicas. Pero las carcajadas de placer por el acoplamiento entre máquinas y mujeres las harán estallar en mil pedazos. O, al menos, eso es lo que anuncia el ciberfeminismo.

La crisis de los movimientos sociales se sitúa en torno a los años noventa. Es entonces cuando el derrumbamiento de un mundo basado en el pacto social interclasista, en la macropolítica de bloques y en los grandes discursos de emancipación ya no puede ocultarse por más tiempo. Las transformaciones sociales que se producen a partir de ahí pueden llamarse, según distintos autores, el paso de la sociedad disciplinaria a la sociedad de control, o de la sociedad fábrica a la sociedad metrópoli, o de la sociedad industrial a la sociedad red, según pongamos el acento en las formas de dominación, las formas de lo social o las formas de producción, dando lugar al mundo tal y como ahora nos ha tocado vivirlo.

La desestructuración, desregulación o desesperanza señalan como lamento aquello que se perdió ante un mundo que se muestra, más altivo que nunca, como «mundo por demoler aún», «indiferente y extraño a nuestro paso», porque, sencillamente, no se deja transformar. El mundo «se ha quedado solo», no solamente por la globalización o por la homegeneización cultural, sino más que nada porque «se nos ha vuelto imposible pensar y vivir en relación a un mundo otro». «La soledad de hoy es la que no guarda ni el recuerdo ni el proyecto de algo común. Perdidos sin haber perdido, no dejamos nada atrás ni nos encaminamos hacia ninguna fecha». Pero «ni lamentamos lo que se acabó ni celebramos el punto al que hemos llegado». Sabemos que ahora ya «no se trata de asaltar el cielo», sino de «morder la realidad», por más que cueste pulverizar entre los dientes una realidad que tiene mucho de virtual, que se reproduce infinitamente con coste cero y cuyo soporte material son nuestras propias vidas[4].

4. Las expresiones entrecomilladas están tomadas de Garcès, Marina (2002) *En las prisiones de lo posible*. Edicions Bellaterra, Barcelona.

El ciberfeminismo no tiene cojones[5]

Rompiendo desde dentro

Si los años ochenta son los de la interactividad, el diálogo y la creación de un espacio privado con los ordenadores personales, los años noventa, con las redes, son los de la comunicación y la socialización electrónica. Paradójicamente, las posibilidades de comunicación se multiplican coincidiendo con las crisis de los movimientos sociales. Sin embargo, la ciberrevolución se abre camino como una nueva posibilidad de intervención social. No es de extrañar que algunas feministas, contagiadas de ese entusiasmo, imaginaran en la red la posibilidad de un mundo liberado de las violencias de género. En 1992, un grupo de tres artistas australianas Josephine Starrs, Francesca da Rimini y Julianne Pierce lanzaban el *Manifiesto ciberfeminista para el siglo XXI*, en el que podemos leer:

> *...we are the virus of the new world disorder*
> *rupturing the symbolic from whithin*
> *saboteurs of big daddy mainframe*
> *the clitoris is a direct line to the matrix...*[6]

Una de las integrantes del grupo, Julianne, explica en una entrevista:

> *Al mismo tiempo que comenzamos a usar el concepto de ciberfeminismo, también empezó a aparecer en otras partes del mundo. Fue como un meme espontáneo que emergió alrededor al mismo tiempo. Desde entonces el meme se ha extendido con rapidez y ciertamente es una idea que ha sido acogida por muchas mujeres que están interesadas en la teoría y práctica de la tecnología. [...] El concepto ha crecido y se ha expandido porque mucha gente diferente desarrolla las ideas de ciberfeminismo.*[7]

Telares electrónicos

Sadie Plant comenzaba, paralelamente, a usar el término ciberfeminismo abriendo una argumentación teórica en la que el ciberespacio se convierte en el territorio privilegiado donde experimentar la femineidad como motor de transformación: «El ciberfeminismo es una cooperación (para la liberación de la mujer) entre mujer, máquina y nuevas tecnologías».

Según Plant, los avances que, en la era moderna, asientan el desarrollo tecnológico actual, parten de hallazgos de mujeres, como Ada Lovelace y

5. Una de las 100 anti-tesis de lo que el ciberfeminismo no es, elaboradas durante el Primer Encuentro Ciberfeminista: http://www.icf.de/obn.
6. www.obn.org/reading_room/ manifestos/down/vns_cyberfeminist.rtf:
«...somos el virus del desorden del nuevo mundo
rompiendo lo simbólico desde dentro
saboteador@s de la computadora central del gran papaito
el clitoris es una linea directa a la matriz...»
7. http://www.aec.at/www-ars/matrix.html.

muchas otras sin nombre conocido, que comienzan a trabajar mayoritariamente como secretarias, recepcionistas, telefonistas, etc. Las mujeres despliegan entonces capacidad de organización multitarea (hasta entonces reducida al espacio doméstico) y habilidades comunicativas, herramientas indispensables en el ciberespacio actual.

> *Esta era una nueva masa de trabajo que se unía a una emergente capa de trabajos continuos, procesos uniformados, habilidades intercambiables: ordenar, clasificar, escribir a máquina, archivar, clasificar, procesar, contar, grabar, multicopiar, calcular, recuperar información, copiar, transferir.*[8]

Mientras, la identidad masculina se retroalimenta en una ficción de superioridad:

> *El hombre no es un hecho natural ni un producto de su propia creatividad, un cyborg que incluso entonces es un androide surgido directamente de las líneas de producción de las disciplinas de la modernidad. Lo que hace tan trágica a esta figura es la medida en que ha sido programada para creer en su propia autonomía. Autocontrol, autodisciplina, éstos son los mejores logros del poder moderno [...] La criatura llamada hombre que ahora vigilaba el escenario «aprende poco a poco en qué consiste ser una especie viviente en un mundo viviente, tener un cuerpo, condiciones de existencia». ¿Y qué aprendía? Simplemente a ser uno. Uno que cree que siempre ha sido uno. Un miembro que se acuerde de ser un hombre.*[9]

La historia de las mujeres ha venido ligada a la actividad de tejer y Plant convierte el sentido original en metáfora que describe la producción informática de muchas mujeres:

> *Cuando el tejer surgió en las pantallas pixeladas de los monitores del ordenador, la historia se enmarañó de nuevo. Las mujeres fueron de las primeras artistas, fotógrafas, artistas de vídeo y creadoras de películas en subrayar el potencial de las artes digitales.*[10]

Confía plenamente en el ciberespacio como territorio postgenérico en el plano simbólico y comunicacional, y en la nueva economía como fin de la pobreza y la precariedad femeninas y la desigualdad en educación y formación.

> *La identidad masculina tiene todo que perder con estas nuevas técnicas. Disminuyen los recuentos de esperma mientras los replicantes se*

8. Plant, Sadie (1998) *Ceros+Unos*, Destino, Barcelona.
9. Ibidem.
10. Ibidem.

empiezan a rebelar y la carne aprende a ser autodidacta. Lo cibernético es feminización. Cuando el espacio inteligente surge paralelo a la historia de la liberación de la mujer, no hay culpables.[11]

Las conexiones indirectas, tortuosas, a las que se han asociado siempre las mujeres, y el establecimiento de redes informales en las que ellas han destacado son ahora protocolos normales para todo el mundo.[12]

Las ideas de Plant se corresponden con el incremento de mujeres usuarias de las nuevas tecnologías de la información y el desarrollo virtual de *fem.art*. Pero las redes telemáticas necesitan un intenso desarrollo de hardware y software que permitan esos usos. Se queda en el aire la pregunta que otras ciberfeministas plantean: ¿por qué hay pocas mujeres programadoras y hackers? Nos parece, además, que aún debemos comprobar qué influencia liberadora suponen esos usos tecnológicos en las vidas cotidianas de esas *tejedoras*.

Las informáticas de la dominación

La identidad MUJER como sujeto político absoluto se desvanece, aunque se mantenga la crítica al patriarcado desde distintas preocupaciones, distintas posiciones políticas, distintos contextos socioeconómicos.

Ante la crisis de la identidad mujer, los feminismos son desafiados en términos que Donna Haraway describe de esta manera:

No existe nada en el hecho de ser «mujer» que una de manera natural a las mujeres. No existe incluso el estado de «ser» mujer, que en sí mismo es una categoría enormemente compleja construida dentro de contestados discursos científico-sexuales y de otras prácticas sociales. [...] Y ¿quién cuenta como nosotras en mi propia retórica?[13]

Coincidimos con Haraway en que cada «nosotras» discursivo dentro del feminismo habrá de referir a la práctica de «algunas mujeres» pero no a «todas las mujeres», aunque hábitos feministas y la nostalgia de lo universal nos mantenga en un juego en el que, al nombrar MUJER, queremos decir mujer. Haraway propone inventar formas diversas de coalición, afinidad, alianza, parentesco políticos.

De la ficción de futuro que propone la taberna de *La guerra de las galaxias* reemplazando al tradicional bar de la esquina, Haraway crea una figura que se revuelve contra el patriarcado: el cyborg. Un organismo polimorfo que surge de un mundo en el que van desapareciendo los límites entre lo humano y lo animal; entre organismos animales-humanos y máquinas y entre lo físico y lo no-físico.

11. Plant, Sadie: *Reflexión sobre Mujer y Realidad Virtual*, http://www.estudioson-line.net/texts/feminizaciones.htm.
12. Plant, Sadie (1998) *Ceros+Unos*, Destino, Barcelona.
13. Haraway, Donna (1985) «Manifiesto para cyborgs», en *Ciencia, cyborgs y mujeres. La reinvención de la naturaleza*, Cátedra, Madrid.

Un cyborg es un organismo cibernético, un híbrido de máquina y organismo, una criatura de realidad social y también de ficción. La realidad social son nuestras relaciones sociales vividas, nuestra construcción política más importante, un mundo cambiante de ficción. [...] El cyborg no sueña con una comunidad que siga el modelo de la familia orgánica aunque sin proyecto edípico. El cyborg no reconocería el jardín del Edén, no está hecho de barro y no puede soñar con volver a convertirse en polvo. Quizás sea por eso por lo que yo quisiera ver si el cyborg es capaz de subvertir el Apocalipsis de volver al polvo nuclear mediante la compulsión maníaca de nombrar al Enemigo. Los cyborgs no son reverentes, no recuerdan el cosmos, desconfían del holismo, pero necesitan conectar: parecen tener un sentido natural de la asociación en frentes para la acción política, aunque sin partidos de vanguardia. Su problema principal, por supuesto, es que son los hijos ilegítimos del militarismo y del capitalismo patriarcal, por no mencionar el socialismo de estado. Pero los bastardos son a menudo infieles a sus orígenes. Sus padres, después de todo, no son esenciales. [...] Las feministas de cyborg tienen que decir que nosotras no queremos más matriz natural de unidad y que ninguna construcción es total.[14]

La apuesta de Haraway nos sugiere la construcción de un imaginario poblado de subjetividades cambiantes que se deshacen tanto de las relaciones de dominio como de las viejas ideologías emancipatorias. Pero, ¿cómo deshacerse de la herencia del cuerpo mujer sexuado? Las nuevas tecnologías, como ella anuncia, han generado en los últimos años nuevas relaciones sociales, pero aún nos queda analizar qué tipo de relaciones, qué lugar ocupan mente y cuerpo en ellas, y si, realmente, anuncian un mundo postgenérico.

Por otro lado, aunque Haraway habla de alianzas o parentescos políticos, aún se nos escapa cuáles serían las formas colectivas de reinventarse en cyborgs. Haraway describe las «informáticas de la dominación» enfrentando el viejo marco histórico e ideológico al nuevo, y lo expresa en dicotonomías de las que resaltamos algunas en la tabla adjunta.

Representación	*Simulación*
Organismo	Componente biótico
Fisiología	Ingeniería de comunicaciones
Familia/mercado/fábrica	Mujeres en circuito integrado
Público/privado	Nacionalidad cyborg
Cooperación	Aumento de las comunicaciones
Sexo	Ingeniería genética
Mente	Inteligencia artificial
Patriarcado capitalista blanco	Informáticas de la dominación

14. Ibidem.

Resulta un mapa de intervención política difícil de aprehender: cómo amenazar las formas de dominio extendidas a través de las redes, cómo criticar e interrumpir el sentido del propio flujo informativo/comunicativo.

Política de la parodia

«Soy un ser mortal, de categoría femenina, humano, sexuado, con capacidad para usar el lenguaje: llámame simplemente: mujer.»
Rosi Braidotti, *Un ciberfeminismo diferente*[15]

Avanzando los noventa, hay ciberfeministas que resaltan el fracaso del paraíso de la liberación tecnológica. Rosi Braidotti no comparte la esperanza idealista de nuevas sociedades en red pobladas de seres polimorfos, carentes de identidad sexual, pero admite los cambios que se están produciendo, que anuncian nuevos periodos culturales, y no renuncia a explorar caminos de transformación.

«El cyborg es éter, quintaesencia», afirma Haraway. Braidotti habla de «cuerpos posthumanos»: superficies de códigos sociales enmarcados en coordenadas de espacio y tiempo, *cuerpos múltiples*. Hay cuerpos posthumanos que temen la vejez y la muerte. Se reconstruyen plásticamente y se imponen como símbolos del estereotipo dominante: raza blanca, heterosexualidad, poder económico, belleza prototípica, claves del éxito de un mundo capitalizado, rebelión contra la naturaleza al servicio del contrato sociosimbólico patriarcal.

> *El presunto triunfo de la alta tecnología no se ve correspondido con un salto de la imaginación humana encaminado a crear nuevas imágenes y representaciones. [...] En los momentos de gran desarrollo tecnológico, Occidente siempre reitera sus hábitos más ancestrales, especialmente la tendencia a crear diferencias y organizarlas jerárquicamente.*[16]

Las feministas pueden construir cuerpos posthumanos diferentes, a través del arte y la política, que contribuyan a un imaginario que se aleje de esa imposición y permita la recuperación del cuerpo diverso y su anexión a la máquina como una prolongación semiótica del mismo. La tecnología puede servir a las mujeres «para liberar nuestra imaginación colectiva del falo y sus valores accesorios, como son el dinero, la exclusión, la dominación, el nacionalismo, la femineidad icónica y la violencia sistematizada».[17] La liberación de ese imaginario impuesto tiene un camino a través de lo que denomina «política de la parodia» o del «como si», y de la ironía como una posible practica de esa política:

> *La filosofía feminista del como si no es una forma de rechazo sino más bien la afirmación de un sujeto que carece de esencia, es decir, cuyo*

15. Braidotti, Rosi: *Un ciberfeminismo diferente*, http://www.estudioson-line.net/texts/diferente.html.
16. Ibidem.
17. Ibidem.

ENVIAR UNA HISTORIA

ENCUENTROS

En septiembre de 1997 se celebró en Alemania el Primer Encuentro Internacional Ciberfeminista. En julio de ese mismo año se celebraron los Segundos Encuentros Zapatistas. La actividad de encuentro y convivencia que tuvo lugar en Madrid se desarrolló en el centro social okupado El Laboratorio. Entre la multitud de charlas y discusiones colectivas organizadas, una buena parte pertenecía al espacio de género, iniciativa de la casa de mujeres okupada La Eskalera Karacola. En estas discusiones, entre otros temas, se abordaba el problema de los límites de lo natural, usando como referencia textos que aportaban miradas polarizadas frente al uso de las nuevas tecnologías: ciberfeminismos

fundamento ya no es la idea de la naturaleza humana o femenina, pero un sujeto que es capaz, a la vez, de acciones éticas o morales. Como nos advierte lúcidamente Judith Butler, la fuerza de lo paródico radica, precisamente, en convertir la práctica de la repetición en una postura que nos dote de poder político. [...] La ironía es la ridiculización aplicada en dosis sistemáticas; es una provocación continua; es desinflar una retórica excesivamente vehemente. Una posible respuesta al talante general de nostalgia que domina la cultura popular no puede resumirse en unas palabras, ha de practicarse.[18]

Parece que la intención de Braidotti es arrancarnos de esa nostalgia a la que hace referencia, y cuyo efecto paraliza la intervención política, aunque hay que seguir investigando en los restos que permanecen como signos en nuestros cuerpos. Nos invita a un juego de figuraciones donde piensas en tu yo individual de peculiares características biográficas y, a la vez, en la potencialidad de un yo colectivo que se aleja de lo biográfico y vuelve a lo social; su ironía te arranca de la solemnidad teórica.

Lo cierto es que necesitamos despedirnos de ese segundo sexo, ese eterno femenino que se nos ha pegado a la piel como una materia tóxica. [...] Como colectivo, necesitamos tomarnos el tiempo necesario para el luto por el antiguo contrato sociosimbólico y así subrayar la necesidad de un cambio de intensidad, un cambio de ritmo.[19]

18. Ibidem.
19. Ibidem.

versus ecofeminismos. Apenas seis años pero entonces, entre nosotras, no había muchas mujeres que tuvieran un uso cotidiano e intenso del ordenador. Pocas conocíamos Internet, menos aún entenderlo. Un ejemplo: se decidió que de cada discusión se elaborara una pequeña memoria que se enviara diariamente a la lista de correo de los segundos encuentros. Recuerdo esto como un auténtico problema: quién tiene ordenador, desde dónde se envía, qué es una lista de correo... De hecho, muchas de esas memorias se enviaron ya finalizados los encuentros. Esas mismas tareas, ahora, podrían llevarnos tan sólo unos minutos.

El cyborg quedaba lejos. Los encuentros desvelaron algo que ahora parece obvio: la dificultad de aunar un discurso que abarcara las realidades de las mujeres que participábamos de los encuentros, provenientes de contextos socioeconómicos y culturales bien distintos. Sin embargo, tu cuerpo

Las afueras de la red

Braidotti cita como ejemplo de actividad paródica la del grupo Riot girls (chicas disturbio). Éste y otros grupos de mujeres pueblan el ciberespacio: *web grrls, guerrilla grrls, bad grrls*...[20] www.girlgeeks.org y otras, lo que Faith Wilding ha denominado *cibergrrl-ismo*.[21]

Su gesto enérgico se traduce en un *simple* «si quieres hacer algo, hazlo». El aumento de dominios por parte de estos grupos y los contenidos de sus webs aumentan la visibilidad de mujeres en el ciberespacio. A la vez, evidencia su diversidad, porque se puede hallar desde carteles criticando el gobierno estadounidense hasta consultorios sentimentales. En opinión de Wilding, esta presencia adolece de una falta de teoría y práctica de mayor intención política, por ejemplo, cuando «se reapropian y reproducen imágenes sexistas y estereotipadas de las mujeres, propias de los medios tradicionales».[22]

Según Wilding, no hay que olvidar que el ciberespacio reproduce la estructura sexista en la que ha surgido.

> *¿Por qué el porcentaje de mujeres que programan, diseñan software, analizan sistemas o son hackers es tímido mientras que la mayoría son grabadoras de datos, trabajadoras en las fábricas de chips y teleoperadoras que mantienen los bancos de información y de datos globales? [...] Contrariamente a los sueños de muchos utópicos de la red, Internet no borra las jerarquías al permitir libres intercambios de información mas allá de las fronteras. Asimismo, el ciberespacio no es una utopía del no-género, está todavía inscrito socialmente en los límites de los cuerpos, sexo, edad, economía, clase social y raza.*[23]

20. www.gurl.com, www.techiegirl.com, www.guerrillagirls.com, www.badgirls.co.uk.
21. Wilding, Faith: *Where is Feminism in Cyberfeminism?*, http://www.obn.org/cfundef/faith_def.html.
22. Ibidem.
23. Ibidem.

mujer sexuado mantenía con los otros una relación de íntima solidaridad. Desayunar con un montón de mujeres con las que luego confabularías para cambiar el mundo, y, después, irte de fiesta, fue una auténtica delicia.

Al cabo de seis años hemos vuelto a hablar con algunas amigas sobre su acercamiento a las tecnologías.

CAROLINA PARA RADIO PWD (JUNIO, 2003)

Cuando iniciamos el camino en el hacklab al principio y durante muchos meses yo era la única chica que estaba presente. Me interesan las tecnologías pero, sobre todo, el desarrollo, el compartir y la transmisión del conocimiento, y veo en las tecnologías esa facilidad, al margen del ámbito técnico cien

Frente a las críticas que algunas ciberfeministas plantean sobre el carácter excesivamente antitecnológico y esencialista del feminismo de los setenta, Wilding insiste en la importancia de no deshacerse del pasado activista: intentar comprender los errores y trascenderlos hacia nuevas fórmulas:

> *El ciberfeminismo puede imaginar maneras de ampliar las prácticas filosóficas e históricas del feminismo hacia proyectos y redes feministas tanto fuera como dentro del ciberespacio, y hacia las vidas materiales y las experiencias de mujeres, en un circuito integrado que tenga en cuenta la edad, raza, clase y diferencias económicas. [...] El problema del ciberfeminismo reside en cómo incorporar las lecciones de la historia a un activismo político feminista que se adecue a los asuntos de las mujeres en la cultura tecnológica.*[24]

La intención de Wilding de devolver el análisis del ciberespacio a su materialidad es imprescindible. Lo que parece despotenciar su discurso es la no renuncia a la herencia del paradigma feminista. Quizá la complejidad del nuevo marco socioeconómico requiera que ese *intervenir sobre los asuntos de las mujeres*, si tal afirmación sigue teniendo sentido, se plantee desde nuevos paradigmas.

En septiembre de 1997, por iniciativa del grupo OBN (Old Boys Network), surgido de la fusión de VNS Matrix e INNEM, otro grupo de artistas alemanas, se desarrolla en Alemania el Primer Encuentro Internacional Ciberfeminista, práctica feminista de organización a través de la red, mezcla de discusiones presenciales y *on-line*. El encuentro puso de manifiesto las diferencias respecto a la necesidad o no de definir conceptualmente el ciberfeminismo y la diversidad de estrategias políticas. Resultado de ese encuentro y de esa manera irónica de la que habla

24. Ibidem.

por cien. No he vivido la ausencia de mujeres como un problema. La formación del hacklab salió en conjunto, con la particularidad de que el resto eran hombres, pero éste no es un hecho que me haya condicionado. Todo este tiempo he estado a gusto. Lo cual no resta que me haya preguntado muchas veces cómo en un ámbito ya bastante generalizado como las tecnologías, conociendo gente que trabaja con ellas en otros espacios, en ámbitos más sociales no haya muchas mujeres participativas.

Algo de lo que me voy dando cuenta con el tiempo es la diferente relación que se tiene con la tecnología: en los chicos, según he observado en el hacklab, la obsesión por un solo tema se da con más frecuencia y a las chicas nos interesa, nos gusta, pero no le dedicamos la mayor parte de la vida: nuestra vida es más repartida a nivel afectivo y queremos realizar otras actividades. No tenemos prisa por adquirir el conocimiento de una manera inmediata.

Braidotti, se redactó un documento que recoge las *100 antitesis* de lo que el ciberfeminismo no es: no es una ideología, no es dogmático, no es natural, no es esencialista, no es inteligencia artificial, no es...

La red es femenino

Hemos abordado las diferentes propuestas con que los ciberfeminismos quieren actualizar el feminismo en la red. Nos interesamos, ahora, por saber qué es lo que encuentran las mujeres cuando conectan el módem.

Los elegidos

La red está llena de hackers, y no es de extrañar que así sea. Ellos han producido la nueva base tecnológica de la sociedad conectada. Desde el ordenador personal hasta los protocolos TCP/IP, todo el hardware y el software sobre el que se sustenta la posibilidad de una nueva modalidad de organización social son una producción genuinamente hacker. Los hackers viven en la red, la producen, la entienden y la disfrutan. ¿Quiénes son ellos?

De todas las caracterizaciones que se han hecho de la figura hacker, quizás la más sistemática sea la de Pekka Himanen expuesta en el libro *La ética del hacker y el espíritu de la era de la información*, con prólogo de Linus Torvalds y epílogo de Manuel Castells.

Himanen describe al hacker como el portador de una ética basada en un conjunto de valores en relación con el trabajo, el dinero y el bien común que se contrapone a los valores de la ética protestante, tal y como la expuso Max Weber a principios del siglo XX en *La ética protestante y el espíritu del capitalismo*. Según Himanen, la ética protestante es, en la actualidad, dominante en el conjunto de la sociedad e incluso en la sociedad red. La ética hacker supondría un desplazamiento de la ética protestante, sustituyendo la obligación del trabajo monótono y disciplinado por la actividad apasionada y creativa elegida libremente. Este desplaza-

A mí me gusta entender la actividad hacker como de apasionamiento por algo. El apasionamiento está desligado del género, el interés por algo, en este caso por la tecnología, puede ser igual pero expresado de forma distinta: puedes dedicar horas a un tema sin reflejarlo, sin que eso suponga pasar veinticuatro horas sin dormir. Se es hacker en cuanto apasionado por un tema, no tanto en la cantidad de horas o la productividad que tengas sobre ese tema, sino por lo que te reporte; no va directamente unido a la productividad estándar de hacer cosas y mostrarlas, sino a lo que ello te aporta personalmente.

La concentración y dedicación son necesarias a la hora de superar o analizar determinados problemas. El clásico de ensayo/error implica una cantidad de horas superior y una forma de análisis que se parece a la tarea de la hormiga que va avanzando y, cuando choca, corrige y va hacia otro

miento afectaría a todos y cada uno de los valores de la ética protestante: la búsqueda del beneficio se convertiría en compartimiento de conocimientos, la acumulación de capital en obtención de reconocimiento social, el tiempo disciplinado en tiempo autoorganizado, etc. Y lo más importante: la ética hacker podría generalizarse al conjunto de la sociedad.

Dice Himanen:

> *Considerado en un contexto histórico más amplio, no es sorprendente este continuado predominio de la ética protestante pues, si bien nuestra sociedad red difiere en gran medida de su antecesora, la sociedad industrial, su nueva economía no comporta una ruptura completa con el capitalismo descrito por Weber; se trata sólo de un nuevo tipo de capitalismo. [...] La sociedad red no pone en tela de juicio la ética protestante. Campando a sus anchas, este mismo espíritu centrado en el trabajo sigue dominando sin problemas.*
>
> *En este contexto más amplio, la naturaleza radical del hackerismo consiste en su propuesta de un espíritu alternativo para la sociedad red, un espíritu que finalmente cuestiona la ética protestante. Y sólo en este sentido cabe afirmar que todos los hackers son realmente crackers: porque intentan romper el cerrojo de la jaula de acero.*[25]

Dejemos de momento a un lado las críticas que hacemos a las propuestas de estos autores, basadas en un antiautoritarismo individualista, según el cual «mi vida es mi vida» y, por tanto, puedo y debo organizarla libre y responsablemente (como proyecto). Dejemos el hilo de la crítica y preguntémonos cómo los ciberfeminismos, desde su punto de vista, considerarían los valores de la ética hacker.

25. Pekka Himanen (2002) *La ética del hacker y el espíritu de la era de la información*. Destino, Barcelona.

lado, y va reteniendo, es una manera de adquirir conocimiento. Pero hay otras formas de acercarse a los mismos conocimientos que, en un primer momento, requieren mayor necesidad de abstracción o un esfuerzo que implica pensar qué queremos hacer sin tener delante una máquina, enfrentarse a qué haces, por qué lo quieres hacer, y que sea ese pensamiento original lo que te conduzca a hacer las cosas que necesites, lo cual, al final, puede significar ahorro de trabajo.

MAR PARA RADIO PWD (JUNIO, 2003)
Parece que todas las máquinas son lo mismo, pero no. Hay herramientas con las que trabajas con fluidez, las conoces, pero al tener que saltar de tecnología, por ejemplo pasar un material digital a soporte vídeo, señal analógica, descubres que son mundos aparte, y te encuentras con que no

Masculinos, pero menos

La respuesta no es sencilla para nosotras, porque ni somos propiamente ciberfeministas ni nuestros amigos son puramente los hackers caracterizados por Himanen. Lo más que podemos hacer es aventurar algunas hipótesis basadas en nuestra limitada y concreta experiencia.

Nuestra relación con la tecnología se inicia en el área telemática de un centro social okupado en Madrid, el Laboratorio, y gira en torno a sinDominio, el software libre, los hackmeetings, hacklabs, y otras prácticas que son el objeto de este libro.

Todas ellas están vinculadas a propuestas que vienen de «Italia» y que derivan de una «línea política» que denominamos «autonomía».

Muy brevemente, «autonomía» significa que «nosotros», colectivamente y al margen del sistema de dominación impuesto, poseemos la única capacidad productiva: la cooperación. Si el deseo de comunismo es fuerte podemos «separarnos» del sistema llevándonos la capacidad productiva del mismo (la cooperación) y construir espacios autónomos donde las relaciones sociales no sean de dominación. Los espacios autónomos forman redes de contrapoder que reproducen la vida social independientemente de los sistemas de dominación, y su prioridad no es enfrentarse «al enemigo» y vencer, sino proliferar hasta que los sistemas de dominación «se queden solos». Naturalmente, «autonomía» no es un dulce viaje a la utopía, es un proceso duro de luchas contra todas aquellas fuerzas que reducen, bloquean y menguan el deseo de comunismo y, en la medida en que somos «nosotros» quienes reproducimos esas fuerzas, también de lucha contra nosotros mismos.

¿Qué relación hay entre «autonomía» y tecnologías?

En primer lugar, reapropiarse de las tecnologías es una tarea prioritaria, pues, no lo olvidemos, éstas son producto de la cooperación social, en tanto que se han producido no gracias al mando capitalista sino gracias a la comunicación y al compartimiento de conocimientos. Si nos resultan ajenas las tecnologías es

hay «la tecnología» o «una tecnología», sino que lo que tenemos es un mosaico de tecnologías que tienen límites, y dar el salto de unas a otras requiere una reunión de saberes.

Yo me acerqué por curiosidad y por necesidad laboral. Los ordenadores son herramientas que te permiten ahorrar tiempo y espacio. Por ejemplo, en el mundo de la imagen, donde necesitabas un complejo mundo fotográfico, ampliadoras, serigrafía... gran cantidad de técnicas que de repente te las encuentras reunidas en un ordenador. Ésa es una realidad muy potente desde los noventa, tener un ordenador con posibilidades para el diseño gráfico te daba la posibilidad de asumir tareas que de otra manera habrías necesitado un montón de profesionales, laboratorios. Y, de repente, dabas un salto cualitativo respecto a tus capacidades porque podías desarrollar cosas que antes no podías hacer sola.

porque nos han sido expropiadas; hay que reapropiarse de lo que nos pertenece y nos ha sido arrebatado. En segundo lugar, producir relaciones horizontales de cooperación es imprescindible, pues el capitalismo destruye el vínculo social, que debe ser reconstruido mediante la autoorganización. En tercer lugar, lo anterior debe hacerse visible y público, pues la «autonomía» se extiende por contagio, por conexión, por seducción, contamina lo social con su alegría y su belleza.

Un ejemplo claro de «autonomía» serían los hackmeetings: compartimiento de conocimientos en un espacio público autoorganizado que debe «resonar» en lo social.

Es evidente que esta propuesta política pone el acento en los procesos «constituyentes» y, por tanto, no está interesada en otros procesos más, digamos, disipativos, propios de lo que podríamos llamar el *underground* de la red: juegos, chateo, piratería, intrusiones, virus, *cracking*, rumores, dinero ajeno y, en general, transgresiones desde la clandestinidad con una fuerte dosis de ambigüedad en su significado.

Por eso, no es de extrañar que «autonomía» mire con ojos de complicidad al movimiento por el software libre, pues éste es una colosal demostración de la capacidad productiva de la cooperación (bastante) autónoma. Y, por eso, nuestros recorridos por la red frecuentan las prácticas mencionadas al principio, en detrimento de otras más propiamente ciberfeministas.

En general, los ciberfeminismos toman como punto de partida las posibilidades de una disolución del género (también de la raza y de otras categorías de dominación) en la red, en tanto que en ésta no hay ni cuerpos, ni rostros, ni voces...

Según Sadie Plant, la ausencia de cuerpo, su disolución en la red, disuelve la identidad en una matriz reminiscente del útero materno en la que el cuerpo queda atrás, fluctuando en lo inmaterial y volviendo obsoleto el problema de la identidad, que se hace mutante e incierta. Helena Velena (http://www.helenavelena.com), audaz en la experimentación del cibersexo, ha insistido en las capa-

Para mí no ha sido una experiencia traumática el acercarme a la informática, porque siempre he tenido la suerte de contar con la ayuda de gente. Los avances suponen tener que ir saltando de unos saberes a otros, necesitas tener una actitud muy ágil y estar siempre estudiando, leyendo... y quizá eso es lo que veo menos positivo: el ritmo tan acelerado de aprendizaje que se exige. Para gestionar bien nuestra posición dentro de esa tecnología difusa, cada vez se hace más necesario la reunión de saberes y eso implica trabajo colectivo y mi experiencia está basada en eso.

Todo nuestro mundo pertenece al aparato de la lógica, nuestra cultural occidental está basada en el aparato de la lógica y ese aparato es masculino porque todo en nuestra cultura occidental es masculino. Yo defiendo que los sujetos somos seres múltiples, capaces de evolucionar. No haría una crítica de la tecnología *per se*, por manejarse en esos parámetros de la lógica, sino que tomaría de

cidades liberadoras del ciberespacio, que tiene la facultad de desanclar los cuerpos de los géneros y liberar lo reprimido, traspasando los confines de una sexualidad binaria. Para Donna Haraway la experiencia cyborg de simbiosis con el software y el hardware de la máquina crea un contexto en el que la sexualidad, el género e incluso la propia humanidad se han vuelto anacrónicos.

Pero toda experimentación en este sentido requiere renuncia a la identidad, travestismo, anonimato, algo que choca de lleno con los valores individualistas de la ética hacker y, especialmente, con el valor que esta ética sitúa como base del vínculo social: el reconocimiento.

Como ya hemos dicho anteriormente, nuestros amigos hackers no son ni mucho menos un calca del perfil que traza Himanen pero, ciertamente, tampoco están interesados en cuestionar esa ética, más proclive a reforzar yoes que a disolverlos y que, acríticamente, se toma como modelo.

Las relaciones entre los cuerpos físicos y los cuerpos virtuales podrían ser un nodo crucial para la emergencia de herejías de género pero, por decirlo de alguna manera, en los espacios que frecuentamos no hay interés por ello. Y a pesar de esto, en una serie de charlas mantenidas con algunas amigas con el propósito de elaborar estos textos (disponibles casi totalmente en la web de radio pwd: http://www.sindominio.net/radiopwd) todas han reconocido a los hacklabs, los «sindominio» y otros espacios hackers materiales o virtuales como «menos» masculinos que «el mundo en general» y, por supuesto, que los espacios «militantes».

Esta disminución de la masculinidad podría ser la resultante de varias fuerzas: la crítica feminista, que ha hecho mella en los espacios donde se ha desplegado; la propia estructura de la red, que es más performativa si las diferencias de género se atenúan...

Lo que nos preguntamos ahora es si ese «masculino, pero menos» es característico de los espacios que persiguen «autonomía» o bien es generalizable al conjunto de la sociedad (red).

ella lo mejor y trataría de subvertirla, igual que subvertimos los lenguajes y la expresión, igual que subvertimos nuestras formas estereotipadas de relacionarnos y creamos nuevos modos. Quizás el reto sea ése: crear nuevos modos o modelos de aprovechar la tecnología.

Las mujeres somos más pobres y digo «somos» por utilizar un término que nos reúna a todas, si eso es posible; hay más pobreza femenina, hay más dificultad de acceso a la educación. Eso si te pones en una perspectiva global, no en mi pellejo, sino en el de mujeres con dificultades económicas y de acceso a la educación. Yo sé que no soy un paradigma, porque he tenido acceso a la educación y dentro de la dificultad económica, digamos, que me manejo.

Yo sé que todas estas cosas pertenecen a áreas de discurso en las que se ha profundizado mucho, a mí me cuesta hacer afirmaciones categóricas porque se podría decir eso es feminismo de la dife-

Se espera de ellos que sean... femeninos

Desde que Max Weber escribiera su obra, hace unos cien años, grandes ciclos de lucha han socavado, con su crítica radical y directa del trabajo, los fundamentos del sistema capitalista. Pero, tras la Segunda Guerra Mundial, se establece un pacto social que supone una tregua en la lucha de clases: la clase obrera ofrece estabilidad social y altos niveles de productividad a cambio de democracias parlamentarias, garantías sociales y altos niveles de consumo. Este pacto social, pacto entre clases, dio lugar al «Estado de bienestar»: un conjunto de derechos sociales ligados al trabajo asalariado (jornada de ocho horas, vacaciones pagadas, jubilación, viudedad, orfandad, prestaciones por enfermedad o invalidez, etc.), pero, eso sí, a cambio de intensos ritmos de trabajo impuestos por la patronal mediante la aplicación de una «organización científica del trabajo», basada en el estudio de «métodos y tiempos» (fordismo y taylorismo), y que dio lugar a la cadena de montaje como forma de organización de la producción y como metáfora de la vida social: alta división del trabajo, especialización, masificación, maquinización, jerarquía, disciplina, monotonía, rigidez, separación de espacios y tiempos, etc.

A finales de los años sesenta, coincidiendo con el fin de lo que Millet denomina la contrarrevolución sexual, desde distintas culturas y con diversos lenguajes, un intenso ciclo de luchas puso la crítica del trabajo (podríamos decir: la crítica de esa modalidad de trabajo asalariado propia de la cadena de montaje) en el centro de la vida de mucha gente, que ya no estaba dispuesta a someterse a los ritmos repetitivos y alienantes de la producción de mercancías.

Multitud de consignas desafiantes, antiautoritarias, contra la democracia formal, contra la política de izquierdas, contra el trabajo, por la libertad sexual... fueron utilizadas como passwords que daban acceso a la posibilidad de una subversión total en todos los ámbitos de la vida. Estas consignas quedan muy lejos y, a la vez, muy cerca, porque, aunque fueron derrotadas, no han sido aniquiladas: la (sociedad) red nos las devuelve ahora en forma de prestaciones.

rencia o de la igualdad o... Intentando situarme al margen de esas áreas de discurso, creo que lo que sí existe es un modelo imperante de relaciones que pertenecen al mundo de lo patriarcal; y la tecnología, hoy por hoy, se usa como casi todo dentro de esos modelos de relación. Ahora bien, ¿qué es lo que hay que cambiar?, ¿la tecnología? Lo que hay que cambiar son los modelos de relación que nos afectan tanto a mujeres como a hombres. Otra cosa es si hablamos de problemas más concretos: índice de reparto de la riqueza, acceso a la educación, acceso al trabajo, entonces sí hablaría de situaciones a subsanar sólo con respecto a las mujeres.

No etiquetaría la tecnología de patriarcal *per se*. Toda nuestra cultura está basada en la competitividad, en el individualismo, en el dominio del otro, y todo eso configura la cultura patriarcal; pero eso es un modelo de relaciones que está en la base de todo lo demás. Cuando se leía el texto en el que

En su obra *El nuevo espíritu del capitalismo* Luc Boltanski y Ève Chiapello analizan la actual crisis de la crítica del capitalismo y, como parte del análisis, estudian los componentes del nuevo espíritu del capitalismo a partir de una lectura de los textos utilizados por la patronal para la gestión empresarial.

> *No es difícil reconocer* [en la nueva gestión empresarial] *el eco de las denuncias antijerárquicas y de las aspiraciones de autonomía que se expresaron con fuerza a finales de la década de 1960 y durante la de 1970. De hecho, esta filiación es reivindicada por algunos de los consultores que, provenientes del izquierdismo y, sobre todo, del movimiento autogestionario, subrayan la continuidad, tras el giro político de 1983, entre su compromiso de juventud y las actividades que han llevado a cabo en las empresas, donde han tratado de hacer las condiciones de trabajo más atractivas, mejorar la productividad, desarrollar la calidad y aumentar los beneficios. Así, por ejemplo, las cualidades que en este nuevo espíritu* [del capitalismo] *son garantes del éxito —la autonomía, la espontaneidad, la movilidad, la capacidad rizomática, la pluricompetencia (en oposición a la rígida especialización de la antigua división del trabajo), la convivencialidad, la apertura a los otros y a las novedades, la disponibilidad, la creatividad, la intuición visionaria, la sensibilidad ante las diferencias, la capacidad de escucha con respecto a lo vivido y la aceptación de experiencias múltiples, la atracción por lo informal y la búsqueda de contactos interpersonales— están sacadas directamente del repertorio de mayo de 1968. Sin embargo, estos temas, que en los textos del movimiento de mayo de 1968 iban acompañados de una crítica radical del capitalismo (y, en particular, de una crítica de la explotación) y del anuncio de su fin inminente, en la literatura de la nueva gestión empresarial se encuentran de algún modo autonomizados, constituidos como objetivos que valen por sí mismos y puestos al servicio de las fuer-*

se hablaba de la Revolución Industrial como el primer momento en el que se identifica progreso tecnológico con progreso social y con cultura, ésa es la base de todo, lo que hemos llamado «cultura del progreso». Yo intercambiaría progreso por desarrollismo, por desarrollo acelerado o continuamente acelerándose, porque todo lo que no es eso es llevar una vía descendente, entrar en recesión, y eso es la base del acceso a la tecnología: de que cada año tengamos que comprar un ordenador nuevo, que cada año tengamos que estar actualizando saberes pero que nunca cuestionemos la base de relaciones interpersonales y colectivas sobre las que se construye todo eso.

MARTA PARA RADIO PWD (JUNIO, 2003)
Yo, digamos que tenía una ajenidad absoluta con respecto a cualquier tipo de tecnología [...] hasta

zas que antes trataban de destruir. La crítica de la división del trabajo, de la jerarquía y de la vigilancia, es decir, de la forma en que el capitalismo industrial aliena la libertad es, de este modo, separada de la crítica de la alienación mercantil, de la opresión de las fuerzas impersonales del mercado que, sin embargo, eran algo que la acompañaba casi siempre en los escritos contestatarios de la década de 1970.[26]

¿Quién encarna, mejor que nadie, este nuevo espíritu del capitalismo? El *manager*.

El manager *es el hombre de la redes. Tiene como primera cualidad su movilidad, su capacidad para desplazarse sin arredrarse por las fronteras —sean estas geográficas o derivadas de pertenencias de tipo profesional o cultural—, por las diferencias jerárquicas, de estatuto, de papel desempeñado, de origen, de grupo, y su capacidad para establecer un contacto personal con otros actores, a menudo muy alejados social o espacialmente.*

[...] La autoridad que adquieren sobre sus equipos está ligada a la «confianza» que les es otorgada gracias a su capacidad de «comunicación» y de «escucha», que se manifiesta en el cara a cara con los demás.

Los managers *se diferencian de los cuadros a través de la oposición entre intuición creativa versus fría racionalidad calculadora y gestora, retomando una temática inserta, de múltiples maneras, desde mediados del siglo XIX aproximadamente, en un gran número de oposiciones taxonómicas, ya se trate, por ejemplo, de las formas de inteligencia (hemisferio izquierdo/hemisferio derecho del cerebro), de la oposición entre los sexos, entre grupos sociales (artistas/ingenieros o financieros), incluso entre países.*

26. Luc Boltanski y Ève Chiapello (2002) *El nuevo espíritu del capitalismo*. Madrid, Akal.

que llegué al Laboratorio y empecé a aprender y a utilizarlas con absoluta normalidad, sobre todo ordenadores, pero no sólo. Al mismo tiempo, empecé a leer cosas sobre ciberfeminismo que decían que Internet, al eliminar el cuerpo, eliminaba las diferencias de género, que en Internet nos podíamos inventar por completo las identidades y hacer que se multiplicaran los géneros y sexos. Sin embargo, a medida que fui abriendo campos y fui conociendo gente que se relacionaba de manera más activa con las tecnologías, fui descubriendo que la mayoría de hombres era abrumadora. Recuerdo cosas que contabais, como congresos de Hispalinux donde había 600 hombres y 3 mujeres, y era algo que me sorprendía muchísimo, me preguntaba por qué sería y no conseguía darme ninguna explicación convincente. Recientemente, a través de Precarias a la Deriva, he empezado a encontrar algunas respuestas, que, por un lado, tienen que ver con la división sexual del trabajo: a

> *[...] Suele pedirse a los responsables que sean eficaces, emprendedores y audaces. Se espera de ellos que decidan, realicen sus objetivos, controlen sus resultados y triunfen. Todas ellas son cualidades masculinas y dinámicas. Sin embargo, el mundo está evolucionando rápidamente. La empresa debe ser capaz de anticipar, de localizar los cambios y de adaptarse. Necesita para ello de un nuevo registro de competencias: escucha, intuición, observación, comunicación, participación del personal, creatividad, sentido de servicio, motivación... Cualidades que destacan por ser más bien de apertura y de receptividad.*[27]

Es decir, femeninas. Sadie Plant iba bien encaminada cuando decía que la identidad masculina tiene todo que perder en las redes. Ciertamente, la red ha feminizado, pero no como queríamos.

Netocracia

Hackers, managers, y quien quiera que viva con naturalidad de forma propositiva en la red es que ha desplegado cualidades femeninas (sin desprenderse de las masculinas, claro está). Nos gustaría ver esto como una disolución de los géneros pero, más bien, lo que constatamos es que lo masculino ha integrado jerárquicamente lo femenino, como si los unos ya no pudieran conectar entre sí si no van rellenos de ceros. Y es que las redes integran aquello que atrapan. Y lo peor del caso es que parecen haber atrapado la vida toda. Bueno, quizás lo peor no sea eso, sino la escasa problematización que de esta integración hacemos los hackers cuando pensamos sobre nosotros mismos.

27. Ibidem.

primera vista, en la experiencia más inmediata, podría parecer que la división sexual del trabajo se ha atenuado, se ha desdibujado, pero si miras datos, realmente, ves que las mujeres, si se relacionan con la tecnología, lo hacen sobre todo como usuarias, pero no las construyen. En el uso activo de las tecnologías (programadores, etc.) sigue habiendo arrolladora mayoría de hombres. Esto tiene que ver, creo, con que las mujeres siguen teniendo una mayor presencia en el sector de los cuidados, de la atención, de la comunicación, del trabajo relacional, de los servicios al consumidor, etc., y tal vez podría decirse que esta división sexual del trabajo se traduce en que las mujeres, actualmente, en nuestras sociedades (y digo las mujeres, por un lado, haciendo, claro, una abstracción que aplasta experiencias singulares y, por otro, refiriéndome a un conjunto determinado social, histórica y espacialmente) tienden más a la relación, a la actividad relacional (de ahí, quizá,

Los primeros en hablar de netocracia fueron los suecos Bard y Söderqvist. [...] Recoglan su tesis central de Pekka Himanen (autor de La ética del hacker*) y otros sociólogos cercanos a Manuel Castells. Al capitalismo seguirá un nuevo orden social y económico: el informacionismo, del que estamos viviendo los primeros albores. Paralelamente, y ésta era su principal aportación, si los anteriores sistemas sociales vieron el protagonismo de la nobleza y la burguesía, el nuevo verá el de los netócratas, una nueva clase social definida por su capacidad de relación y ordenación en las redes globales. Una clase definida no tanto por su poder sobre el sistema productivo como por su capacidad de liderazgo sobre el consumo de los miembros masivos de las redes sociales.*

Bard y Söderqvist no sólo crearon nombre y concepto, nos dibujaron a los hackers de Himanen (nosotros mismos) un paso más allá en el tiempo y la influencia. Los netócratas son los hackers que no se han integrado en el mundo establecido como asalariados y que han conseguido alcanzar —normalmente usando Internet de un modo u otro— un estadio de independencia económica y libertad personal. Sus netócratas son hackers con influencia política y económica real. Son microempresarios tekis, creativos, innovadores sociales, los héroes locales de la sociedad del conocimiento...

«En una organización social en continua revolución, en la que la información en sí misma tiene un valor limitado y lo realmente valioso es la atención y sobre todo la capacidad para generarla, la jerarquía social viene determinada por la pertenencia a las redes más valiosas. Redes que se hacen y deshacen continuamente en una competencia sin fin y sin triunfadores estables.

[...] El netócrata hereda del hacker su concepción del tiempo, el dinero y el trabajo. Tiempo que no se mide ya con el cronómetro ni con la jornada. Su trabajo es creativo, su tiempo es flexible. Piensa a medio plazo, no mide el tiempo en horas sino en proyectos. Vitalmente ocio y trabajo se confunden en placer y reto intelectual. El tiempo de trabajo ya no es una

como decíais, el uso masivo por parte de mujeres del chat), mientras que los hombres tienden más hacia una autorrealización que, en estos momentos, se produce sobre todo programando y construyendo máquinas.

La práctica feminista que he vivido siempre como más interesante pero sobre todo la que más fuerza ha demostrado, desde mi punto de vista, para enfrentar problemas cotidianos es la autovalorización desde la diferencia (desde las diferencias), esto es, desde espacios y prácticas exclusivamente de mujeres: desde ahí se mueven cosas que operan en estratos muy profundos de tu subjetividad, cosas que permiten romper con determinadas barreras, descubrir potencia donde antes podía haber inseguridad, inventar devenires, redefinir lo importante y lo que no lo es, lo real y lo irreal. Cosas que cuando estás en espacios mixtos no suceden.

no-vida opuesta y separada, contingentada por una barrera de jornada y salario. El netócrata se expresa en lo que hace. Vive su yo, sus yoes y cobra en reconocimiento intelectual y social una vez alcanza los ingresos monetarios que le permiten dedicarse exclusivamente a ser y expresarse.

Al igual que su tiempo y su hacer no se separan en diques, sus relaciones personales tampoco. Trabaja con quien quiere; si trabajo y vida no se oponen, cómo va a diferenciar entre relación personal y relación de trabajo. El netócrata quiere vivir las relaciones, maximizar su valor de disfrute. Da a cambio accesibilidad a su ser, no propiedad sobre su tiempo o localización física. Importa el flujo que la relación genera, no capitalizarla convirtiéndola en stock.[28]

Los unos recubren los ceros, el trabajo recubre la vida. El ciberfeminismo se queda perplejo, y la singularidad de «las mujeres» debe ser replanteada.

Y Penélope se cansó[29]

Habitualmente, la aplastante falta de participación de mujeres en las actividades relacionadas con las tecnologías se ve, justamente, como eso: falta de participación, es decir, déficit, carencia. Desde este punto de vista, la consecuencia es muy clara: hay que hacer una llamamiento a la participación de las mujeres poniendo en marcha los procesos materiales que faciliten la superación de estas deficiencias (formación, superación de la división sexual del trabajo, etc.).

Pero la participación no es el problema, porque estos llamamientos tienen lugar dentro de un sistema que impone la participación como obligación, aunque bajo el formato de elección libre.

28. De Ugarte, David, *Como una enredadera y no como un árbol*, http://www.ciberpunk.com/indias/enredadera_12.html.
29. Muchas de estas ideas están tomadas de otros, entre ellos el Colectivo Situaciones (www.situaciones.org), la fundación Espai en Blanc (www.espaienblanc.net) y la Oficina 2004 (www.sindominio.net/ofic2004).

Yo no creo que el uso de las nuevas tecnologías sea un factor especial o esencialmente liberador, así, en abstracto, para las mujeres, sobre todo en la medida de que no es un terreno privilegiado de presencia femenina, pero no cabe duda de que, en tanto en cuanto el mundo se construye cada vez más a través de las nuevas tecnologías, es inevitable abordarlas, hay que tomarlas como apuesta y desafío.

Para intentar explicar en qué sentido decimos que «la participación no es el problema» tomemos un ejemplo: hace años un reducido grupo de afinidad decidimos que debíamos «abandonar» la batalla por el acceso universal a Internet, puesto que este acceso universal iba a ser asumido por el sistema como una necesidad suya propia y que, en cambio, debíamos centrarnos en la construcción de comunidades con autonomía existencial, económica y comunicativa (y así nació Sindominio). Tomamos esta decisión aun a sabiendas de que el acceso universal que el sistema iba a ofrecer no sería absolutamente igualitario, pero, incluso aceptando ese déficit, pusimos en marcha unas líneas de actuación (que se demostraron muy acertadas) bajo la premisa de que «el acceso no era el problema».

Bien. Pero, entonces ¿cuál es el problema?

Van a llegar tarde, van a llegar tarde

En las conversaciones que hemos mantenido para elaborar estos textos, uno de los temas más recurrentes ha sido el asunto del «tiempo».

Ojalá fuera más rápida. Quiero decir, ojalá una cabeza humana o mi cabeza en todo caso, pudiera abarcar más y más rápidamente de lo que lo hace; y si hubiera fabricado mi propia cabeza, hubiera dotado a los deseos y ambiciones un poco más según su capacidad.... con el tiempo lo haré todo, muy probablemente. Y si no, por qué, no importa, y, al menos, me habré divertido.[30]

Lejos de compartir las aspiraciones de Lovelace, pronunciadas cuando el trabajo era mucho menos abstracto que ahora, las mujeres con las que hemos hablado se preguntan: «¿Por qué tiene que hacerse todo con tanta prisa? Nosotras no pode-

30. Ada Lovelace en septiembre de 1840, citada por Plant, Sadie: *Ceros+Unos*, *op. cit.*

mos estar continuamente en el ciberespacio, tenemos otras cosas que hacer». «Además», añaden, «las relaciones virtuales no compensan». Mujeres que se resisten a aceptar como propio el gesto obsesivo del conejo ante Alicia: «voy a llegar tarde, voy a llegar tarde».

> *Paul Virilio sostiene, desde su libro* Vitesse et politique *de 1977, que la velocidad es el factor decisivo de la historia moderna. Gracias a la velocidad, dice Virilio, se ganan las guerras, tanto las militares como las comerciales. [...] La aceleración de los intercambios informativos ha producido y está produciendo un efecto patológico en la mente humana individual y, con mayor razón, en la colectiva. Los individuos no están en condiciones de elaborar conscientemente la inmensa y creciente masa de información que entra en sus ordenadores, en sus teléfonos portátiles, en sus pantallas de televisión, en sus agendas electrónicas y en sus cabezas. Sin embargo, parece que es indispensable seguir, conocer, valorar, asimilar y elaborar toda esta información si se quiere ser eficiente, competitivo, ganador. [...] El universo de los emisores (o ciberespacio) procede ya a velocidad sobrehumana y se vuelve intraducible para el universo de los receptores (o cibertiempo) que no puede ir más rápido de lo que permiten la materia física de la que está hecho nuestro cerebro, la lentitud de nuestro cuerpo o la necesidad de caricias y de afecto. Se abre así un desfase patógeno y se difunde la enfermedad mental, como lo muestran las estadísticas y, sobre todo, nuestra experiencia cotidiana.*[31]

Autonomía significa autoafirmación, capacidad de producir un tiempo propio que se sustraiga de las exigencias ajenas. La capacidad de fijarse tiempos, temas, recursos, espacios e iniciativas propios es difícil de conseguir, especialmente si esto no quiere hacerse desde los espacios centrales de concentración de poder y de saber, que son los que asignan significados, sino desde la reproducción inmediata de la vida, desde la atención a los cuerpos propios y ajenos.

No hay posibilidades de imponer un espacio, un tiempo, un pensamiento y unos recursos propios sin desarrollar grupos capaces de encontrarse con otras experiencias, de anudar circuitos reproductivos autónomos, de producir, sostener y proteger las experiencias de autonomía.

Mujeres que se resisten a estar siempre dispuestas, siempre en red. Mujeres que se resisten a la obsolescencia, a la obligación compulsiva de abarcar la novedad, de aprender hasta el infinito porque justo cuando lo acabas de aprender (y precisamente por eso) pierde su valor. Mujeres que se resisten a perseguir un *uptime*, a someterse a un *upgrade*, al estrés de la infoproducción. Resistencias que no alcanzan a producir ese tiempo y espacio propios. No alcanzan a crear «otro mundo» pero su gesto escéptico desafía al mundo sólo de la *net-economy*. Resistencias extremadamente ambiguas. Intuiciones de gran valor.

31. Berardi, Franco («Bifo») (2003) *La fábrica de la infelicidad, nuevas formas de trabajo y movimiento global*, Traficantes de sueños, Madrid.

Módems, muchos módems

Cuando aceptamos el encargo de redactar estas líneas presuponíamos que la relación de las mujeres con las tecnologías era escasa y poco significativa. Tras hablar con algunas mujeres, navegar por Internet y buscar referencias, hemos descubierto gran cantidad de grupos, ideas y experiencias. Jude Milhon, veterana hacker y feminista fallecida a causa de un cáncer mientras escribíamos estas líneas (y una completa desconocida para nosotras hasta ese momento), afirmaba que las mujeres necesitan módems. Y, de hecho, los tienen. En sus casas, en el trabajo o en los cibercafés hablan en chats y foros, usan el correo electrónico, crean espacios de autonomía informativa en la web y emplean sus terminales tanto de forma instrumental como creativa. Su presencia es tan masiva que lo verdaderamente sorprendente es que la actividad de las mujeres no haya dado lugar a la autocreación de una figura similar a lo que la figura del hacker supone para la representación que de sí mismos se hacen ellos.

Ya nos lo había dicho Haraway: «No existe nada en el hecho de ser "mujer" que una de manera natural a las mujeres. No existe incluso el estado de "ser" mujer». Nada de naturaleza. Cyborgs antes que diosas. De esta manera, el feminismo ha socavado sus cimientos y, afortunadamente, esos cimientos no se han recimentado en términos de unidad, de representación ni de proyecto. Mujeres que se resisten a la representación, a la construcción de figuras de concentración de saber y de poder. No tenemos una versión femenina del hacker y, añadimos, ni falta que nos hace.

Desde el discurso del poder las identidades surgen mecánicamente de la estructura social. De esta manera, la multiplicidad se pierde. Pero las identidades de lucha son otra cosa. En lugar de identificar a quienes la estructura social ha colocado en la misma posición (trabajadores con trabajadores, parados con parados, jóvenes con jóvenes, mujeres con mujeres...) las identidades de lucha dislocan la estructura misma, de manera que las expresiones «trabajador», «parado», «joven», «mujer»... pierden su sentido. Las identidades de lucha son frágiles, porque persiguen la línea de la potencia a través de la investigación, el pensamiento, el afecto y la producción de los nuevos saberes, sin producir concentraciones de poder ni de saber. Y, además, necesitan «luchas».

La sociedad red conecta tanto como margina. Mujeres que ya se han resistido a ser representadas mediante una figura que las unifique y se resisten también a construirse como marginadas. El capital destruye los vínculos sociales para reconstruirlos en modo despolitizado. La comunicación afectiva se destruye para reconstruirse como inseguridad y miedo. La experiencia del placer se destruye para reconstruirse como experiencia de la identidad. La erotización de la vida inmediata se destruye para reconstruirse como pasión por el trabajo. Mujeres que se resisten a la abstracción, a la virtualización de las vidas. Ni conectadas ni marginadas. Gestión del silencio.

Esa particular batalla

No es posible combatir al capital como si fuera algo exterior. En rigor, no hay otra forma de combatir el capitalismo, como forma de hegemonía de la tristeza, de la explotación, del individualismo y del mundo de la mercancía, más que produciendo otras formas de sociabilidad, otras imágenes de felicidad, otra política. Resistir es crear (modos de vida). Los modos de vida son frágiles. Requieren cuidados.

Resistencias que no consiguen, ciertamente, alumbrar modos de vida. Resistencias todavía demasiado ambiguas y, sin embargo, muy valiosas.

Tradicionalmente, las luchas contra el capital, por la emancipación, por la libertad... las hemos concebido como procesos en los que la vida se alzaba contra la muerte. El trabajo es la muerte diferida, decíamos; el poder es poder matar... Contra la negrura de la muerte social y colectiva impuesta por el capital mediante un sistema de dominación siempre actualizado luchábamos blandiendo los múltiples colores de la vida: el rechazo del trabajo, la revolución sexual, la democracia directa, la libertad, la autonomía... En definitiva: la vida contra la muerte.

Pero ahora ya sabemos que trabajo y vida no se oponen. Nos lo dice la ideología felicista, nos lo explican los relatos sobre la netocracia y los estudios sobre el cognitariado, lo afirman los hackers cuando hacen de la «pasión» uno de los valores más importantes de su ética y nos lo impone el propio sistema al configurarse como red.

> *En la percepción social, empresa y trabajo cada vez se oponen menos. Lo mismo vale para la consciencia de los trabajadores cognitivos, es decir, de los trabajadores que expresan el nivel más alto de productividad y la mayor capacidad de valorización, y que encarnan la tendencia general del proceso de trabajo social. Quien desarrolla un trabajo de alto contenido cognitivo y, por ello, de baja intercambiabilidad, no contrapone su trabajo a la creación de empresa. Al contrario, tiende a considerar su trabajo, a pesar de que éste sea dependiente desde el punto de vista formal y también sustancial, como la empresa a la que dedica lo mejor de sus propias energías, con independencia de la dimensión económica y jurídica en la que se manifiesta. [...] La palabra empresa ha recuperado algo de su significado humanista original y viene a significar la iniciativa que la persona carga sobre sí para la transformación del mundo, de la naturaleza y de la relación con los demás. [...] En el proceso de trabajo cognitivo queda involucrado lo que es más esencialmente humano: no la fatiga muscular, no la transformación física de la materia, sino la comunicación, la creación de estados mentales, el afecto, el imaginario son el producto al que se aplica la actividad productiva.*[32]

32. Ibidem.

Pero la red no sólo dice que trabajo y vida no se oponen. Lo que dice es que es simplemente viviendo (las vidas concretas que llevamos) como reproducimos esta realidad que es el capitalismo como sociedad red. Y ¿cómo lo dice? Imponiendo la obligación de movilizar la vida para obtener más y más conexiones que siempre están por renegociar, y con la continua amenaza de desconexión si la movilización desfallece.

> *Cada uno de nosotros está solo en su conexión con el mundo. Cada uno libra, con su vida, su particular batalla para no dejar de ingresar en el mundo, para no quedarse fuera, para no hacer de su biografía un relato más de la exclusión. Ésta es la verdad de la sociedad red, ésta y no la participación ciudadana es la realidad de la ciudad-empresa. La inclusión/exclusión de cada uno no se juega en las relaciones de pertenencia a un grupo más amplio (una clase, una comunidad, etc.) sino en la capacidad de conexión, permanentemente alimentada y renovada, que cada uno sea capaz de mantener a través de su actividad como empleado del todo. En esto consiste el contrato social en la sociedad-red. Es un contrato biopolítico, porque pone la vida entera a trabajar. Un contrato fascista, porque no admite alternativas. Un contrato postmoderno, porque en él la soberanía del pueblo y la lucha de clases han desaparecido. Tan precario como los contratos laborales, como los contratos matrimoniales, como los alquileres, como todas las relaciones formalizadas con las que nos vinculamos a lo social, este contrato social se establece unilateralmente con cada uno y obliga autoobligando, controla autocontrolando, reprime autorreprimiendo. Una sola amenaza sin garantías es su arma: «mejor dentro que fuera...», «o conmigo o contra mí». Son las dos fronteras, los dos abismos, que conocen y transitan las dos principales figuras del mapa político actual: el inmigrante y el terrorista.*[33]

Trabajo y vida ya no se oponen. El trabajo ya no está en el lado de la muerte, sino en el de la vida. Por eso, nuestras experiencias de lucha ya no consisten en poner la vida contra la muerte (como hizo, por ejemplo Radio Alicia), aunque tampoco pueden consistir en poner la muerte contra la vida (como acontenció, por ejemplo, el 11 de septiembre). Ahora, se trata de poner la vida contra la vida, la vida concreta y propia contra la vida puesta a trabajar (que, por supuesto, también es concreta y propia). Las vidas son frágiles, requieren cuidados. Mujeres que se resisten a olvidar el cuerpo.

Nuestros problemas no son la falta de participación, de comunicación, de pasión o de creatividad, porque también en esa vida-puesta-a-trabajar hay de todo eso. El problema está en establecer una diferencia entre ambas vidas que, en realidad, son una misma, la de cada cual. El problema, lo que te corroe y te

33. Garcès, Marina: «BARCELONA: *DEL NO A LA GUERRA AL 2004*», distribuido por correo electrónico.

mata por dentro, es la dificultad, en ausencia de procesos colectivos (colectivos de «verdad», no de activismo voluntarista), de separar lo que el capitalismo en red ha integrado, de abrir una brecha en la experiencia de vivir. La comunicación, por ejemplo. ¿Cómo saber cuándo la comunicación del grupo deviene colaboración con el sistema, movilización total? Ellas son sensibles. Dicen que se nota al momento, en la presión sobre el discurso, sobre la voz... Dicen que es cuando notan que tienen que callar. Gestionar el silencio, la media voz, como espacio de resistencia. Resistencias.

El cuerpo es lo que se cansa, lo que envejece y muere, lo que siente miedo, lo que se resiste. Resistencias de mujeres que, ya lo sabemos, también tienen que devenir-mujer. No lo van a tener más fácil por el hecho de decirse en femenino. Penélope está rodeada de hombres, sola y cansada. Espera, como todas, el acontecimiento que destruya su posición, tejer en el espacio público, destejer en el espacio clandestino. La espera no puede ser más que una lucha. La vida contra la vida. Cuidar las vidas. ¿Cuidar la vida-puesta-a-trabajar? De nuevo, ambigüedad.

> *Las circunstancias señalan que las fuerzas hostiles, favorecidas por el tiempo, han tomado la delantera. En este caso lo que corresponde es la retirada, y es precisamente gracias a la retirada que se obtiene el logro. El éxito consiste en el hecho de que pueda realizarse correctamente la retirada. Es menester no confundir retirada con huida, una fuga que sólo tiene en cuenta la propia salvación, a cualquier precio. La retirada es signo de fortaleza. Es necesario no dejar pasar el momento indicado, mientras uno esté en plena posesión de su vigor y conserve su posición. De este modo sabrá interpretar a tiempo los signos pertinentes y emprenderá los preparativos para una retirada provisional en lugar de trabarse en una desesperada lucha de vida o muerte. De este modo tampoco se abandona sin más el campo a merced del enemigo, sino que más bien se dificulta a este el avance, mostrando todavía una persistencia en ciertos aspectos. De tal manera, en la retirada ya va preparándose el viraje, el cambio. No es fácil comprender las leyes de semejante retirada activa. El sentido que se oculta en un tiempo como éste es importante y significativo.*[34]

Resistencias de mujeres. No aspiran a ser comprendidas, reconocidas ni admiradas. No constituyen una organización, ni una subjetividad ni una identidad. No proyectan, no reflejan y quizás ni siquiera comunican. Islas, enclaves, baluartes. Cuevas, madrigueras, agujeros. Están ahí.

34. I Ching (1979) *El libro de las mutaciones*, Edhasa, Barcelona.

CHAOS COMPUTER CLUB (CCC)

Fernando Blanco Dopazo

El Chaos Computer Club (CCC) es un club alemán de hackers y otras personas interesadas en la información libre, fundado en 1981. Con más de 1.500 miembros es una de las organizaciónes más importantes en la escena europea.

Aboga por la privacidad, la información y el software libre y contra la censura y el control. Todos los años, entre Navidad y Nochevieja, se organiza el *Chaos Communication Congress* en Berlín:

http://es.wikipedia.org/wiki/Chaos_Computer_Club

El Chaos Computer Club es uno de los grupos de hackers más famosos del mundo. En esta nota vemos por qué su fama es merecida.

Existe mucha controversia acerca del Chaos Computer Club (CCC), el que sin duda ha sido el más célebre grupo de hackers de toda la historia. Contó entre sus miembros con los más selectos hackers de aquella generación. Su «cuartel central» está en la ciudad de Hamburgo (Alemania), y aún continua en actividad. Muchos de los miembros más destacados de sus épocas doradas, mediados y fines de los ochenta, se han retirado de las actividades y algunos de ellos son actualmente consultores en seguridad informática o asesores de grandes empresas en este tema. El hecho que los destaca entre todos los distintos grupos de hackers es el haber sido quienes pudieron internarse más profundamente en los «supersecretos» sistemas de la NASA. Hay quienes los ensalzan hasta colocarlos en un nivel mítico, otros los defenestran sin piedad. Pero, en general, lo que existe es un gran desconocimiento de quiénes fueron sus miembros y cuáles sus actividades. Voy a tratar de ofrecer en este artículo algunos detalles técnicos acerca de este espectacular hecho en la historia del hacking.

Todo esto sucedió en máquinas DEC, que corren bajo el sistema operativo VMS. Para quienes no la conocen, Digital Equipment Corporation (DEC) es una empresa líder en el mercado de las computadoras, y cuenta entre sus usuarios con una gran cantidad de empresas privadas e instituciones gubernamentales en todo el mundo. Fue a principios de 1987 o fines de 1986 cuando DEC lanzó al mercado la versión 4.4 de su sistema operativo VAX/VMS. Esta versión incluía algunas novedosas funciones de seguridad. Una de estas funciones tenía un horrible agujero, a través del cual los usuarios sin nivel de acceso podían obtener privilegios para los que no estaban autorizados. Este bug fue corregido en las versiones posteriores del sistema operativo.

El CCC no accedió a las computadoras de la NASA a través de un llamado directo. Sabemos de las medidas de seguridad que tienen, que enseguida identificarían a un usuario extraño tratando de acceder a sus sistemas. Como dice el viejo refrán, que es ley para muchos hackers: «La cadena se rompe por el eslabón más débil». Así fue que los miembros del CCC pudieron acceder a la NASA por medio de la red DECnet. Los miembros del CCC consiguieron obtener privilegios en una máquina miembro de la red que no estaba bien protegida en algún lugar de Alemania. A través de esta máquina, consiguieron introducir un gusano muy simple que se copiaba a todas las máquinas a las que tenía acceso. Si bien el sistema de propagación era un tanto rudimentario, han quedado algunos fragmentos del código de ataque que, por el contrario, era brillante. A través del estudio de este código puede verse que los autores conocían a fondo la nueva versión del sistema operativo. Demostraron también amplios conocimientos en el uso de equipos DEC. Este fascinante código de ataque se basaba en el ya citado bug en los servicios de seguridad, por medio del cual obtenía los privilegios. Luego modificaba (*patcheaba*) varias de las imágenes del sistema y se autoeliminaba. Estos patches son realmente interesantes. Modificaba las imágenes de los programas Monitor, Show y Loginout y agregaba un nombre de usuario especial al archivo de autorización del VMS. Los patches a Monitor y Show conseguían que esos utilitarios ignoraran el nombre de usuario especial que el código de ataque había agregado al archivo de autorización. Esto les permitía a los miembros del CCC permanecer invisibles mientras estaban logeados con ese nombre de usuario especial.

El patch sobre Loginout servía para poder acceder con el nombre de usuario agregado. Además, tomaba todos los passwords con los cuales los usuarios validados se registraban, los encriptaba con un algoritmo simple y los guardaba en una porción muy poco conocida y utilizada del registro de autorizaciones.

Una vez más, vemos los profundos conocimientos que los autores tenían del código de ataque acerca de este tipo de sistemas. Luego de un tiempo, y logeándose con el nombre agregado, podían acceder al registro de autorizaciones, tomar los passwords encriptados que allí había colocado el patch a Loginout y desconectarse. En casa podían desencriptar los passwords (tarea muy sencilla, ya que ellos mismos habían

sido quienes los encriptaron) y, a partir del siguiente acceso, ya podían ingresar por medio de la red a una cuenta legítima sin despertar ningún tipo de sospechas como cualquier usuario normal. Periódicamente se utilizaba el nombre de usuario especial para ir a buscar los nuevos passwords que se habían recolectado en el registro de autorizaciones. Usaban el nombre de usuario especial agregado para que esto pasara inadvertido.

Al contar con diversos passwords, se conseguía distribuir el tiempo de uso del sistema entre diversos usuarios sin recargar demasiado ninguna de las cuentas legítimas, ya que si alguna cuenta aparecía demasiado utilizada podía despertar sospechas. El patch de Loginout registraba todos los passwords ingresados, así consiguieron algunos de máxima seguridad del sistema atacado. Por otra parte, si los encargados de seguridad cambiaban los passwords, sólo había que esperar unos días para que los nuevos se acumularan en el registro de autorizaciones.

Como vemos, el circulo se cerraba completamente, y el plan era prácticamente perfecto. De hecho, por medio de este sistema los miembros del CCC pudieron utilizar gran parte de las máquina de la red DECnet, entre las cuales hay, como ya he señalado, máquinas de grandes empresas privadas y también de muchas instituciones públicas. Fueron descubiertos a principios de abril de 1987 en la NASA, tal vez por un exceso de confianza o de ansiedad de uno de sus miembros. En vez de realizar un acceso breve para verificar si ya había conseguido otros nuevos passwords legítimos y retirarse, este joven miembro pasó largo tiempo husmeando los archivos secretos de la NASA con el nombre especial agregado, en lugar de utilizar un password válido. Uno de los system managers de los sistemas DEC de la NASA vio que se estaban consumiendo muchos recursos de su máquina (por ejemplo, ciclos de CPU), y para intentar ver qué era lo que estaba sucediendo, ejecutó los utilitarios Show y Monitor (que ya estaban patcheados). Así descubrió muy sorprendido que «nadie» estaba utilizando la máquina. Encontrando esta situación muy extraña, este system manager, del que nunca pudo conocerse el nombre, ejecutó un utilitario llamado SDA. El SDA (System Dump Analyser) es un utilitario de las máquinas que corren sistemas operativos VMS que ofrece vuelcos de memoria, es muy poco utilizado ya que son realmente pocas las personas que pueden interpretar un dump (vuelco de memoria). Utilizando el dump, el system manager pudo tener una idea de lo que estaba sucediendo. Si bien el ataque fue descubierto por la imprudencia de uno de los miembros del CCC, debemos también reconocer la calidad técnica de este system manager anónimo, que

demostró conocer muy bien su oficio, resolviendo la situación con solvencia técnica y demostrando grandes conocimientos. El system manager informó de los hechos, y los técnicos de la NASA, junto a especialistas de DEC, pudieron solucionar este problema rápidamente. Se agregaron al sistema nuevos métodos de seguridad que imposibilitaron el acceso a los miembros del CCC, y el error fue corregido.

La NASA dio informaciones ambiguas sobre este hecho, a veces negándolo, a veces señalando que sólo habían accedido a niveles muy bajos, lo que no es verdad. Si bien nunca los pusieron a conocimiento público por temor a las represalias, los miembros del CCC pudieron acceder a los proyectos más secretos de la NASA y tuvieron los password de los más altos miembros de dicha institución. Se dice que algunos de sus miembros y ex miembros todavía guardan algunos archivos de la NASA como «trofeos de guerra» de aquella legendaria acción.

HACKERS: ACTIVISMO POLÍTICO EN LA FRONTERA TECNOLÓGICA

Gustavo Roig Domínguez*
(Nodo50,
gustavo@nodo50.org)

«Extiende un mapa del terreno; coloca sobre éste un mapa del cambio político; sobre este un mapa de la red, especialmente de la contra-red con su énfasis en logística y el flujo de información clandestina; y finalmente, encima de todo, el mapa 1:1 de la imaginación creadora, de la estética, de los valores. La trama resultante cobra vida, animada por remolinos y brotes de energía, coágulos de luz, túneles secretos, sorpresas.»
Hakim Bey, *TAZ*

Dedicado a toda la gente que este verano peleó y resistió en las calles del barrio de Gràcia de Barcelona y del Casco Viejo de Iruña.

SAPIENS SAPIENS: SUPERVIVENCIA, PODER Y CAMBIO TECNOLÓGICO

«¿Dejará el cuerpo productivo la férula patronal para situarse bajo la del Estado? O, por el contrario, ¿aprenderá a trabajar y a producir libremente?, ¿a vivir, tras siglos de traumatizante disciplina, la indisciplina creadora?»
Gaudemar, *El orden y la producción*

La tecnología atraviesa todos los planos de la vida. Media en la relación comunicativa del hombre con sus iguales, de ahí que lo *técnico* sea parte de *lo social* y *lo político*. Lo hace también en la relación del ser humano con su propio cuerpo mediante el conocimiento y el cuidado de sí mismo[1]. De igual manera, la relación del hombre con el mundo físico es fundamentalmente tecnológica, hasta el punto de que la antropología desarrolla el concepto mismo de *cultura* íntimamente relacionado con el de técnica: la *sapientización* de los prehomínidos se explica, en parte, por las ventajas adaptativas que experimentan los *sapiens arcaicos* al desarrollar tecnologías más eficientes de caza y recolección de alimentos[2].

* Madrid, agosto de 2004.

1. «Mi objetivo, desde hace más de veinticinco años, ha sido el de trazar una historia de las diferentes maneras en que, en nuestra cultura, los hombres han desarrollado un saber acerca de sí mismos: economía, biología, psiquiatría, medicina y penología. El punto principal no consiste en aceptar este saber como un valor dado, sino en analizar estas ciencias como "juegos de verdad" específicos, relacionados con técnicas específicas que los hombres utilizan para entenderse a sí mismos». Foucault, M. (1996) *Tecnologías del yo y otros textos afines*. Paidós, Barcelona.
2. Al hablar de *sapientización*, lo hacemos pensando en un conjunto de procesos, a medias fisiológicos, a medias culturales, claramente relacionados y que dan como resultado, en torno al año 35.000 BP (*before present*, en arqueología se conviene que el año 1950 es el punto de partida para datar la antigüedad en la evolución humana), hominidos de gran cerebro sobre los que operó una selección favorable al desarrollo de la actividad cultural articulada sobre una inteligencia y facilidad lingüística crecientes. Harris, M (1989) *Introducción a la antropología general*. Alianza, Madrid.

La revolución más profunda en la historia y en la organización social de la humanidad, la revolución neolítica[3], tiene una base eminentemente tecnológica. La agricultura, la domesticación (de no homínidos) o el dominio de la metalurgia permiten al hombre salir de su estadio de nomadismo salvaje para pasar, con todas sus consecuencias, al sedentarismo, la estratificación social y el desarrollo de la organización [técnica] del Estado. La guerra y la coerción política como tecnologías del poder y del dominio son la base de la civilización[4]. Así, es fácil entender que la aventura de la humanidad es la aventura de la cooperación (la base de lo social) y el mando político de la mano del conjunto de técnicas o disciplinas que doblegaron el medio físico (y el propio cuerpo) y permitieron la supervivencia, garantizando *el orden* y la disciplina social.

La naturaleza social de *lo técnico*, entendida como estrategia de supervivencia del hombre frente al medio físico, se despliega a lo largo de la historia en los diversos modos de producción y propiedad sobre lo producido y sus materias primas. Se explica en la esclavitud cómo técnica de producción y dominio de los imperios hidráulicos[5] mesopotámicos, en Grecia y en Roma[6]. En la servidumbre feudal y tras la revolución industrial (esa revolución del vapor, del acero, de la química y la electricidad), en la alienación del proletario liberado de su condición de medio de producción privado (ya no es el siervo vinculado como un árbol o una mula a la tierra), reconvertido en trabajador social «libre»: dispositivo vivo integrado en el complejo productivo de la cadena de montaje, componente humano de la máquina productiva contemporánea.

Hoy, una vez que el proletariado ha sido expulsado como un cuerpo extraño de la cadena de montaje (condenado al paro y a la precariedad estructural), y el capitalismo se rearticula sobre la producción y gestión de información, dominio militar de recursos naturales y automatización informática de cada vez más espacios de la producción mercantil, cobra forma un nuevo territorio definido por la técnica y redimensionado por la naturaleza política de la vida humana. A la mutación (técnica) en la forma (económica) de producir, se solapa un proceso de redefinición de las condiciones de vida y de las concepciones que sobre el mundo han

3. Harris, M (1989).
4. «Allá en el antiguo Oriente ocurrieron al menos algunos de los episodios del gran drama de la conquista de la civilización. Los más destacados fueron: la revolución que condujo al hombre de ser meramente parásito a la adopción de la agricultura y el almacenaje de provisiones, convirtiéndole en creador, emancipado de las trabas de su medio ambiente, y después el descubrimiento del metal y el conocimiento de sus propiedades. En efecto, todo esto pasó antes de que el telón de ese gran drama se alzase para nosotros». Gordon Childe, V. (1985) *Nacimiento de las civilizaciones orientales*. Ediciones Peninsula, Barcelona.
5. «En la época en que el aumento de producción dependía ante todo del perfeccionamiento del sistema de riego, se formó un grupo de hombres sobre los que recayó el cuidado del mantenimiento de las instalaciones hidráulicas y que decidían sobre la necesidad y utilidad de éstas. A la cabeza de estos grupos se encontraban aquellas personas que, bien por haber concentrado en sus manos una gran cantidad de medios de producción o bien por poseer determinados conocimientos, habían conseguido constituirse en una clase dirigente. Aquel que, sirviéndose de estos medios, pudiera decir la última palabra sobre el sistema de riegos, alcanzaba igualmente el poder sobre todo el territorio». Klima, J. (1983) *Sociedad y cultura en la Antigua Mesopotamia*. Akal Universitaria, Madrid.
6. «Catón indica cuál era la escuadra normal de esclavos necesaria para el mantenimiento de un olivar de 240 yaguadas (más o menos 60 hectáreas): un guardián (vigilante de los esclavos, elegido entre ellos mismos); una guardiana (gobernanta, la más de las veces mujer del guardián); 5 obreros; 3 carreteros; 1 caballerizo; 1 porquero; 1 pastor: en total 13 hombres». Kovaliov, S. I. (1979) *Historia de Roma*. Akal Textos, Madrid.

LA ACTITUD DEL HACKER

Eric S. Raymond

Los hackers resuelven problemas y construyen cosas, y creen en la libertad y la ayuda mutua voluntaria. Para ser aceptado como hacker, debe comportarse como si tuviera esta clase de actitud en su interior. Y para comportarse como si tuviera esta actitud, debe creerse de verdad dicha actitud.

Pero si piensa en cultivar las actitudes de hacker simplemente como una forma de ganar aceptación en esta cultura, no acertará. Transformarse en la clase de persona que cree estas cosas es importante para usted, para ayudarle a aprender y mantenerse motivado. Como en todas las artes

utilizado tradicionalmente los actores sociales contemporáneos: las clases (objetivas), los movimientos (la conciencia en acción), sus estructuras de intervención política (la voluntad de poder organizada en forma de partidos) y su imaginario, reaccionario o insurgente. Un nuevo escenario, un nuevo sujeto, un nuevo conflicto se esboza en un contexto de producción y vida que nace sobre un paradigma tecnológico emergente que impone el desarrollo de las telecomunicaciones y la representación digital de lo real.

El *ciberespacio*[7]: zona en la que se cruzan, digitalizados, los eventos y las relaciones sociales que fluyen desde todos los planos o campos de la realidad humana, de lo social. Un *sitio* inmaterial y real a un tiempo, ubicado entre miles de máquinas interconectadas, espacio de comunicación entre dispositivos más o menos automatizados, diseñados y administrados por personas, que es territorio de acción y por tanto de conflicto. En él se compra, se vota, se vende, se opina, se conspira, se pierde y se gana dinero, se investiga, se escribe, *se lucha*. Se generan códigos e identidades compartidas, se estructuran movimientos sociales y se traslada el conjunto de la actividad social, a la que, dada la especificidad del medio, se le superpone un conjunto de elementos característicos, novedosos o incluso novísimos, que lo convierten en un fascinante objeto de estudio en cada una de sus dimensiones. De la misma manera que la fábrica y la metrópoli escenificaron en los últimos doscientos años buena parte de la conflictividad social contemporánea, este nuevo territorio se configura como (un) nuevo escenario para la creación política, la organización y extensión de la protesta. ¿Sobre qué presupuestos?, ¿cómo?, ¿quiénes?, ¿diciendo qué? Sobre ello hablaremos en este artículo.

7. «Un escritor de ciencia ficción acuñó el útil término "ciberespacio" en 1982. Pero 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, el dispositivo de plástico de tu mesa. No en el interior del teléfono de la otra persona, en otra ciudad. El lugar entre los teléfonos. El lugar indefinido de ahí fuera, donde vosotros dos, dos seres humanos, os encontráis y os comunicáis». Sterling, B. (1994) *The hacker crackdown*. http://www.bufetalmeida.com/textos/hackercrack/libro.html (visitada por última vez el 29-06-04).

creativas, el modo más efectivo de llegar a ser un maestro es imitar la mentalidad de los maestros, no sólo intelectualmente, sino también emocionalmente.

Por lo tanto, si quiere ser un hacker, repita lo siguiente hasta que se lo crea:

1. *El mundo está lleno de problemas fascinantes que esperan ser resueltos.*

Ser un hacker es muy divertido, pero es una clase de diversión que requiere mucho esfuerzo. El esfuerzo requiere motivación. Los atletas ansiosos de éxito obtienen su motivación de un tipo de placer físico que surge al hacer trabajar su cuerpo, al forzarse a sí mismos más allá de sus propios límites físicos. De manera similar, para ser un hacker usted debe sentir un estremecimiento de tipo primitivo cuando resuelve problemas, aguza sus habilidades y ejercita su inteligencia. Si no es el tipo de persona que siente de esta manera de modo natural, necesitará acabar siéndolo para

Las lecturas del hacker

«Yo tengo una teoría similar que desarrollé cuando estaba en matemáticas: la anarquía es un límite matemático, en el que la ariable es el individuo tendiendo a la solidaridad, y la ecuación o expresión matemática de la que queremos calcular el límite es la sociedad.»
genis, hackmeeting@listas.sindominio.net

En 1983, William Gibson escribe su primera gran novela sobre la vida en las redes de ordenadores, la circuitería electrónica y los flujos de datos digitalizados que soportan la estructura de la civilización contemporánea. *El Neuromante*[8], el clásico del ciberpunk y la generación de ciberactivistas que se crea en los noventa y es objeto de investigación de este trabajo. Cuando Gibson inventa la palabra *ciberespacio*[9] lo hace con la intención de dar forma a la metáfora futurista del mundo moderno en el que la concentración del poder en las manos de unas pocas familias empresariales sólo es posible sobre la base del dominio y desarrollo de las tecnologías digitales de la comunicación y la automatización de la producción. Gibson acuña un nuevo término para dar salida a la crítica de la tecnología en manos de un puñado de grandes corporaciones empresariales, que convierten el mundo en su dominio sobre un basural de chatarra mecánica y humana. En el universo desolado en el que las máquinas (sería mas correcto decir el *software* que las gobierna) consiguen unificarse en una inteligencia artificial global (Wintermute junto a Neuromante, la IA global) que lo controlará TODO, los protagonistas sobreviven individualmente y a duras penas en el negocio del crimen organizado y el tráfico de datos. El resquicio a través del cual es posible la vida autónoma lo proporciona la capacidad de supervivencia (basada en la inteligencia, la pericia técnica y el acceso ilegal a los datos corporativos), en un escenario de acelerada degradación psíquica y violencia generalizada. Ése es el escenario en el que el protagonista, Case, desempeña sus labores

8. Gibson, W. (1989) *El Neuromante*. Minotauro ed., Barcelona.
9. Gibson, W. (1994) *Quemando cromo*. Minotauro ed., Barcelona.

llegar a ser un hacker. De lo contrario, encontrará que su energía para *hackear* se agotará en distracciones como el sexo, el dinero y la aprobación social.

(Además, deberá desarrollar una especie de fe en su propia capacidad de aprendizaje: la creencia de que, aun cuando pueda no saber todo lo que necesita para resolver el problema, si toma sólo una parte de él y aprende desde allí, aprenderá lo suficiente como para resolver la siguiente parte, y así sucesivamente hasta que lo resuelva por completo).

2. *Ningún problema tendría que ser resuelto dos veces.*

Los cerebros creativos son un recurso valioso y limitado. No deberían desperdiciarse reinventando la rueda cuando hay tantos y tan fascinantes problemas *nuevos* esperando por ahí.

Para comportarse como un hacker, debe creer que el tiempo que otros hackers dedican a

de *vaquero de consola, operador* que sobrevive desviando o robando información protegida tras el ICE (intrusión *countermeasures electronics*), *el hielo* que protege las estructuras de datos de las grandes empresas o instituciones militares.

Lo paradójico de la historia del término *ciberespacio* es que tiene un origen marcadamente literario, metafórico y crítico; no hace referencia a una realidad *material, objetiva, histórica*, sino que recurre a la construcción de un *modelo de ficción* sobre el que proyectar los rasgos fundamentales del mundo en que vivimos: el poder hegemónico de la economía capitalista, la depredación del medio ambiente y la progresiva dominación de la tecnología de la comunicación sobre todos los ámbitos de la producción y de la vida. El *ciberespacio* de Gibson es desolador y una advertencia acerca del rumbo que toman las cosas en el planeta en el último cuarto del siglo XX. Él mismo lo cuenta:

> *Supongo que el libro plantea esas preguntas, pero no las contesta. Yo no las puedo contestar [...] pero, gente como ésta de Autodesk* [y del Media Lab de MIT] *que están construyendo el ciberespacio —me cuesta creerlo, y ya casi lo tienen—, simplemente no se enteran. Mi percepción de lo que estaba haciendo era intentar llegar a algún tipo de metáfora que expresara mi profunda ambivalencia respecto a los medios de comunicación en el siglo XX. Y tuve la satisfacción de conseguirlo en cierto modo, y entonces estos cerebritos llegan y dicen: «¡Demonios, esto es una buena idea! ¡Vamos a ponerlo a funcionar!» Pero, sabes, me deja pensando, «¿Qué es esto?». Esto es incluso más raro que tener a gente haciendo tesis sobre tu trabajo: tener a gente construyendo esta mierda demencial que tú has soñado, cuando estabas intentando hacer una cierta crítica de la sociedad industrial. Es una cosa bastante rara.*[10]

10. *An Interview with William Gibson and Tom Maddox by Darren Wershler-Henry.* http://www.eff.org/Misc/Publications/William_Gibson/maddox.interview. Traducción de Hackitectura.net en http://www.hackitectura.net/osfavelados/el_retorno/cyberpunk/02cyberspace.html (visitadas por última vez el 29-06-04).

pensar es precioso; tanto, que es casi una obligación moral para usted el compartir la información, resolver los problemas y luego exponer la solución de manera que otros hackers puedan resolver *nuevos* problemas, en lugar de tener que enfrentarse perpetuamente con los viejos.

(No tiene que creer que está obligado a regalar *todo* su producto creativo, aunque los hackers que lo hacen son los que obtienen más respeto por parte de los demás hackers. Es compatible con los valores de un hacker vender lo necesario para pagar la comida, el alquiler y las computadoras. Está bien emplear sus habilidades de hacker para sostener a su familia, o incluso hacerse rico, siempre que no olvide la lealtad a su arte y a sus colegas hackers mientras lo hace).

3. ***El aburrimiento y los trabajos rutinarios son perniciosos.***
Los hackers (y las personas creativas en general) nunca deberían aburrirse o ser sometidos a

La pregunta que habría que responder para despejar lo que de paradójico tiene el caso debería ser: ¿cómo pudo haberse convertido esta advertencia apocalíptica sobre los peligros de la recombinación entre poder y tecnología en una de las referencias literarias del activismo tecnológico de los 90?, ¿cómo pudo construirse técnica y culturalmente el *ciberespacio* en el imaginario hacker sobre la base de una anticipación tan descarnada de lo que puede ser el mundo sometido a una racionalidad tecnológica extrema?

Habría que empezar aclarando que un vaquero en la obra de Gibson es un pirata (eminentemente solitario, que coopera tácticamente con otros vaqueros o bandas organizadas de traficantes de datos) que hace de *corsario informativo* al servicio de algún cliente al que en más de una ocasión, tarde o temprano, acaba traicionando. En el conjunto de pautas o premisas ideológicas sobre las que vive un vaquero como Case, el cuerpo es un lastre, un saco de carne sujeto a necesidades elementales, tales como el hambre, el deseo o el sueño, todas ellas prescindibles en la inmaterialidad de las relaciones sociales que se dan en la red. Conectada a la *matriz* mediante neurotransmisores o *trodos*, la mente se desprende del cuerpo y fluye por los múltiples escenarios y realidades que existen en el *ciberespacio*. Sus límites (los de la mente) se establecen en su propia capacidad de trabajo, en la inteligencia operativa del vaquero, en la capacidad de producir o aprovechar el producto del trabajo de otros operadores empeñados en saltar las barreras del hielo, superar las pruebas mas arriesgadas, llegar más lejos.

> *Case tenía veinticuatro años. A los veintidós, había sido vaquero, un cuatrero, uno de los mejores [...] Operaba en un estado adrenalínico alto y casi permanente, un derivado de juventud y destreza, conectado a una consola de ciberespacio hecha por encargo [...]. Ladrón, trabajaba para otros: ladrones más adinerados, patrones que proveían el exótico software*

estúpidos trabajos repetitivos, porque cuando esto sucede significa que no están haciendo lo que sólo ellos pueden hacer: resolver nuevos problemas. Este desperdicio daña a todo el mundo. Por ello, el aburrimiento y los trabajos rutinarios no sólo son desagradables, sino intrínsecamente perversos.

Para comportarse como un hacker, debe creer esto lo suficiente como para querer automatizar las partes aburridas cuanto sea posible, no solamente por Ud., sino para beneficio de todos los demás (especialmente otros hackers).

(Hay una aparente excepción a esta regla. Los hackers hacen a veces cosas que pueden parecer repetitivas o aburridas a un observador, como ejercicio para aclarar la mente, adquirir cierta habilidad u obtener algún tipo de experiencia que no se podría conseguir de otro modo. Pero lo

requerido para atravesar los muros brillantes de los sistemas empresariales, abriendo ventanas hacia los ricos campos de la información.[11]

Un vaquero, pues, es un pirata individualista, un corsario que vive en el límite de la legalidad, en el borde frágil de la materialidad y, por lo tanto, en un espacio novedoso respecto a la realidad social. En ese espacio su cuerpo no le sirve:

Esto era lo que él era. Olvidó comer. [...] A veces se resistía a tener que dejar el tablero para utilizar el inodoro químico que habían instalado en un rincón de la buhardilla. [...] Un laberinto multicolor de puntos electrónicos fue lo primero que vio al despertar. Iría directamente al tablero sin molestarse en vestirse, y se conectaría. Estaba entrando, estaba trabajando. Perdió la cuenta de los días.[12]

Como veremos más adelante, nuestro trabajo aborda el universo político de un tipo de activista que define su ámbito de acción en el cruce de planos entre determinadas redes sociales urbanas y telemáticas. Una concepción de lo tecnológico en relación a lo social desde donde se definirá *una praxis*, se articulará *un discurso* y tomará cuerpo un *proyecto político*: el ciberactivismo, el *hacking* político-social de la última década. Pero ¿qué relación hay entre este nuevo modelo de militancia electrónica y el antihéroe, vaquero delincuente, de *El Neuromante*? Podríamos pensar que ninguna, si nos limitáramos a extraer de la trama la figura del vaquero que si bien puede representar el tipo ideal de *free-rider* o *bad boy* de las redes telemáticas, poco tiene que compartir con el activista ideologizado, con un discurso y universo conceptual modelado en los espacios de producción identitaria de las redes sociales. ***Poco o nada en común salvo el medio***.

11. Gibson, W. (1989).
12. Gibson, W. (1989).

hacen por elección, nadie capaz de pensar debería ser nunca metido a la fuerza en situaciones que le aburran.)

4. ***La libertad es buena.***

Los hackers son antiautoritarios por naturaleza. Cualquiera que pueda darle órdenes, puede obligarle a dejar de resolver el problema que le esté fascinando, dado el modo en que trabajan las mentes autoritarias, generalmente encontrará alguna razón espantosamente estúpida para hacerlo. Por ello, las actitudes autoritarias deben ser combatidas donde quiera que las encuentre, no sea que le asfixien a usted y a otros hackers.

(Esto no es lo mismo que combatir toda autoridad. Los niños necesitan guía, y los criminales, restricciones. Un hacker puede estar de acuerdo en aceptar algún tipo de autoridad para poder

Sobre la base de sus limitados conocimientos técnicos, Gibson intuye, imagina e inventa un nuevo escenario para la vida, un nuevo medio que comunica a las máquinas y, junto con ellas, a las personas. Una dimensión inmaterial de la relación social en la que es perfectamente posible *ser algo* y sobre todo *ser alguien*, disponer de una identidad y experimentar sensaciones reales. El *ciberespacio* de Gibson es un terreno de lucha y conflicto entre sujetos sociales que articulan relaciones de mando, dominio y poder como proyección de las que existen ya en el mundo material, que instituyen incluso nuevas (por virtuales) formas de relación y control social; por lo tanto, espacio óptimo para las resistencias, para la guerrilla informacional, la reapropiación tecnológica como estrategia de liberación y la superación del paradigma mercantilista sobre la producción de conocimiento[13]. En este medio y en este plano del imaginario ciberpunk cristaliza la corriente de activismo político tecnológico que nace en los primeros grupos de hackers[14] del MIT[15],

13. «Pero a la teoría del mercado tan centrada en el individuo y en lo que se puede medir y vender le cuesta aceptar este hecho. No consigue entender cómo unas comunidades estructuradas sobre la confianza, el trabajo voluntario y la colaboración pueden ser más eficientes y flexibles que los mercados convencionales del "mundo real". Y es que no consigue valorar en sus justos términos el potencial en creación de valor de la "producción entre iguales". Quizá sea porque en el mundo de los negocios se busca el máximo rendimiento en un plazo corto, mientras que esta producción entre iguales es sobre todo un proceso social continuo que gira alrededor de valores compartidos. En los negocios se buscan recursos que sea fácil convertir en bienes de consumo y vender, mientras que el resultado del trabajo en estas relaciones entre iguales tiende a considerarse propiedad inalienable de toda la comunidad». Bollier, D. (2003) «El redescubrimiento del procomún». *Biblioweb*. http://www.sindominio.net/biblioweb/telematica/bollier.html» (visitada por última vez el 1 de julio del 2004].

14. «Los comienzos de la cultura hacker, tal como la conocemos actualmente, se pueden fechar con seguridad en 1961, año en que el MIT adquirió la primera PDP-1. El comité de Señales y Energía del Tech Model Railroad Club adoptó la computadora como su juguete tecnológico preferido e inventó herramientas de programación, un argot y toda una cultura en torno a ella que aún hoy puede reconocerse entre nosotros. Estos primeros años han sido examinados en la primera parte del libro de Steven Levy, *Hackers*.

«La cultura en torno a las computadoras del MIT parece haber sido la primera en adoptar el término "hacker". Los hackers del Tech Model Railroad Club se convirtieron en el núcleo del Laboratorio de Inteligencia Artificial del MIT, el centro más destacado de investigación sobre Inteligencia Artificial de todo el mundo a principios de los 80. Su influencia se extendió por todas partes a partir de 1969, año de creación de ARPANET». Raymon, E. (2000) «Breve historia de la cultura hacker». *Biblioweb*. http://www.sindominio.net/biblioweb/telematica/historia-cultura-hacker.html (visitada por última vez el 1 de julio del 2004].

15. «En este nuevo mundo ya no basta con hacer nuestro trabajo: se supone que debemos iluminarnos a nosotros mismos y nuestro trabajo, darle la vuelta, examinarlo, rehacerlo y volver a examinarlo otra vez». Williams, R. (2004) *Cultura y cambio tecnológico: el MIT*. Alianza ed., Madrid.

obtener algo que desea más que el tiempo que gasta en seguir órdenes. Pero éste es un pacto limitado y consciente; la clase de sumisión personal que desean los autoritarios no está en oferta).

Los autoritarios prosperan en la censura y el secreto. Y desconfían de la cooperación voluntaria y el intercambio de información, sólo les agrada la cooperación que tienen bajo su control. Así que, para comportarse como un hacker, deberá desarrollar una hostilidad instintiva hacia la censura, el secreto, y la utilización de la fuerza o el fraude para someter a adultos responsables. Y deberá estar preparado para actuar en consecuencia.

5. ***La actitud no es sustituto de la competencia.***

Para ser un hacker, deberá desarrollar algunas de estas actitudes. Pero simplemente cuidar la actitud no le transformará en hacker, como tampoco le transformará en un atleta campeón o en estrella

y se despliega con su potencia máxima en el fenómeno del software libre[16] y las prácticas tecnicopolíticas de los últimos años. El vínculo entre el escenario originario y las prácticas actuales lo percibe con claridad alguno del los activistas más destacados del hacking sevillano para el que Gibson es referencia obligada:

> *Mientras la mayor parte de la población vive una existencia bastante previsible entre los concursos de la tv, el trabajo burocrático, el consumo estandarizado y el turismo de masas, los zapatistas desde un rincón de la selva centroamericana proponen una interpretación de los procesos globales radicalmente nueva; dos hackers en un garaje de California diseñan el primer ordenador personal; un grupo de investigadores y comerciantes diseñan desde Seattle las herramientas para habitar el ciberespacio que usarán el 95% de los internautas; una banda de hackers y activistas que se encuentran en Evian producen un agenciamiento de tecnologías con el potencial de revolucionar el uso y la apropiación de las imágenes; otra banda de mediactivistas construye un puente virtual para unir a la multitud a ambos lados del Estrecho de Gibraltar [...] Este mundo y este orden de deseos es el que recrea la ficción de Gibson.*[17]

La distopía de Gibson alcanza y sostiene el imaginario de la acción colectiva. Pero el salto entre el ciberespacio que anticipa *El Neuromante* y las redes sociales de activismo tecnicopolítico de finales de los noventa no se da sobre el vacío. Hakim Bey[18], visionario, poeta y militante de la cultura y la política *under-*

16. Garcia, J. y Romeo, A. (2003) *La pastilla roja. Software libre y revolución digital.* EditLin ed., Madrid.
17. Hackitectura/Osfavelados.
http://www.hackitectura.net/osfavelados/el_retorno/cyberpunk/04tecnologias.html#02_taylor.
18. «Hakim Bey, de supuestamente auténtico nombre Peter Lamborn Wilson, escritor, poeta y filósofo, residente en algún lugar cercano a Nueva York, se hizo famoso al desarrollar en los años 70 la teoría de las Zonas Autónomas Temporales (TAZ), ideología fundamental de los grupos rebeldes que actúan en y desde Internet». Molist, M. (?) *Hakim Bey: adiós a la red.* http://ww2.grn.es/merce/hakim.html (visitada por última vez el 29-06-04).

del rock. Llegar a ser un hacker le exigirá inteligencia, práctica, dedicación y trabajo duro. Por lo tanto, debe aprender a desconfiar de la actitud y respetar la competencia en todas sus formas. Los hackers no permiten que gente que adopta la pose de hacker les haga perder el tiempo, pero veneran la competencia, especialmente la competencia al hackear, pero la competencia en cualquier ámbito es buena. Especialmente buena es la competencia en habilidades exigentes que pocos pueden dominar, y la mejor es la competencia en habilidades exigentes que requieren agudeza mental, maña y concentración. Si usted respeta la competencia, disfrutará desarrollándola en sí mismo; el trabajo duro y la dedicación se volverán una especie de juego intenso, y no una rutina. Esa actitud es vital para llegar a ser un hacker.

ground en los ochenta-noventa, hace de puente e imprime al activismo la impronta libertaria y un alambicado imaginario poético y político, liberando el concepto de *ciberespacio* de su base estrictamente literaria y sus reminiscencias ciberpunks para colocarlo en el plano del análisis y las estrategias del conflicto político. A partir de Bey, analizar el ciberespacio y las prácticas posibles es hablar, de alguna manera, de teoría política, de programa político.

Bey redefine el espacio de actuación, lo delimita y lo reduce a una dimensión fundamentalmente política: transforma la percepción del *ciberespacio* como una definición genérica de un nuevo mundo para la interacción social (el plano de Gibson), y lo eleva a la categoría de territorio para la fuga conspirativa, para la liberación de zonas ocultas e intangibles al poder del Estado, *móviles*, *nómadas* y especialmente bien pensadas para la experimentación colectiva de utopías presentes, «aquí y ahora». Es la base de su teoría sobre la TAZ o *Zona Temporalmente Autónoma*[19]. Las utopías piratas son las primeras referencias históricas de las que disponemos para imaginarnos una TAZ:

> *Los contrabandistas y corsarios del siglo XVIII crearon una red de información que abarcaba el mundo entero: primitiva y entregada fundamentalmente a siniestros menesteres, la red funcionaba en todo caso de manera portentosa. Diseminadas a lo ancho de la red había islas, remotos escondites donde las naves podían ser aprovisionadas de agua y víveres o usadas como botín a cambio de lujos y necesidades. Algunas de estas islas sostenían «comunidades liberadas», completas sociedades en miniatura viviendo conscientemente al margen de la ley con la determinación de mantenerse, aunque sólo fuera por una corta pero venturosa vida.*[20]

19. Bey, H (1994) *T.A.Z. Zona Temporalmente Autónoma*. Talasa Ediciones, Madrid.
20. Bey, H (1994).

COSAS QUE HAY QUE HACER PARA SER RESPETADO POR LOS HACKERS

Básicamente hay cinco clases de cosas que puede hacer para ser respetado por los hackers:

1.º Escriba software libre. **Lo primero (lo más central y más tradicional) es escribir programas que otros hackers piensen son divertidos o útiles, y dar las fuentes del programa para que los use toda la cultura hacker. Los más reverenciados semidioses del hackerismo son las personas que han escrito programas grandes y capaces que satisfacen una necesidad general, y los han liberado, de modo que ahora todos los utilizan.**

2.º Ayude a probar y depurar software libre. **También reciben reconocimiento aquellas personas que depuran errores en el software libre. En este mundo imperfecto, inevitablemente pasaremos la mayor parte de nuestro tiempo de desarrollo en la fase de depuración. Éste es el motivo por el**

La «piratería informática», si pensamos en ella como en las múltiples experiencias de resistencia política y contracultural que hay en Internet, también se puede entender como una red y archipiélago de islas interconectadas, conjunto de «zonas liberadas». Para Bey, la tecnología de los noventa hacía posible el *dominio total* de manera que pensar en zonas del mapa fuera de control implicaba moverte en el plano de las utopías inalcanzables. «*Hay que construir nuevos mapas*» sobre el desarrollo de un nuevo tipo de tecnología liberadora con la que es posible la *desaparición* y la *autonomía* respecto del Estado. «¿Debemos quizá esperar a que el mundo entero haya sido liberado de todo control político antes de que incluso uno de nosotros pueda afirmar conocer la libertad?»[21]. La historia cuenta con la experiencia de «enclaves libres» y utopías que no sólo han sido posibles: son posibles, de hecho existen y nos permiten hablar de libertad aquí y ahora, sin nostalgias ni metarrelatos sobre el progreso (Marx) y su sistemático empeño por desplazar las utopías liberadoras siempre hacia adelante.

Así, la TAZ es una línea de fuga, un plano diferente al de la confrontación revolucionaria a vida o muerte. «La TAZ es una forma de sublevación que no atenta directamente contra el Estado, una operación de guerrilla que libera un área (de tierra, de tiempo, de imaginación) y se disuelve para reconfigurarse en otro sitio/otro momento, antes de que el Estado pueda aplastarla»[22]. Es «la mejor de las tácticas posibles» en un momento de omnipresencia física, política y técnica del Estado, al que la TAZ puede habitar en sus fisuras, en sus grietas o en sus propias redes de datos. La TAZ «golpea y se defiende» rehuyendo el enfrentamiento directo, la violencia; se hace inalcanzable en la invisibilidad y el movimiento continuo. De ahí que en la TAZ se pueda representar un mapa de escala 1:1 fuera del mapa del imperio, fuera del mapa real. Es decir, sólo la TAZ puede inventarse otra realidad fuera de la que ya está definida por el mapa del poder y en la que no hay territorio sin dominar. Se trataría de encontrar espacios geográficos, sociales, culturales o ima-

21. Bey, H (1994).
22. Bey, H (1994).

que cualquier desarrollador de software libre inteligente le dirá que los buenos evaluadores de versiones beta (los que saben cómo describir claramente los síntomas, pueden localizar correctamente los problemas, pueden tolerar errores en una versión apresurada y están dispuestos a aplicar unas cuantas rutinas sencillas de diagnóstico) valen su peso en rubíes. Uno solo de estos evaluadores puede suponer la diferencia de que la fase de depuración sea una prolongada y agotadora pesadilla, o sólo una saludable molestia.

Si usted es novato, trate de encontrar un programa en desarrollo en el que esté interesado, y sea un buen evaluador de versiones beta. Hay una progresión natural desde ayudar a probar programas, a ayudar a depurarlos, y después ayudar a modificarlos. Aprenderá un montón de esta manera, y generará buen karma con gente que le ayudará más adelante.

ginarios y se trata también de encontrar *tiempos* en los que este nuevo espacio se haga proyecto de vida, en el olvido del Estado y de los cartógrafos de la realidad:

> *Estos nómadas orientan su curso bajo estrellas extrañas, quizás luminosos racimos de datos en el ciberespacio, o quizás alucinaciones. Extiende un mapa del terreno; coloca sobre éste un mapa del cambio político; sobre éste un mapa de la red, especialmente de la contra-red con su énfasis en logística y el flujo de información clandestina; y finalmente, encima de todo, el mapa 1:1 de la imaginación creadora, de la estética, de los valores. La trama resultante cobra vida, animada por remolinos y brotes de energía, coágulos de luz, túneles secretos, sorpresas.*[23]

Dentro de la red del comercio y el ejército hay zonas de acceso público y otras de acceso restringido. En ese espacio público se ha creado una *contra-red* de usos clandestinos e ilegales, de rebeldía y piratería. La *contra-red* se levanta sobre una *trama* o estructura horizontal, no jerárquica y orientada al intercambio de datos. La TAZ puede ubicarse también en *la trama* y existir tanto en el mundo real como en el virtual. Para Bey, la capacidad de «comprimir tiempo y espacio» de los medios digitales y las redes telemáticas puede proporcionar a la TAZ algún «sustituto» del tiempo y espacio, al que renuncia en el mundo material y en el que es posible una nueva vida invisible para el Estado. La *trama* suministra la épica a la TAZ, es su fuente de *mitopoiesis*: almacena información secreta y clave, sus leyendas, su ideario y sus sueños. La contra-red es imposible de cerrar, controlar o congelar[24].

23. Bey, H (1994).
24. La influencia de Bey en las redes activistas es fuerte. Margarita Padilla, fundadora de Sindominio, escribe claramente influenciada por la idea de la TAZ: «Persiguiendo eliminar las mediaciones y experimentar la inmediatez, la propuesta ya no será construir la red, sino parasitaria a la manera de virus. [...] construyendo la red secreta, la antirred de la guerrilla que golpea y corre. Sabiendo que la mayor fuerza reside en la invisibilidad, construirá una minisociedad underground al margen de la ley, una subred de transgresiones que mostrará la arbitrariedad de los límites y que la red oficial nunca conseguirá clausurar». Padilla, M : «Agujeros negros en la red», *Archipiélago*, nº 53, 2002, noviembre, págs. 25-29. Todo el texto suena a TAZ y aparece prácticamente de manera literal en Bey (1994).

3.º Publique información útil. **Otra buena cosa que puede hacer es recopilar y filtrar información útil e interesante, y construir páginas web o documentos de tipo Preguntas Más Frecuentes (P+F, o FAQ en inglés) y ponerlos a disposición de los demás. La gente que mantiene las P+F técnicas más importantes goza de casi tanto respeto como los autores de software libre.**

4.º Ayude a mantener en funcionamiento la infraestructura. **La cultura hacker (y el desarrollo ingenieril de la Internet, para el caso) es llevada por voluntarios. Hay un montón de trabajo *necesario pero* sin glamour que ha de ser realizado para mantenerla en funcionamiento: administrar listas de correo, moderar grupos de discusión, mantener sitios donde se archivan grandes cantidades de software, desarrollar RFCs y otros estándares técnicos.**

La gente que hace bien este tipo de cosas goza de mucho respeto, porque todos saben que

Entre el mundo apocalíptico del *ciberespacio* de Gibson, dominado por la violencia y el control total que consigue la fusión de las inteligencias artificiales, las excitantes utopías autónomas de Hakim Bey representan un salto hacia adelante. La TAZ es una redimensión de lo adelantado por Gibson y una humanización, por politizada, del concepto. En Bey el ciberespacio se recupera para la vida en tanto que proyecto colectivo, libre e independiente del poder. De la misma manera que cuando el mapa del globo aún no había sido cerrado, Hakim Bey ve en 1990 que la redes telemáticas abren una nueva dimensión espacial para el hombre en las que es perfectamente aceptable trasladarnos con los elementos que necesitamos para emprender proyectos en nuestra vida material: la identidad, la voluntad, el espíritu de comunidad y la necesidad de autonomía y libertad. Con independencia de cuánto pueda haber aportado el trabajo de Bey a la teoría política[25], nos interesa como fuente, como texto de referencia y dinamizador de buena parte del activismo telemático. Y lo hace por cuanto que Bey aporta, a lo que comienza a configurarse como *comunidades de hackers activistas* en algunos espacios de la Red, la reflexión política (la naturaleza del poder y la necesidad de liberación) que descongela la fascinación «neutra» por la tecnología y la ficción ciberpunk que le da salida por vía literaria[26].

25. «Los secretos revelados —como los misteriosos divinos— suelen ser frecuente fuente de errores políticos consecutivos. Los exegetas no son tan diferentes de los thélèmitas. La religiosidad se afana en encontrar constantemente nuevos actos de fe que provean mártires, y con ello, nuevos modelos. Igualmente los poetas épicos seculares han recurrido desde siempre a la elucubración de paraisos miticos y primitivos donde instalarse a voluntad. Uno de esos lugares ha sido el (¿recientemente?) territorio de la filosofia politica; desde donde se han soñado utopias (piratas, obreras, nacionales, sexuales, raciales) que sirvieron de musa a la lirica. Se puede recordar el Robinson de Stevenson [sic.] que inauguró el gènero burguès del escapismo, tan lùcidamente comentado por Marx. O la Alemania de Rilke —aquella que se antesoñó imperio de elfos noldos— que se mecia bajo las miradas romànticas. Desde Stevenson a Sterling el genero apenas ha sufrido las mutaciones propias del espiritu de su tiempo. Las comunas ciberpunkies de la ciencia-ficciòn nos recuerdan sobremanera a aquellas tribus aisladas con sociedades antagónicas a las nuestras, o a los falansterios de Fourier, Owen... Toda la literatura de Julio Verne no desmerecia colocarse a la cabeza del pensamiento de H. Bey, inserto en la abadia de Thèleme soñada por Rabelais, donde Gargantúa ordena: «Haz lo que quieras». Mob, K . (?) «Fundamentos para una crìtica del Taz de Hakim Bey». *La Haine*, http://www.lahaine.org/pensamiento/fundamentos_bey.htm (visitada por última vez el 29-06-04).

26. Para matizar esta apreciación podriamos leer *Zona Libre*, un relato de John Shirley: radicalismo politico, ciberpunk y ciencia ficción en cuarenta páginas. Shirley, J: «Zona Libre», en Sterling, B. (1998) *Mirrorshades. Una antologia ciberpunk*. Siruela ed., Madrid.

estos trabajos son grandes consumidores de tiempo y no tan divertidos como jugar con el código. Hacerlos demuestra dedicación.

5.º Haga algo por la propia cultura hacker. **Finalmente, puede serle útil a la cultura hacker en sí misma y propagarla (por ejemplo, escribiendo una buena introducción de cómo llegar a ser hacker). Esto es algo que no estará en posición de hacer hasta que haya estado durante un tiempo en el mundillo y se haya vuelto bien conocido por una de las cuatro cosas anteriores.**

La cultura hacker no tiene líderes, exactamente, pero tiene héroes culturales, ancianos de la tribu, historiadores y portavoces. Cuando haya estado en las trincheras el tiempo suficiente, podrá llegar a ser uno de ellos. Pero tenga cuidado: los hackers desconfían de un ego estridente en sus ancianos de la tribu, así que buscar visiblemente esta clase de fama es peligroso. En lugar

Tecnología: ¿dominio o liberación?

«Bajo el gobierno de una totalidad represiva, la libertad se puede convertir en un poderoso instrumento de dominación.»
Marcuse, *El hombre unidimensional*

La racionalidad científica permite la captura de la realidad objetiva recurriendo a operaciones intelectuales que la representan mediante algoritmos matemáticos, mediante construcciones mentales que hoy en día se encuentran bajo el dominio de la lógica binaria y la representación digital. Lo real es ahora una mera representación o mediación entre el sujeto y sus construcciones (mentales) lógico-matemáticas; se evapora del mundo objetivo, se desmaterializa en complejas fórmulas y conceptos que hacen pertinente afirmar que «la realidad científica parece ser una realidad ideacional»[27]. Se entiende, pues, que la lógica científica colocada en la base de la relación del hombre y la naturaleza permite una recreación imaginaria de lo real: la realidad ya no sólo es manipulable técnicamente en su materialidad, sino, sobre todo, definida en un proceso social de comunicación en tanto que dato procesado: *hoy lo real es información*.

Si estiramos hasta el límite esta conclusión (crítica) de Marcuse y la solapamos con la reivindicación de la interacción comunicativa de Habermas[28], en un contexto en el que el desarrollo científico-técnico ha desbordado su condición de capital productivo y se desplaza al ámbito de relación social práctica (acción política) y comunicación de masas, quizá podamos reconstruir una crítica a la racionalidad técnico-científica en la que liberemos un espacio para el desarrollo de esa otra premisa que adelantaba Marcuse y la Escuela de Frankfurt: la que define a la tecnología como un elemento integrado en una lógica de dominio, al mismo tiempo que se ofrece como condición de posibilidad de toda estrategia de liberación[29]. Situemos el

27. Marcuse, H. (1994) *El Hombre unidimensional.* Ariel, Barcelona.
28. Habermas, J. «La ciencia y la tecnología como ideología», en Barnes, B. (1980) *Estudios sobre sociología de la ciencia.* Alianza, Madrid.
29. Marcuse, H. (1994).

de afanarse por ella, tiene que ponerse en posición de que caiga sobre usted, y después llevar con modestia y elegancia su estatus.

trabajo de ambos en los años sesenta y la necesidad de remozar el marco conceptual de análisis del modo de producción. Efectivamente, las tecnologías productivistas difícilmente podrían ser percibidas como algo más que un mecanismo de integración física del hombre a la cadena de montaje y la producción masiva de mercancías. Cuarenta años después, el despliegue técnico y el diseño productivo se han desarticulado (o rearticulado) en un proceso de descentralización fabril, de mecanización y automatización que, como resultado final, ha expulsado al hombre de la cadena de montaje y de buena parte del proceso productivo[30]. La fuerza humana entendida como presencia física en el proceso productivo se sustituye por inteligencia digitalizada, por procesos de dirección y administración de sistemas y por «nuevas» relaciones de producción que podrían entenderse como *neodecimonónicas*, y que van desde la precariedad del trabajo en las metrópolis occidentales a la esclavitud en la periferia de la opulencia desarrollada. Los microchips de los robots de la Renault pueden perfectamente ser manipulados por niños esclavos en Nueva Delhi, y las mascarillas antiestáticas de los ingenieros de hardware en Silicon Valley pueden ser cosidas a mano por mujeres de las maquilas de México. Ese desequilibrio y desarrollo desigual (esa combinación de tecnología de última generación y trabajo manufacturado) es la base de la coherencia y estabilidad del capitalismo del siglo XXI. El desarrollo técnico-científico de los últimos quince años ha centrado su ámbito de dominio preferente en las tecnologías de la comunicación para dar salida, por un parte, a las imposiciones funcionales y operativas de la producción mercantil, del complejo militar-industrial, y a la necesidad de un nuevo espacio de socialización para el consumo y la asimilación política. *Así, la comunicación pasa a integrarse en el dispositivo ideológico de control social en la misma medida que se convierte de inmediato en el terreno propicio para la resistencia al poder, para la lucha y el desarrollo de dispositivos ideológicos movilizados en clave de liberación*. Mientras que la

30. Uno de los relatos ya clásico sobre el nuevo mundo globalizado y las mutaciones del modo de producción capitalista: Hardt, M. y Negri, T. (2002) *Imperio*. Paidós ed., Barcelona.

maquinaria automatizada y organizada en cadena de montaje, en la que se devora al hombre y su mundo como un elemento productivo más, es irrecuperable para la revolución y sólo se representa en el imaginario insurgente como herramienta de explotación a la que se debe atacar hasta desmontarla[31] (aun a costa de romper con las premisas productivistas del progresismo marxista del XIX), la técnica digital comunicativa se despega de la materialidad de la producción y se hace accesible, autónoma y recuperable para la organización de la protesta, para la liberación subversiva. ¿Podría ser éste un punto de partida para una redimensión política del potencial disruptivo de la tecnología aplicada a la comunicación? La práctica del hacking (mucho más claramente que su discurso) aporta algo en esta dirección.

La práctica del hacking: Metabolik BioHacklab de Bilbao[32]

«Yo creo que casi todo hacker de dentro del movimiento de hacklabs es multimilitante.»
Zert en *#Metabolik*

Hoy en día existen varios *hacklabs*, o laboratorios de experimentación técnica y social que nacen de esta nueva cultura *hacktivista* y la consolidan como movimiento social articulado dentro y fuera de la red. Se reúnen físicamente fuera de Internet con la intención de trabajar en proyectos relacionados con el software libre, ciberderechos, privacidad, criptografía, redes wireles[33] en barrios o ciudades; fuera de su territorio convencional (la Red, que sigue siendo un espacio para la coordinación), *bajando a tierra* en contacto directo con las redes sociales.[34] La mayoría utiliza, nace o se inserta en Centros Sociales Okupados como fue el caso de Kernel Panic de Barcelona, que se reunía en el Centro Social Les Naus. Enseñar, aprender, montar redes, compartir conocimiento y sobre todo difundir una imagen del hacking como cultura de la información libre.[35]

31. «La conexión autovalorización/sabotaje, así como su recíproca, no nos permite insertarnos en el "socialismo", en su tradición, ni mucho menos en el reformismo o en el eurocomunismo. Hablando en broma, podríamos decir que formamos parte de otra raza. No tenemos nada que ver con el inconsistente proyecto del reformismo, con su tradición, con sus infames ilusiones. Estamos en el interior de una materialidad que tiene sus propias leyes, ya descubiertas o por encontrar en la lucha, pero que en todo caso, son otras. El "nuevo modo de exposición" de Marx se ha convertido en un nuevo modo de existencia de clase. Estamos aquí, inamovibles, mayoritarios. Tenemos un método de destrucción del trabajo. Tendemos a buscar una medida positiva del no trabajo. Una liberación de la asquerosa esclavitud que hace regocijarse a los patronos, que el movimiento oficial del socialismo nos ha impuesto siempre como signo de nobleza». Negri, A. (1979) *Dominio y Sabotaje*. El Viejo Topo, Barcelona (edición digital http://www.ucm.es/info/eurotheo/negri-dominio.htm, visitada por última vez el 25-04-04).
32. Todos los enlaces de este apartado relacionados con el Metabolik BioHacklab fueron consultados en el año 2003. El análisis de su web se hizo durante ese año y no refleja las actividades que puedan haberse incorporado con posterioridad, como por ejemplo el desarrollo de la distribución de Linux, X-evian. Ver http://www.x-evian.org.
33. Redes de comunicaciones inalámbricas. Ver, por ejemplo, Bilbo Wireless (http://bilbowireless.net/) o Lavapiés Wireless (http://lavapieswireless.net/).
34. «Si buscas un sitio donde la tecnología no se quede en el mero nivel técnico, sino que busca la aplicación social necesaria y constructiva, si necesitas un lugar para demostrar que sabes más cosas aparte de leer hexadecimal y programar muy bien, o si te gusta la cerveza, este es tu sitio. Somos un grupo muy variado de hombres y mujeres de 15 a 40 años. No tenemos ninguna clase de discriminación por edades, razas, sexo, gustos o creencias. (Incluso aceptamos usuarios de Windows). Cualquiera que se sienta identificado con lo que somos y hacemos será bienvenido. No es necesario tener ninguna clase de preparación técnica, pero sí que te guste compartir el conocimiento». FAQs: http://www.hacklabs.org/wiki/wiki.pl?FaQs.
35. «El conocimiento es poder, cualquier cosa que puedas aprender sobre redes, ordenadores y sistemas lógicos en general, te ayudará a comprender mejor nuestro mundo real. No toleramos el uso del conocimiento para el control social de ninguna manera. La información tiene que ser libre y sin fronteras ni censuras». Presentación: http://sindominio.net/kernelpanic/index2.php.

En el Gaztetxe de Udondo (Leioa), en Bilbao, se reúne como un grupo de trabajo del Centro Social, el Metabolik Bio Hacklab. Éste nace en el *hackmeeting*[36] de septiembre de 2001 y en su primer año despliega una actividad en diversos frentes. Se presenta a través de un *manifiesto rizomático*[37], en conexión evidente con la vanguardia posmoderna que nace años antes en algunos sectores del movimiento de okupación de Madrid y Barcelona, empeñados en la asimilación colectiva de algunos textos de Deleuze y Guattari como base sobre la que superar el «estrecho horizonte de la vieja izquierda» y poder dar forma a un nuevo discurso alejado de las «representaciones binarias» de lo social[38]:

> *Me gusta ser libre, expandir mi código, compartirlo, difundirlo, copiarlo, enlazarme con otras páginas, otros proyectos, otros seres... disfruto al experimentar con diversos lenguajes y protocolos, aprender y ser aprendido, participar de los procesos tecnológicos y humanos que me constituyen, interactuar con mis entornos a través de mis diversos cuerpos para defender la autoorganización y la autonomía que me da la vida. Por eso uno de mis fundamentos autocatalíticos primarios (quizás es el más importante) es el* [software libre], [generarlo], *usarlo, difundirlo y disfrutarlo me permite compartir técnicas y materiales, conocimientos y prácticas, y crear así una fuente común de recursos colectivos, colaborar con una red autoorganizativa de conocimientos abiertos, libres y reutilizables que me alimentan, mientras alimentan a otras.*[39]

El colectivo se suma en breve a las campañas contra la LSSI («No queremos vivir así»[40]), a la Campaña SOS Privacidad («STOP 1984»[41]), a la difusión del software libre («Nosotros hablamos de Software Libre»[42]) y a la campaña contra las patentes de software de Proinnova («No a las patentes de software»[43]). Pone en marcha

36. Un hackmeeting es un encuentro anual de hackers de los diferentes proyectos activistas del estado. Empiezan a organizarse en Italia hace cinco años y se consolidan en España fundamentalmente en torno a hacklabs, Centros Sociales Okupados y nodos locales de Indymedia. Las diferentes webs sobre los hackmeetings de los últimos años son accesibles desde http://www.hacklabs.org.
37. «Para Deleuze y Guattari, existen tres tipos de libro: el libro-árbol, que seguiría una lógica binaria; el sistema raicilla, de raíces múltiples, y el libro-rizoma, constituido por mesetas [fragmentos] autónomas, comunicadas por "microfisuras". En este libro-rizoma cada fragmento puede leerse por cualquier sitio y ponerse en relación con cualquier otro: un libro así, según Deleuze y Guattari, "se niega al logos, a la trascendencia de la idea, a la interioridad del concepto, al tribunal de la razón, a los funcionarios del pensamiento, al sujeto legislador"». *Rizoma*: http://sindominio.net/metabolik/wiki/index.pl?RiZoma.
38. «Mil Mesetas es el desierto que queremos recorrer, tal vez para salir de él, pero pasando por él, por las mesetas que la multiplicidad Deleuze-Guattari supieron dibujar. Y es por ello que necesitamos de vuestras cartografías y vuestros aullidos que bajo el título de ponencia sepan escapar a la *forma masa. Laboratorio de nomadología*, pues, para tod@s l@s que huyendo buscan un arma, laboratorio que quisiera ser un espacio de experimentación, de composiciones contranatura, devenir-lobos, esto es, andar por el desierto acompañad@s. Que vuestras ponencias sean armas o tal vez aún herramientas, que el laboratorio sea tal mera sala de autopsias dependerá de la vida que seamos capaces de poner en juego, de la lobitud que seamos capaces de crear». *Entre Mil Mesetas, trayectos, travesías, tropiezos, I er. laboratorio de nomadología*. Barcelona, 7, 8 y 9 de octubre de 1997, Facultat de Filosofia de la UB, CSO Hamsa. http://www.sindominio.net/laboratorio/documentos/milmesetas/home.htm.
39. Manifiesto Metabolik. http://www.sindominio.net/metabolik/wiki/index.pl?*ManifiestoMetabolik*..
40. http://www.ugr.es/~aquiran/cripto/tc-lssi.htm.
41. http://www.stop1984.com.
42. http://www.fsfeurope.org/documents/whyfs.es.html.
43. http://proinnova.hispalinux.es/.

talleres sobre la LSSI, programación en Perl, PHP[44], introducción al software libre, electrónica e introducción a GNU/Linux. En marzo del 2003 organiza unas Jornadas sobre Wireless y Redes Ciudadanas Libres junto a BilboWireless y MadridWireless[45].

En febrero del mismo año el colectivo decide dar respuesta desde una posición de crítica social a la tecnología y su modelo dominante, el modelo de la globalización capitalista, del mercado y de las corporaciones transnacionales. La ocasión se la brinda el Congreso Internacional sobre la Sociedad de la Información IT4ALL, que se celebra en Bilbao del 5 al 7 de febrero[46]. Promovido por el Gobierno vasco en el marco de programas europeos, cuenta con el apoyo y la participación de la SGAE, la CNN, el BBVA, Petronor, Grupo ITP, Hewlet Packard y Microsoft[47]. Un contramodelo que se levanta sobre claras dinámicas mercantiles y militaristas relacionadas con el cambio tecnológico, un contramodelo de la visión cooperativa, social y anticapitalista de los hacktivistas de Leioa. Frente a estos «*señores del aire*» los hackers recurren a la agitación, la denuncia y la acción directa, repertorio de acción compartido con otros movimientos. Su manifiesto denuncia:

> *La brecha digital la construyen día a día quienes patentan tecnologías de la comunicación, quienes monopolizan el software, quienes no respetan lo estándares consensuados, quienes exigen continuamente la renovación de máquinas útiles, quienes hacen de la tecnología un instrumento para la guerra, quienes comercializan con el saber, quienes esclavizan a sus clientes, quienes privatizan longitudes de onda, quienes prohíben compartir información, quienes crean leyes que favorecen los monopolios, quienes invierten en una educación hacia productos tecnológicos esclavizantes. Y, por supuesto, la brecha digital es la brecha del pan, la brecha de la pobreza. Una sociedad más tecnologizada con la tecnología de los señores del aire (cerrada, esclavizante, secreta, de mala calidad...), una sociedad informada por los señores del aire, una sociedad educada para consumir sus productos, no es una sociedad ni más avanzada, ni más informada, ni más comunicada, ni más libre.*[48]

Esta carta se hace pública como parte de la campaña Money4them[49] que incluye acceso a los media convencionales[50], a los media independientes[51] y acciones de calle frente al Palacio de Congresos[52], reclamando otro modelo de comu-

44. Lenguajes de programación interpretados (no necesitan ser compilados para poder ejecutar su código), orientados al desarrollo de aplicaciones web. En Perl se ha escrito el código de algunos Indymedias y con PHP infinidad de aplicaciones orientadas a la comunicación y el trabajo en grupo en la red: SPIP, Wiki's, Nukes, foros entre otros.
45. Agenda del 2002, http://www.sindominio.net/metabolik/wiki/index.pl?AgendaDel2002; agenda del 2003, http://www.sindominio.net/metabolik/wiki/index.pl?AgendaDel2003.
46. http://www.bilbaoit4all.com/castellano/home_cast.html.
47. http://www.bilbaoit4all.com/castellano/patrocinio/patrocinio.html.
48. *Carta abierta a los señores del aire*, http://www.sindominio.net/metabolik/carta/money4them.txt.
49. http://www.sindominio.net/metabolik/it4all_money4them.html.
50. Comunicado de Prensa: http://www.sindominio.net/metabolik/com.pdf..
51. Noticia en Euskalherria Indymedia, http://www.euskalherria.indymedia.org/eu/2003/02/3975.shtml.
52. Acción Directa Telemática Frente al Euskalduna, 6 de Febrero 2003 - Congreso it4all, Bilbao, Bizkaia: http://www.sindominio.net/metabolik/adt/#::_it4all__money4them_::

nicación posible basado en la creación de redes ciudadanas independientes, la difusión de herramientas basadas en software libre, la expansión de los hacklabs como centros de experimentación de base, el desarrollo de medias independientes y servidores de Internet organizados desde la autogestión de los recursos técnicos[53].*

53. «Desde la brecha digital queremos recordar a los señores del aire [...] que llevamos mucho tiempo construyendo puentes:
    1. Creando redes metropolitanas libres: de conectividad libre y gratuita, donde la conexión se puede hacer a través de una antena hecha con una lata de patatas fritas y con una velocidad de hasta 11Mb/s. http://www.bilbowireless.com
    2. Creando, difundiendo y educando en software libre: en tecnologías colectiva y libremente construidas, cuyo código fuente es accesible a tod*s, donde no hay que pagar por compartir, adaptadas a todo tipo de hardware, también al reciclado, al obsoleto para microSoft pero perfectamente útil para cualquiera. http://www.gnu.org http://www.debian.org
    3. Creando espacios de conectividad, de experimentación, laboratorios tecnológicos libres y participativos. http://www.hacklabs.org http://www.sindominio.net/metabolik
    4. Creando medios de comunicación horizontales, donde la participación es libre y respetada, donde cabe contrastar y comentar las noticias, donde no hay división entre informante e informado, entre sujeto y narrador de la noticia. http://www.indymedia.org http://euskalherria.indymedia.org
    5. Creando servidores libres, experimentos de inteligencia colectiva asamblearia, de gestión horizontal de recursos tecnológicos y telemáticos, rompiendo la división entre prestador de servicios y cliente.»
    http://www.sindominio.net.» *Carta abierta a los señores del aire*,
    http://www.sindominio.net/metabolik/carta/money4them.txt.

* Para hacer más ágil la lectura y por darle un orden lógico a los contenidos de este apartado, la segunda parte de este artículo, «Los discursos del hacking», se ha puesto a continuación del artículo «Hacklabs, hackmeetings».

Bibliografía

BARANDIARÁN, X. (2003) *Activismo digital y telemático. Poder y contrapoder en el ciberespacio* v.1.1. http://www.sindominio.net/~xabier/textos/adt/adt.html.

— (2003) *Hacklabs: tecnologías y redes de ensamblado colectivo de autonomía digital* v.0.9. http://www.sindominio.net/~xabier/textos/hl/hl.html.

BEY, H (1994) *T.A.Z. Zona Temporalmente Autónoma*. Talasa Ediciones, Madrid.

BOLLIER, D. (2003) «*El redescubrimiento del procomún*». Biblioweb, http://www.sindominio.net/biblioweb/telematica/bollier.html.

CONTRERAS, P. (2004) *Me llamo Kohfam. Identidad hacker: una aproximación antropológica*. Gedisa ed., Barcelona.

FOUCAULT, M. (1996) *Tecnologías del yo y otros textos afines*. Paidós, Barcelona

GARCÍA, J. y ROMEO, A. (2003) *La pastilla roja. Software libre y revolución digital*. EditLin ed., Madrid.

GIBSON, W. (1989) *El Neuromante*. Minotauro, Barcelona.

— (1994) *Quemando cromo*. Minotauro, Barcelona.

GORDON CHILDE, V. (1985) *Nacimiento de las civilizaciones orientales*. Ediciones Península. Barcelona.

HABERMAS, J. (1980) «La ciencia y la tecnología como ideología«, en Barnes, B.: *Estudios sobre sociología de la ciencia*. Alianza, Madrid.

HARDT, M. y NEGRI, T. (2002) *Imperio*. Paidós ed., Barcelona.

HARRIS, M (1989) *Introducción a la antropología general*. Alianza, Madrid.

KLIMA, J. (1983) *Sociedad y Cultura en la Antigua Mesopotamia*. Akal Universitaria, Madrid.

KOVALIOV, S. I. (1979) *Historia de Roma*. Akal Textos, Madrid.

LEVY, S. (2002) Cripto. *Cómo los informáticos libertarios vencieron al gobierno y salvaron la intimidad en la era digital*. Alianza ed., Madrid.

MARCUSE, H. (1994) *El hombre unidimensional*. Ariel, Barcelona.

MOB, K . (?) «Fundamentos para una crítica del Taz de Hakim Bey». *La Haine*, http://www.lahaine.org/pensamiento/fundamentos_bey.htm.

MOLIST, M. (?) *Hakim Bey: adiós a la red*. http://ww2.grn.es/merce/hakim.html.

NEGRI, A. (1979) *Dominio y Sabotaje*. El Viejo Topo, Barcelona (edición digital http://www.ucm.es/info/eurotheo/negri-dominio.htm, visitada por última vez el 25-04-04).

PADILLA, M : «Agujeros negros en la red», *Archipiélago*, nº 53, 2002, noviembre, págs. 25-29.

RAYMON, E. (2000) «Breve historia de la cultura hacker». *Biblioweb*, http://www.sindominio.net/biblioweb/telematica/historia-cultura-hacker.html.

ROIG, G. y SÁDABA, I. (2003) «Internet, nuevos escenarios, nuevos sujetos, nuevos conflictos», en Aparici, R. y Marí, V.: *Cultura popular, industrias culturales y ciberespacio*. UNED, Madrid.

— (2004) «El movimiento de okupación ante las nuevas tecnologías. Okupas en las redes», en ADELL, R. y MARTÍNEZ, M.: *¿Dónde están las llaves? El movimiento okupa, prácticas y contextos sociales*. Libros de la Catarata, Madrid.

SHIRLEY, J. (1998) «Zona Libre», en Sterling, B.: Mirrorshades. *Una antología ciberpunk*. Siruela ed., Madrid.

STERLING, B. (1994) *The hacker crackdown*. http://www.bufetalmeida.com/textos/hackercrack/libro.html.

WILLIAMS, R. (2004) *Cultura y cambio tecnológico: el MIT*. Alianza ed., Madrid.

HACKLABS, HACKMEETINGS

Xabier Barandiaran
(Metabolik BioHacklab,
laboratorio hacker de Bilbao)*

«Para mí tanto los hackmeetings como los hacklabs representan una interesantísima y fructífera tensión-interacción entre lo social, lo tecnológico y lo político y nacieron con la idea de integrar y contaminar mutuamente a gente de estos campos y aprovechar las sinergias específicas de cada uno, guardando un equilibrio inestable necesario para hacer surgir lo mejor de cada uno. En el interno interrogante de quienes somos y hacia donde vamos, esta tensión se manifiesta de forma constante y nos obliga a estar repensando y revisando continuamente nuestras posiciones.»
Azalai[1]

HACKLABS.ORG: DADME UN LABORATORIO Y MOVERÉ EL MUNDO

«En los estudios de laboratorio, no sólo se encontrará la clave para una comprensión sociológica de la ciencia; sino también, creo, la clave para una comprensión sociológica de la sociedad misma, porque es en los laboratorios donde se genera la mayor parte de las nuevas fuentes de poder.»
Bruno Latour

Si entendemos por laboratorio el espacio en el que se generan códigos y se construyen máquinas no es difícil comprender, desde una perspectiva tecnopolítica, cómo el laboratorio se convierte en fuente de poder. En un artículo que lleva por título «Dadme un laboratorio y moveré el mundo»[2] el sociólogo de la ciencia Bruno Latour analiza cómo el estudio de laboratorio borra los límites entre las macro y microestructuras sociales, dentro y fuera de las prácticas tecnocientíficas, ya que lo que se produce en los laboratorios (nivel micro) puede llegar a alterar las condiciones y relaciones sociales (nivel macro) y viceversa. Si bien el análisis de Latour se centra en el laboratorio de Pasteur y la forma en la que el descubrimiento de los microbios y las vacunas transformó las prácticas y

* Este texto es un extracto y modificación de Barandiaran, X. (2004) *Hacklabs*, que puede consultarse en: http://sindominio.net/~xabier/textos/hl/

1. Extracto de un mensaje enviado a la lista de correo hackmeeting@sindominio.net.
2. Latour, B.: «Give Me a Laboratory and I will Raise the World», en K. Knorr-Cetina y M. Mulkay (eds.) (1983) *Science Observed: Perspectives on the Social Study of Science. Sage*, Londres, pp. 141-170. Versión en castellano traducida por Marta I. González García en: http://www.campus-oei.org/salactsi/latour.htm

MANUAL DE INSTRUCCIONES PARA EJECUTIVOS

CÓMO CREAR Y HACER FUNCIONAR UN HACKLAB

Como todo buen manual éste presenta un fácil y sencillo algoritmo con el que ustedes podrán crear un hacklab en apenas un par de semanas, sin inversiones considerables, sin esfuerzo y con la garantía del Ministerio de Ciencia y Tecnología.

Sigan detenidamente las instrucciones de este manual, un algoritmo en siete pasos adaptado a todas las edades, sin discriminación de raza, sexo, religión, orientación sexual o minusvalías políticas. Al final de la ejecución del algoritmo les aseguramos que ustedes se sentirán aliviados, con la con-

estructuras sociales encaminadas a proteger la salud pública y la ganadería (extendiendo el laboratorio y sus resultados al entorno social e introduciendo las problemáticas sociales —epidemiológicas— en el laboratorio), sus conclusiones se amplifican en el espacio de los laboratorios de tecnologías de la información y las comunicaciones (TIC).

Al margen de los grandes centros de investigación académicos y corporativos, el laboratorio por antonomasia de las TIC es la red, con los múltiples procesos de experimentación y producción desencadenados por el movimiento de software libre y la cultura hacker. Los hacklabs (o laboratorios hacker) no pretenden sustituir a la red en esos procesos de experimentación, sino insertarse en ellos asumiendo explícitamente el carácter de laboratorios tecnopolíticos locales, materiales y socialmente situados y que, por tanto, pueden atravesar límites que la red (por su virtualidad y deslocalización) no puede.

Los hacklab comenzaron a finales de los noventa en Italia y, hoy en día, hay más de treinta repartidos por Italia, España, Francia, Londres y Latinoamérica. Generalmente situados en Centros Sociales Okupados y Autogestionados (CSOA) ,los hacklab son espacios autónomos de experimentación, difusión y politización de las tecnologías. Para entender el sentido de los hacklabs proponemos un análisis en tres movimientos: a) el que va de la sociedad al laboratorio, b) el que se produce dentro del laboratorio y c) el que va del laboratorio a la sociedad.

De la sociedad al laboratorio

En cuanto a contenidos, en el movimiento que va de la sociedad al laboratorio, el hacklab recoge problemáticas sociales y las introduce en el universo experimental y productivo hacker como objetos y objetivos del propio laboratorio. Estas problemáticas van desde la necesidad de hacer frente a un desarrollismo tecnomercantilista (que fuerza a las personas a depender constantemente de las nuevas actualizaciones tecnológicas que salen al mercado) a las necesidades telemáticas de coordinación y comunicación de diversos movimientos sociales (el movi-

ciencia social bien tranquila, situados en la vanguardia de la política tecnológica y orgullosos de pertenecer a la gran franquicia Hacklabs (TM).

1. Dispongan ustedes de un espacio autogestionado, libre de intereses externos y de dependencias económicas. Preferiblemente un espacio okupado que podrán ustedes alquilar al módico precio de asistir a las asambleas locales de tribus anarquistas, hacer turnos en barras y, esporádicamente, enfrentarse a las fuerzas de la ley (lo cual quizás les asuste en un primer momento pero les aseguramos que las heridas de porrazos cicatrizan y que, a pesar de que algunos sectores de la sociedad les miren mal, acabarán incluso disfrutando secretamente de sus miradas indignadas).

2. Proveanse de material informático y tecnológico de todo tipo y recuerde: ¡todo artefacto tiene más de un uso! Les sorprenderá a ustedes comprobar que hay gente dispuesta a solidarizarse con

miento de resistencia global), pasando por la alfabetización digital, el derecho de acceso a la red o la defensa de la privacidad en el espacio informacional. La naturaleza física pero a la vez virtual del hacklab permite un input de dos espacios sociales que se superponen: el ciberespacio y el espacio físico. Esto hace que encontremos en los hacklabs una serie de transformaciones y experimentos que no son posibles exclusivamente en la red (donde sucede la mayoría de la producción de software libre), ni exclusivamente en el espacio físico y social fuera del ciberespacio. Esto permite a los hacklab desarrollar una serie de iniciativas tecnopolíticas híbridas (que mezclan ambos espacios) que no pueden desarrollar otros grupos políticos. Ejemplos de estos proyectos híbridos son la creación de redes wireless o la alfabetización digital.

En cuanto a los componentes, el hacklab recoge también cuerpos dispersos de individuos con intereses tecnopolíticos que buscan un espacio colectivo físico de experimentación y encuentro, a la vez que un espacio virtual de trabajo y comunicación. También se recoge «chatarra» tecnológica para su reutilización y reapropiación colectiva. En este sentido el hacklab *re-une* fragmentos dispersos de la periferia tecnológica y social para constituir un colectivo tecnopolítico experimental. Puede parecer una estupidez resaltar que un hacklab reúne cuerpos alrededor de un espacio físico; eso es, al fin y al cabo, algo que sucede en todos los colectivos tradicionales y nunca resulta algo recalcable, se da por supuesto. Pero en el contexto del ciberespacio y la descorporalización progresiva de la identidad humana en registros informacionales gubernamentales y corporativos, reafirmar el encuentro presencial de los cuerpos biológicos es, también, una apuesta política. El ser humano siempre ha estado controlado por una serie de registros manejados por instituciones disciplinarias. Sin embargo con el aumento de la capacidad de transferencia, almacenamiento y manipulación de la información, el cuerpo de datos de un ser humano (el conjunto de información personal registrada en archivos médicos, escolares, laborales, financieros, legales, etc.) amenaza con ser más importante incluso que su cuerpo biológico. En palabras del Critical Art Ensemble «lo que tu cuerpo de datos dice

su nuevo hacklab y donar hardware ¡sin compromisos! Y lo que es todavía más asombroso: podrán beneficiarse de la amplia gama de material informático que tiran las grandes corporaciones a la basura, AUNQUE SEA COMPLETAMENTE ÚTIL.

3. Háganse expertos en las nuevas tecnologías. Si ustedes no disponen de conocimientos técnicos relevantes en el mundo de la informática y las tecnologías no se preocupen. Pueden adquirir expertos en la red, basta con que se acerquen a grupos de usuarios de Linux, foros de debate y otros hacklabs. Los individuos que pueblan estos foros y grupos son de una generosidad asombrosa y les transmitirán sus conocimientos. ¡E incluso se presentarán voluntarios a dar clases COMPLETAMENTE GRATIS! Además podrán acceder a manuales completos en la red, escritos y coordinados por gente voluntaria con el ánimo de contribuir a la comunidad: únanse a ellos.

de ti es más real que lo que tú dices acerca de ti mismo»[3]. Imaginemos por un instante que alguien borrara tu cuerpo de datos, que hiciera desaparecer todos tus registros oficiales. Inmediatamente te convertirías en un fantasma social, de nada serviría el conocimiento que posees, ni los bienes, ni tu nombre, ni tu procedencia si no puedes demostrarlo a través de los registros oficiales. Esta situación supone una especie de triunfo del control a través de la representación (o información) sobre la realidad física y biológica. Este hecho (la virtualización informacional de la identidad civil y administrativa) es relativamente independiente de la socialización en el ciberespacio (en el que uno puede adquirir diversas identidades independientemente de su cuerpo real de datos, experimentar con el anonimato y con nuevos canales de comunicación). Por eso los hacklab no abandonan el ciberespacio como espacio legítimo de comunicación y coordinación, pero buscan resituar el cuerpo y el encuentro *presencial* como un momento insustituible, como un espacio que no se puede *re-presentar* completamente en el universo informacional.

En el movimiento que va de la sociedad al laboratorio se recogen, pues, toda una serie de problemáticas sociales (tanto de la sociedad localizada, como del ciberespacio y de la sociedad global), y se insertan en procesos locales y virtuales que reúnen a máquinas y personas entorno a un espacio presencial de encuentro y experimentación que se refuerza a través de diversas redes de comunicación e información. La pregunta es ahora: ¿qué sucede en ese espacio?

En el laboratorio

Los cuerpos dispersos con sus experiencias y habilidades diversas se unen así para crear una red de intercambio de habilidades. A través de estas redes de intercambio de habilidades el hacklab también se convierte en sujeto tecnológico y político, en un colectivo que busca superar los límites del

3. Critical Art Ensemble: *Digital Resistance*. Autonomedia, Nueva York, 2001. Versión en la red: http://www.critical-art.net/books/digital/.

4. **Realicen acciones subversivas en la red, sin pasamontañas, sin tener que correr ni sudar y, lo que es mejor, ¡sin que se les note en el trabajo! Divertidas acciones telemáticas orientadas a subvertir los símbolos y códigos de las grandes corporaciones: esos monstruos sanguinarios y aburridos que sabotean sus vidas.**
5. **Socialicen, compartan, difundan... Una actividad en la que sin duda saldrán ganando porque (una vez más, este manual esconde sorpresas impensables)... ¡al compartir, GANAN TODOS! Experimenten la libertad de circulación de los saberes, recombinen, reutilicen conocimientos, aprendan y compartan. ¡¡¡Asombroso, pero cierto, cuando compartan una idea no tendrán que dividirla sino que obtendrán DOS o MÁS ideas (dependiendo de con cuanta gente la compartan) completamente gratis!!!**

aislamiento y la especialización tecnológica para la experimentación y la creación colectiva. Un repaso por los objetos característicos que pueden encontrarse en la mayoría de los hacklabs quizás nos ayude a comprender lo que sucede dentro y la forma en la que funciona esa red de intercambio y coordinación de habilidades en proyectos de aprendizaje y experimentación.

Objetos

• *Procesadores 486:*

La renovación constante de material informático para hacer funcionar nuevos programas y sistemas operativos (sin los cuales la transferencia de archivos en lenguajes cerrados como Word resulta imposible) no es más que una exigencia del capitalismo para acelerar los ritmos de consumo. La socialización de las tecnologías a través del mercado impone ritmos y necesidades que no responden a los de la sociedad. Los procesadores 486 son un ejemplo del material que queda obsoleto en ese proceso pero que resulta absolutamente útil, siempre y cuando la utilidad sea definida por el usuario y no por un mercado que intenta imponer estándares y modalidades de uso para el consumo de otros productos de mercado. Reciclar es una actividad permanente en los hacklab.

• *Destornillador:*

El destornillador es una herramienta fundamental para desensamblar ordenadores y ensamblar componentes. El destornillador es el símbolo de ese reciclaje pero también de dar otros usos a los artefactos tecnológicos. El ensamblaje creativo no es solamente el proceso de reciclar componentes para reconstruir máquinas que recuperen su funcionalidad (utilidad) original, sino sobre todo para romper esa funcionalidad pre-especificada. Ese acto de ruptura y desensamblaje se convierte así en un acto de liberación y desobediencia al diseño original al tiempo que en una necesidad de (re)creación tecnológica.

6. Realicen asambleas, procesos comunicativos vinculantes en los que los conflictos se resuelven por consenso, para discutir sobre las consecuencias del uso de diversos artefactos, sobre los conflictos a los que se enfrentan como grupo dentro de su contexto social y tecnológico, sobre quiénes son y cómo van a hacer lo que hacen. No sin esfuerzo, descubrirán que es posible (¡incluso efectivo!) trabajar sin un presidente de empresa. Y lo que es más asombroso todavía: ¡SIN JEFE DE PERSONAL!

7. Y finalmente experimenten. Cómo hacerlo va más allá de este manual, lamentamos comunicarles que no existen manuales para ello, y sin embargo, sin que nosotros se lo expliquemos, les aseguramos que ustedes sabrán hacerlo cuando llegue el momento. Si ustedes no quedan satisfechos les devolvemos su ingenuidad, su tiempo de ocio consumista y su aburrimiento.

- *Cable de red:*
  Un espacio lleno de ordenadores y atravesado de cables de red es un espacio tecnológico conectado. Conectar aparatos, proyectos y otras redes es un trabajo típico del laboratorio hacker. Siempre quedan cables sueltos: las redes en los hacklab (ya sean estas redes de ordenadores, de proyectos políticos o de intercambio de saberes y técnicas) son siempre redes abiertas a nuevas conexiones. Las redes de ordenadores de los hacklab (conectadas a Internet) se convierten también en redes públicas de acceso libre (y gratuito), utilizadas por individuos y colectivos para sus necesidades comunicativas e informáticas. La red permite a su vez experimentar la gestión tecnológica de forma colectiva (rompiendo así con el uso y consumo individualista y aislado al que fuerza el mercado). Los sistemas UNIX, como GNU/Linux, fueron diseñados y siguen desarrollándose para permitir a cualquier usuario acceder a sus archivos y su configuración desde cualquier terminal de una red, rompiendo así con la estructura característica de la tecnología de máximo consumo de *un usuario un ordenador*.
- *Servidores:*
  La experimentación colectiva con la red exige también decidir colectivamente la estructura del servidor, la forma de compartir archivos, de estructurar, en definitiva, la interfaz de una red para que sea accesible a todos y desde cualquier terminal. En esta línea resulta especialmente interesante el proyecto «sinroot» del hacklab de Vallekas, que busca anular la figura del administrador central de la red (el superusuario o root) y romper una de las separaciones y asimetrías de poder más enraizadas en los sistemas informáticos: el de administrador/usuario.
- *Una antena de lata de melocotón en almíbar:*
  Las tecnologías wifi de conectividad sin cables permiten superar la dependencia (económica y tecnológica) con las grandes operadoras de cable. El compromiso de los hacklab con las redes metropolitanas wireless (sin cable) es una apuesta por las redes de comunicación autogestionadas y autónomas, una forma de cortocir-

cuitar el control físico de las redes. Cuando no directamente involucrados en la creación de estas redes, los hacklab suelen ser nodos activos de las mismas. La experimentación con el alcance y posibilidades de las tecnologías wifi, su uso como infraestructura comunicativa para acciones políticas o los talleres de creación de antenas son prácticas típicas de los hacklab.

- *Manuales:*

  Una colección de manuales es típica de todos los hacklab: poner a disposición social el conocimiento necesario para la autogestión tecnológica. Pero el hacklab no sólo recicla, fotocopia o imprime manuales sino que también los genera. A diferencia de la mayoría de manuales producidos por editoriales, los manuales libres permiten la colaboración y la mejora constante, además de la libre difusión y copia.

- *Regrabadoras de CDs:*

  La libre difusión de conocimientos y técnicas es una de las tareas fundamentales de la cultura hacker. En este sentido, las impresoras y regrabadoras de CDs son objetos característicos también de los hacklab en los que se construyen centros de copia libre de material e información (documentación, música, software, vídeo, etc.) con licencias copyleft. La comunidad copyleft es un conjunto de actores y productores de software, música, literatura, ciencia, etc., que, sin renunciar a la autoría de sus obras, pone éstas a disposición colectiva a través de licencias copyright invertidas[4] o copyleft (extensión de la forma jurídica del software libre al conjunto de la producción inmaterial). Los hacklab forman parte activa de esta comunidad, especialmente en su vertiente tecnológica y de software, y en la defensa de la libertad de flujo de la información contra las barreras legales (copyright, patentes, censura, criminalización de las redes p2p,...) y las tecnológicas (tecnologías anticopia, protocolos cerrados, etc.).

- *Sillas en círculo:*

  Indudablemente, las mesas son necesarias para apoyar cosas como los ordenadores y las sillas para permitir un postura cómoda en la que trabajar. Pero las mesas y las sillas de un hacklab no son sólo una herramienta para situarse enfrente de la pantalla del ordenador; son también, y sobre todo, dispositivos para crear un espacio de reunión y discusión, de trabajo colectivo y educativo. La asamblea presencial (junto con la virtual) es el órgano de decisión y coordinación principal en un hacklab, la toma de decisión se resuelve por consenso, la inteligencia es colectiva, resultado de esa red de intercambio de habilidades, conocimientos y pasiones.

4. Podemos citar aquí cuatro de los referentes más importantes de la comunidad copyleft que han desarrollado licencias específicas:
- El proyecto GNU y la Free Software Foundation: http://www.gnu.org/.
- Creative Commons: http://www.creativecommons.org/.
- Art Libre - Copyleft Attitude: http://www.artlibre.org/.
- Procomún (coordinación a nivel estatal de iniciativas copyleft): http://procomun.net/.

Experimentación distribuida e integrada

Los productos de la reducción de complejidad en las redes de actores hacktivistas se crean y se destruyen constantemente en proyectos, espacios y acciones que se condensan y se diluyen en múltiples dimensiones, en una topología tecnopolítica dinámica en constante reconfiguración: un espacio rizomático de saberes, técnicas e intervenciones tecnopolíticas. Al margen de las charlas, talleres y cursos específicos que tienen lugar en los hacklab, lo más interesante surge de los proyectos que engloban habilidades de diversos individuos, que se conectan con otros colectivos y procesos, proyectos que comprenden desde momentos de acción junto a momentos de aprendizaje (aprender haciendo), discusión y práctica, investigación y producción. Por ejemplo, la creación de un programa que creara registros (logs) aleatorios de visitas a un servidor y la difusión del mismo programa se convierte en un punto nodal atravesado de experiencias colectivas de creación, aprendizaje, estrategia, diversión, expresión y reflexión. En el mismo proyecto convergen las habilidades necesarias para programar en perl (un lenguaje típico de scripts para el sistema operativo), el diseño del marketing político del producto, el proceso de estructuración de un programa, cursos sobre el funcionamiento del almacenamiento de datos y la reflexión sobre el control gubernamental y corporativo sobre el flujo de datos en la red. Por lo tanto, un proyecto hacktivista de un hacklab agrupa código de alto nivel, de bajo nivel y también otros códigos que atraviesan al ser humano en múltiples dimensiones (códigos asamblearios, estéticos, políticos, etc.), en un proceso que sirve de aprendizaje, socialización, producción y acción política al mismo tiempo.

Del laboratorio a la sociedad

Retomando el análisis de Latour, para que el trabajo en el laboratorio tenga un efecto sobre la sociedad, hará falta que el laboratorio se extienda, extienda sus condiciones de verificación, sus métodos de evaluación, sus procedimientos para que éstos sean aplicables más allá de los muros del laboratorio. La forma habitual en la que la producción tecnocientífica se extiende a la sociedad es a través del mercado; con las consecuencias obvias de ofrecer sólo cajas negras orientadas a maximizar el beneficio económico (y la carrera de consumo) a corto/medio plazo.

Los mecanismos de extensión de los hacklab a la sociedad son quizás los más elaborados y suponen, sin duda, una de las características más específicas de los hacklab frente a otras formas de activismo tecnopolítico y, sobre todo, frente a los laboratorios tradicionales. El flujo que va del laboratorio a la sociedad es un aspecto muy desarrollado por dos razones. La primera es la tarea asumida de socializar y difundir herramientas tecnológicas, saberes y técnicas para facilitar una autogestión tecnológica global. La segunda es la actitud de intervenir en los sistemas tecnológicos para defender espacios de libertad, abrir nuevas posibilidades de acción y desencadenar procesos de liberación y reapropiación tecnopolítica.

Programas de radio, encuentros o jornadas entorno a las redes wireless, charlas sobre cifrado, funcionamiento de redes o hacktivismo, cursos de instalación y uso de GNU/Linux, creación y difusión de manuales y distribuciones de GNU/Linux, son formas de transmitir y socializar la producción tecnocientífica en los hacklab. El hecho de estar, generalmente, situados en Centros Sociales Okupados Autogestionados (CSOA) facilita a su vez esta labor de socialización (así como el movimiento de la sociedad al laboratorio). Otra forma de difusión, que es a la vez una máquina de uso directo, es la distribución autoinstalable de Debian GNU/Linux *X-Evian*[5] que desarrolló (y sigue desarrollando) el Metabolik BioHacklab (el hacklab de Bilbao) con motivo de la contracumbre contra el G8 en Evian (Francia). Esta distribución está orientada a activistas y mediactivistas, se autoinstala en casi cualquier ordenador y no toca el disco duro, con lo que puede utilizarse en cualquier equipo sin necesidad de dañarlo o modificarlo. La distribución incluye además toda una serie de programas de encriptación, edición de vídeo, foto, etc., además de las aplicaciones típicas de ofimática, navegador, gestor de correo, etc. La distribución incluye una página web de inicio con toda una serie de links a páginas activistas, así como la documentación necesaria para hacer uso de las herramientas que incluye.

El *hacking the streets* (hackeando las calles) es también una iniciativa característica de la difusión pero que también encierra aspectos interventivos. Realizado por primera vez por Kernel Panic (hacklab de Barcelona), el *hacking the streets* está inspirado en el movimiento británico Reclaim The Streets y el objetivo es visualizar el desarrollo de tecnologías alternativas, sacándolas de los muros de los laboratorios, empresas y universidades a la calle para mostrar su accesibilidad y el potencial de uso social que poseen. El *hacking the streets* es además una forma de protesta festiva, educativa y participativa en la que se combinan ordenadores, música, charlas e instalaciones de Debian GNU/Linux. A modo de *happening*, el *hacking the streets* rompe con el aislamiento e individualismo característico del uso tecnológico para reclamar la calle y los espacios públicos como espacios de cooperación, intercambio y solidaridad tecnopolítica. En la misma línea que los *hacking the streets* destacan las Jornadas Circulares que organizó el hacklab de Vallecas. Con motivo de su primer aniversario, el hacklab de Vallecas se decidió a okupar el metro como espacio público para realizar una serie de charlas y conferencias en la línea circular[6].

El espacio telemático (el de la comunicación a distancia posibilitada por nuevas tecnologías de la información) es sin duda uno de los canales más fructíferos del laboratorio a la sociedad. En innumerables ocasiones la publicación rápida y efectiva en la red de material censurado o silenciado o la puesta en marcha de herramientas comunicativas específicas ha sido crucial para el desarrollo de ciclos de protesta y movimientos sociales y políticos. Un ejemplo de ello es la «Cadena Humana na Costa da Morte de Area Negra»[7] que consiguió organizar con herramientas GNU

5. http://www.x-evian.org/.
6. http://www.kaslab.sinroot.net/jornada_circular/.
7. http://www.areanegra.net/.

adaptadas por el hacklab de la Casa Encantada una cadena humana de más de 75.000 estudiantes (más de 1.000 autobuses) de toda Galiza, lo cual consiguió romper en febrero el silencio mediático impuesto por el gobierno gallego/español sobre el vertido y sobre su gestión que derivó en el hundimiento del Prestige. Los recursos tecnológicos y los conocimientos telemáticos que el hacklab puso a disposición de las organizadoras de la cadena fueron de crucial importancia en un contexto de control mediático y social exhaustivo por parte de las autoridades locales, así como para superar las trabas e impedimentos que las instituciones establecían a la coordinación entre centros escolares. Dentro del espacio telemático destaca sobre todo el uso de tecnologías de *streaming* de audio y video (emisión comprimida y en directo por Internet), que permiten cortocircuitar la mayoría de los mecanismos de censura tradicionales.

En definitiva, las redes de intercambio de habilidades, el aprendizaje colectivo y los procesos de comunicación dentro del hacklab permiten el surgimiento de una capacidad de crítica y acción que se condensa en proyectos tecnopolíticos interventivos. Un ejemplo de ellos es la acción directa telemática[8], la guerrilla de la comunicación en el ciberespacio o la producción de programas de carácter hacktivista.

Hay una frontera que los laboratorios tradicionales mantienen celosamente: la autoridad experimental y el control sobre el método. Aquí es también donde los hacklabs se enfrentan al concepto tradicional de laboratorio fomentando la actitud experimental, la autogestión tecnológica en otros espacios sociales, defendiendo que en la producción tecnocientífica de tecnologías de comunicación e información la autoridad última es siempre la sociedad que se construye desde ellas. Es por ello que los hacklab (además de compartir espacios, métodos y prácticas) encuentran en los CSOA una continuidad de experimentación y desarrollo. En palabras de Blicero (miembro del hacklab LOA de Milán):

> *Dos características fundamentales de la ética hacker son la voluntad de dar a los saberes la máxima posibilidad de circulación y el deseo de comprender el funcionamiento de los mecanismos complejos para poder, a continuación, reutilizarlos en favor de los propios deseos. Si trasladamos esas características a un medio no técnico, es muy fácil identificar a los centros sociales okupados y a los espacios autogestionados como intentos claros y evidentes de* reality hacking. *La convergencia de ambos motivos (el histórico y el «comportamental») han hecho que los hacklabs y las experiencias de autoorganización compartan espacios y recorridos.*[9]

8. http://www.sindominio.net/metabolik/it4all_money4them.html/.
9. Conversación con Blicero sobre la experiencia del LOA Hacklab de Milán. Entrevista realizada por Aris Papathèodorou y Ludovic Prieur en la revista *Multitudes*, 5. Versión castellana traducida por Daniel Gil en: http://www.sindominio.net/labiblio/doc/loahacklab.htmhttp://www.sindominio.net/labiblio/doc/loahacklab.htm/.

El hacklab como laboratorio tecnosocial

El flujo de laboratorio a sociedad y de sociedad a laboratorio es tan intenso que apenas merece la pena hacer la distinción, aunque nos haya servido como guía para ir descubriendo una serie de prácticas y actitudes. De hecho si observamos los dos extremos juntos descubrimos una conclusión que no puede comprenderse si los entendemos separadamente: los hacklabs son una forma de construir sociedad, pero de una forma especial: construyendo y deconstruyendo las interfaces, las redes y las herramientas informáticas para una comunicación e interacción liberadas, experimentando con ellas, en un proceso abierto y participativo que busca el conflicto social y la dificultad técnica como espacios en los que ir construyéndonos a nosotros mismos[10].

Hackmeeting: la manifestación de un cyborg de multitudes

«Al principio estaban los hackmeeting...»
Blicero

Si hemos empezado entonces por la palabra misma: hacklab, laboratorio hacker; y por descifrar el significado de «hacker», por un lado, y «laboratorio», por otro, para adentrarnos progresivamente en el tejido de relaciones que fusionan los dos conceptos, pasando por una descripción de los objetos que se pueden encontrar en un hacklab, el flujo de códigos, saberes, técnicas y problemas que van desde la sociedad al laboratorio y del laboratorio a la sociedad, podemos ahora desembocar finalmente en la manifestación de un cyborg de multitudes que es el hackmeeting, un encuentro anual de personas, máquinas, proyectos, expresiones y tendencias que es la matriz original de la que han surgido la mayoría de los hacklabs (tanto en el entorno italiano como en el hispano).

El primer hackmeeting tuvo lugar en Florencia en 1998, y desde entonces se han ido repitiendo anualmente en Italia. En el 2000 se celebró el primer hackmeeting en el estado español en Barcelona, en el 2001 fue en Leioa (Bilbao), y así sucesivamente en Madrid, Iruña, Sevilla y Menorca en 2005. El hackmeeting (como su nombre indica) es un encuentro de hackers en torno a los usos sociales de las tecnologías y la telemática. El primer transhackmeeting de carácter internacional se realizó en el Pula (Croacia), en junio de 2004, y acogió activistas de toda Europa[11]. Eventos similares a los hackmeeting tienen también lugar en los países del norte de Europa, destacan el Plug'n'Politix[12] y el Chaos Computer Camp[13]...

Si antes hemos recogido el concepto de laboratorio científico para ir describiendo paralelamente (resaltando continuidades y diferencias) lo que es un hacklab, podemos ahora trasladar la analogía al hackmeeting y compararlo con los congresos científicos. El hackmeeting rompe con las dicotomías características y las estructuras tradicionales de los congresos científicos. La separación entre organiza-

10. Más textos e información sobre hacklabs pueden encontrarse en: http://hacklabs.org/.
11. http://www.sindominio.net/hackmeeting/, http://hackmeeting.org/, http://trans.hackmeeting.org/.
12. http://www.squat.net/pnp/.
13. http://www.ccc.de/camp/.

TALADRANDO CAJAS NEGRAS

La teoría de la red de actores* muestra cómo la producción tecnocientífica esconde procesos de reducción de complejidad y de relaciones de poder que dificultan una reapropiación abierta de los productos tecnocientíficos por parte de la sociedad. De acuerdo con esta teoría, las comunidades tecnocognitivas están compuestas por seres humanos, aparatos, instituciones, redes electrónicas, publicaciones y un largo etcétera de mecanismos y agentes. Los seres humanos no pueden entenderse aisladamente como productores de conocimiento, sino sólo insertos en una compleja red de referencias, artefactos e instituciones. Incluso el producto tecnocientífico de estas redes se reintroduce en la propia red convirtiéndose en un actor más. Sin embargo, para que la red sea productiva se requiere una reducción de la complejidad. En un proceso que los autores denominan de «translación», subredes del proceso son representadas por actuantes que se convierten en cajas negras (*black-box*) para los otros componentes de la red. Estos actuantes comprimen la complejidad de los procesos de la subred que los genera para poder ser re-introducidos con efectividad en los procesos de una red más amplia. De esta manera los black-box o actuantes se convierten en entidades unificadas que son utilizadas por otros actores de la red o se convierten ellos mismos en actores. El punto de translación se convierte así en espacio de poder y control, de tal manera que los procesos de translación se convierten en fuente de orden social dentro de la propia red, ya que determinan los ensamblajes de (re)organización de las interacciones dentro de ella. Estas cajas negras no sólo esconden la complejidad producida sino el entramado de relaciones de poder y los discursos de la subred productora. Las cajas negras pueden tener la forma de herramientas (artefactos materiales), organizaciones (cuando están representadas por un ser humano) o conceptos clave (cuando son el resultado de un proceso cognitivo). Las cajas negras son máquinas (tal como han sido descritas anteriormente) cuya estructura permanece oculta tanto para facilitar su reinserción en el sistema tecnológico como para responder a intereses de dominio y dependencia por parte de los productores.

Dos factores acentúan la jerarquización de poder en la producción tecnocientífica (financiada con dinero público pero socializada casi exclusivamente por el mercado):

* Esta teoría está desarrollada en Latour, B. y Woolgar, S.: *Laboratory Life: The Construction of Scientific Facts*. Princeton University Press, 1986; y en Latour, B. *Pandora's Hope: Essays on the Reality of Science Studies*. Harvard University Press, 1999

a) La complejidad creciente de la producción tecnocientífica junto a la hiperespecialización que se va dando en el proceso. Un proceso de especialización que aísla al técnico en un dominio específico en el que se le exige el máximo rendimiento, pero desde el que se pierde una visión de conjunto y sentido (más allá de la transacción económica del servicio prestado y el ensamblaje de su trabajo con las especialidades más próximas).

b) La necesidad de la tecnoeconomía capitalista de cerrar las cajas negras y dificultar el acceso a los procesos que encierran para aumentar así la competitividad en los procesos de innovación. Una necesidad que se satisface a través de patentes, secretos de empresa, del código cerrado en el desarrollo de software, tecnologías opacas, etc.

A través del uso, creación y difusión del software libre y de la experimentación con y a través de él, los hacklab rompen con los privilegios de poder de los puntos de traslación en los que se producen las cajas negras que caracterizan a la producción tecnocientífica. No se trata tanto de descomprimir para siempre la complejidad de esas cajas y de hacer que todo el mundo sea experto en todo, sino más bien de abrir los procesos de producción de las cajas, de situarse en los procesos de translación, de hacerlos accesibles a quienes lo necesiten y de reunir para una acción o proceso social concreto las herramientas, las habilidades y los conocimientos necesarios para las relaciones de poder cristalizadas en esas cajas, de forma que puedan ser reconfiguradas de acuerdo con unos objetivos dados. Al mismo tiempo, la experimentación tecnocientífica colectiva fuera de las instituciones laborales y de los roles allí asumidos permite una comunicación e interacción entre especialistas que rompe con el aislamiento. Esta ruptura del aislamiento hiperespecializado, en procesos de conflicto y experimentación, permite construir una visión global de la tecnología y de sus consecuencias políticas, y abre las puertas para el surgimiento de una subjetividad tecnopolítica crítica (en tanto que la comunicación entre especialistas permite la creación de esa visión global) y práctica (en tanto que la red de intercambio de habilidades y la inteligencia colectiva genera un poder tecnopolítico colectivo inalcanzable para los individuos aislados).

dores y participantes no existe, todo participante deviene organizador. La organización del congreso es virtual (a través de una lista de correo que sirve de asamblea permanente y una página web de libre modificación —wiki—) y abierta (tanto la lista de correo como el espacio son de acceso público). Una llamada a la participación call4nodes (llamada para nodos) sustituye al tradicional call4papers de los congresos, abriendo la participación a cualquier nodo posible: talleres, reuniones, performances, charlas, proyecciones, tenderetes, música, etc. Otra característica de los hackmeeting es que rompen con la dicotomía expertos/no-expertos, nosotros/ellos, y se convierte en un espacio de aprendizaje y cooperación en la que pueden encontrarse tanto charlas y talleres de iniciación o divulgación como especializados.

El hackmeeting es un momento de encuentro presencial y corporal de una red distribuida de activistas que realizan su trabajo en entornos locales y virtuales. Es por ello que en el hackmeeting se experimenta generalmente la celebración de una comunidad global pero a la vez diversa, una manifestación productiva de saberes y proyectos, de comunicación y coordinación, en la que se dan cita diversos colectivos e incluso miembros de colectivos cuya naturaleza digital y distribuida dificulta el encuentro presencial.

Los temas que se tratan en el hackmeeting van desde los virus informáticos a la criptografía, pasando por discusiones sobre control social en la red, la vida artificial, el mediactivismo, el software libre o los fallos de seguridad de las redes wireless. Temas que encuentran su expresión en diversas actividades: proyección de películas, charlas, mesas redondas, plataformas de coordinación, exposiciones, debates, talleres... Todo ello condensado en un fin de semana en el que alrededor de 500 personas se reúnen en un CSOA que acoge tanto las actividades como alojamiento para los participantes. La infraestructura tecnológica del hackmeeting (redes, servidores, algunos ordenadores) permanece en el lugar, dando pie al surgimiento de un nuevo hacklab o reforzando la infraestructura del ya existente.

Geografía de un hackmeeting

La mejor manera de saber lo que sucede en un hackmeeting es atravesar su geografía, recorrer sus espacios y describirlos. Empecemos por la entrada. El hackmeeting tiene dos entradas/salidas: la entrada/salida de la red y la del espacio físico. En los hackmeeting italianos es costumbre que la entrada al espacio físico esté precedida de un DHCP humano (una asignación de IP a través de la mesa de recepción), fusionando así las dos entradas en una con el juego de asignar a quien acaba de llegar su dirección dentro de la red informática. La información en la mesa de acogida en la entrada incluye además el horario de las actividades previstas, venta de camisetas (y merchandising diverso con el que cubrir los gastos del evento) así como la información básica sobre la forma de (auto)organización del hackmeeting.

Generalmente, el espacio más grande se asigna al LAN (*Local Network Area* o espacio de la red local), en el que más de cien personas despliegan sus orde-

nadores para conectarse digitalmente al HM; y un buen número de ordenadores se ponen a disposición colectiva para quien no haya podido traer el suyo o no disponga de uno. Más allá del LAN, dos o tres salas para charlas y talleres. Una sala principal de actos suele acoger eventos más numerosos como los Big Brother Awards (Premios Gran Hermano a los individuos, corporaciones e instituciones menos respetuosas con la privacidad y los derechos digitales)[14], conciertos de música copyleft, teatro y charlas para las que se espera mucha audiencia o participación. La sala de actos se utiliza también para las asambleas de apertura y clausura, y se convierte por la noches en espacio para dormir, aunque un buen número de mentes permanezcan despiertas en la LAN y en la barra del bar intercambiando información entre las cervezas y los cables.

Pero la geografía de un hackmeeting comprende también espacios más pequeños pero igualmente importantes. Una pequeña sala se dedica casi exclusivamente a retransmitir las charlas por Internet, recoger diversos testimonios del evento y documentar (en audio y vídeo) el máximo número de contribuciones e historias. La barra del bar es otro sitio de fundamental importancia, lugar en el que aumenta la entropía y el caos dando pie a charlas espontáneas, reuniones improvisadas o descabelladas ideas que terminan generando proyecto colectivos que se desarrollarán en el ciberespacio durante el resto del año. También viene siendo una tradición contar en el hackmeeting con una pequeña sala de cine en la que volver a ver las películas de culto que han inspirado al movimiento (*Tron, 23, Johnny Mnemonic, Matrix, Solaris, Ghost in the Shell, Blade Runner, El Cortador de Césped, Pi,...*). También se proyectan documentales mediactivistas sobre conflictos políticos, movimientos sociales y diversas experiencias activistas, especialmente las relacionadas con el hacktivismo, el mediactivismo y la telemática. También pueden encontrarse en el hackmeeting museos de ordenadores antiguos, pequeñas bibliotecas con artículos y textos de interés, una sala chill-out con música y proyecciones de vídeo, espacios de reciclaje, tenderetes con material de autogestión de diversos colectivos, comedores vegetarianos y un largo etcétera.

Cyborg de multitudes

«El cyborg es un tipo de yo postmoderno personal y colectivo des-ensamblado y re-ensamblado.»
Donna Haraway[15]

Según Tim Jordan[16], el primer dispositivo que instaura un sujeto en la TIC es el login, la primera pantalla o interfaz con la que se encuentra el usuario al acceder a un ordenador, una red y muchas páginas de Internet, pidiéndole el nombre de usuario y la contraseña. El nombre de usuario es la marca de una identidad, una marca de pertenencia a unos privilegios de uso. La contraseña, la protección de la individualidad de esa identidad. Sin embargo, la red de ordenadores que se construyen

14. http://www.es.bigbrotherawards.org/.
15. Haraway, D. (1990) «A manifesto for Cyborgs: Science, Technology and Socialist Feminism in the 1980s«, en Nicholson, L. J. (ed.) *Feminism/Postmodernism*. Routledge, Nueva York, pp. 190-233.
16. Jordan, T. (1999) «Cyberpower and the meaning of *on-line* activism«. *Cybersociology*, 5. Versión en la red: http://www.socio.demon.co.uk/magazine/5/5jordan.html/

en el HM (tanto por ordenadores particulares como por colectivos —reciclados y disponibles al público—) sigue la convención de ofrecer en todas las terminales el acceso al usuario «hm» con contraseña «hm» (aunque de hecho la contraseña suele cambiar generalmente de un evento a otro). Si el dispositivo de nombre y contraseña de usuario se descubre como dispositivo de individuación en el ciberespacio, la creación de un usuario colectivo y una contraseña pública se convierte en una forma de subvertir ese dispositivo y abrir un espacio para la instauración (o manifestación) de ese cyborg de multitudes que es el HM.

Somos cyborgs desde hace milenios, pero solamente la sobrecogedora posibilidad de la cirugía electrónica actual que permite el implante de chips, fusionándonos así físicamente con las máquinas (y las visiones futuristas que se dibujan a partir de ella) hacen que hayamos alcanzado a visualizar nuestra naturaleza cyborg. Mitad máquinas mitad humanos, los cyborg son una amenaza para el concepto tradicional de identidad humana, cuya racionalidad característica se extiende ahora en los artefactos en los que vive empotrada esa identidad, diluida entre ensamblajes, prótesis, códigos y máquinas. Al mismo tiempo, la identidad humana se fragmenta por dentro atravesada por deseos, estructuras inconscientes, funciones sociales y programaciones conductistas publicitarias, hasta el punto de que Deleuze y Guattari prefieran describir la singularidad humana como un haz de multiplicidades; y el movimiento de resistencia global haya recogido el término multitudes para expresar un proceso análogo a escala colectiva. El hackmeeting ilustra perfectamente el concepto de multitud cyborg: una maraña de personas y máquinas (ordenadores, cables, proyectores, altavoces, etc.) conectada a través de redes digitales y sociales, a través de talleres y discos duros, un experimento colectivo en el que se cristalizan y diluyen diversas subjetividades políticas, núcleos de producción tecnocientífica, nodos de redistribución de ideas y proyectos. El hackmeeting es, pues, la manifestación de un cyborg de multitudes que condensa tendencias y proyectos, ilusiones y amistades, posibilidades y conocimiento, máquinas y personas que caminan en múltiples direcciones pero en el mismo sentido: dejar de estar sujetos a la tecnología como espacio del dominio político y generar nuevos sujetos políticos tecnológicamente corporizados.

Enlaces interesantes:

2600: http://www.2600.com/
The phrack: http://www.phrack.org/
Chaos Computer Club: http://www.ccc.de/
Captain Crunch: http://www.webcrunchers.com/crunch/
Ficheros de textos (textfiles) que circulaban por las BBS en los años ochenta: http://www.textfiles.com/
Jargon file: http://www.catb.org/~esr/jargon/

Por años, meses y días, redes y comunidades de individuos han ido intercambiando saberes, proyectando mundos, experimentando juguetes y dispositivos. Venimos desde mil pensamientos diferentes, somos migrantes de la metrópoli y de la red, buscamos un lugar donde crear con prácticas semejantes un espacio-tiempo divergente.

Queremos ensamblar otra vez la realidad y para ello necesitamos laboratorios en los que recombinar sus elementos. En una ciudad llena de falsas seguridades y verdaderos miedos, queremos hacer surgir un lugar hecho de imaginario, sueños, carne, metal y bits.

Nuestras mentes colectivas, cerebros de multitudes, están llenas de tecnología digital-analógico, info-comunicación, conocimiento-distribuido, memética-participativa y mucho mucho más.

Cuatro puntos cardinales no son suficientes. Con Marte tan cerca de la Tierra es la hora para una nueva constelación reticular, para recompilar un bioware entrópico, para sorprender[nos|os] con nuevos y vivísimos efectos especiales.

Reload, Hacklab Milano, 14 de septiembre de 2003. Texto de presentación del LOA (hacklab de Milán) en su reaparición en el 2003 y rebautizado como reLOAd.

LOS DISCURSOS DEL HACKING

rm -rf /capitalism
killall state
apt-get install anarchism
(leído en *hackmeeting@listas.sindominio.net*)

Gustavo Roig Domínguez*
(Nodo 50,
Gustavo@nodo50.org)

El hacklab como comunidad política: «a estas alturas las ideologías, entendidas como hasta ahora, son un lastre»

Después de charlar y entrevistar a algunos miembros activos de los hacklabs, estamos en condiciones de estructurar algunos bloques discursivos que sintetizan y se extraen de un imaginario compartido acerca de *la comunidad* o *movimiento*, de la técnica y de la política. Quizá sea mas preciso hablar del conjunto de *ideas fuerza* (a veces repetidas hasta convertirlas en *cliché*) que definen o dan sentido a prácticas compartidas. Hasta cierto punto, reivindicaciones (agenda política propia) y, en cierto sentido, significantes políticos a los que se pretende dar significado a través de la acción, del *hack*, lejos de la teorización y la elaboración ideologizante.

Gustavo: ¿Definirías el hacklab como una comunidad política?

Towanda: Sí.

G: ¿Cómo lo argumentarías?

T: Pues, digamos que es una comunidad abierta, horizontal... todas las decisiones se toman de forma consensuada entre todos y se trata también de tratar de llevar puesto lo que es el software libre, las redes wireless y todo este tipo de temas, los ciberderechos a... digamos que eso llegue a otros movimientos sociales.

Towanda, que es activo políticamente por primera vez en su vida en el hacking, intuye o siente la dimensión política del trabajo de su comunidad y lo

* Este artículo es la segunda parte de «Hackers: Activismo político en la frontera tecnológica».

expresa en dos líneas conceptuales: *mi comunidad es democrática en lo organizativo («comunidad abierta, horizontal»), y maneja una agenda política propia (software libre, ciberderechos, acceso libre a la conectividad vía wireless) que comparte o abre a otros movimientos o redes sociales.*

G: Bien. ¿Piensas, de alguna manera, que existe una forma de ser, o podemos llamarle una filosofía, hacker?

T: ¿Una filosofía hacker?

T: Claro, es un término difícil, dependiendo de lo que entiendas. Bueno, yo creo que hay varias cosas... digamos que dentro de la cibersociedad, para mí sería el acceso a la información, por un lado. Por otro lado, el tomar control de la tecnología, entenderla, mejorarla. Y, por otra parte, compartir esa información, o sea, ese conocimiento...

G: ¿Qué es para ti una comunidad hacker... o una comunidad de usuarios de Linux, o una comunidad de gente con la que tú te mueves...? O sea, ¿cómo definirías esa gente con la que tú te mueves, ese entorno, ese grupo?

T: Pues... como un grupo de gente con ganas de aprender cosas, de conocer cosas... y de compartir esa información.

G: Ajá. A ti pertenecer a este grupo ¿qué te aporta? La pregunta es también en un sentido amplio...

T: Pues, en un sentido amplio, bueno... primero todas las relaciones que surgen; segundo todo lo que puedes aprender, o todo lo que puedes enseñar... y... luego todo el potencial que puede surgir de ahí: al haber una comunidad, pues ya salen distintos intereses que pueden unirse y a partir de ahí crear otros colectivos, otras historias. Pues por ejemplo, en el caso del hacklab hemos salido de ahí, bueno, de parte de ahí salió Madrid Wireless, u otros proyectos...

La comunidad de activistas se reconoce a partir de planteamientos (conceptos) aglutinadores, sin sesgo político evidente (ese aparente punto neutro de lo técnico) que le permite, desde nuestro punto de vista, establecer puentes entre las experiencias personales políticamente más clásicas y el conjunto de activistas que provienen del mundo «despolitizado» del puro conocimiento técnico-científico. *Acceso a la información, compromiso ético cooperativo, redistribución de la información* en forma de conocimiento procesado (conocimiento y experiencias técnicas) son elementos de un imaginario que se enuncia al definir el nuevo medio como «cibersociedad», reclamar la necesidad de «tomar control de la tecnología, entenderla, mejorarla» y proyectar la acción hacia el exterior, al «compartir esa información... ese conocimiento». Coa, con la que Towanda comparte colectivo, maneja otro registro discursivo y un nivel más elaborado de reflexión política:

(00:28:59) franz: el hecho de cooperar o no cooperar, es decir, decidir por vivir de una forma u otra... es el resultado de una decisión «político ideológica»?

(00:29:17) ***Coa:*** *en el caso del hacktivismo creo que no*

HACKERS Y CRACKERS

El apelativo de «hacker» se crea a fines del siglo pasado cuando los Estados Unidos de América empieza a recibir un masivo movimiento migratorio de personas de todos los países del mundo que esperaban encontrar en el «país de las oportunidades» un bienestar económico y progreso. Los hackers eran entonces estibadores informales que se pasaban todos el día bajando las maletas y bultos de las personas y familias completas que llegaban en los barcos a los puertos de Nueva York, Boston, San Francisco, etc. Estos trabajadores eran —no tenían más narices que ser— infatigables, pues trabajaban muchas veces sin descansar y hasta dormían y comían entre los bultos de los muelles con el objeto de no perderse una oportunidad de ganar dinero. La palabra inglesa «hack»

(00:30:01) **Coa:** *digamos que la palabra ideología, política*

(00:30:10) **Coa:** *no son parte activa de la comunidad hacker*

(00:30:22) **Coa:** *aunque para mí... lo es de forma implícita*

(00:30:27) **Coa:** *quizás por eso funciona*

(00:30:44) **Coa:** *porque no se tiene la presión de que tiene que ser «polítticamente correcto»... simplemente es*

(00:31:41) **Coa:** *a estas alturas la ideología, entendidas como hasta ahora, son un lastre*

(00:32:45) **Coa:** *y más en estos momentos de cambios*

(00:33:08) **Coa:** *desde la globalización, hasta la presencia de las tecnologías, hasta la desaparición del trabajo tradicional...*

(00:33:21) **Coa:** *es un momento de confusión...*

(00:33:34) **Coa:** *y las ideologías que hasta ahora servían ya no lo hacen*

(00:33:57) **Coa:** *y el hacktivismo pulula... pero en otras referencias*

De forma que el *hacking*, en la misma medida en que lo hacen los nuevos movimientos sociales occidentales de los sesenta en adelante, maneja una definición de lo político-ideológico flexible, alejada de los modelos al uso en la izquierda tradicional, del leninismo o incluso el anarquismo militante. Más empeñados en la construcción de comunidades amplias y la extensión de *valores* compartidos, que en la organizaciones estructuradas de intervención política, rígidas y verticales, cohesionadas sobre metarrelatos ideológicos. En el hacklab no hay discursos muy elaborados en relación a patrones político-ideológicos tradicionales, *pero sí existe una reflexión política perfectamente expresada* en la descripción del «momento de cambio»: la globalización de los procesos sociales, el cambio tecnológico, el fin de la centralidad del trabajo. El hacktivismo puede orientarse por construcciones ideológicas sobre la realidad, pero «*pulula en otras referencias*» que no son las de la izquierda clásica. ¿Cuáles?

tiene varios significados en español, entre ellos el de «hacha». Aquellos estibadores sin duda debían ser unos hachas.

De tan remoto (?) origen, la pista vuelve a aparecer con los primeros pasos de la informática moderna, entre los años cincuenta y setenta, cuando los ordenadores eran enormes artilugios que ocupaban varios metros cuadrados, tan grandes que incluso una persona podía pasearse entre sus circuitos y piezas. Pero, de la misma forma que una persona podía acceder a su interior, también lo hacían multitud de insectos, los cuáles provocaban la mayoría de los fallos en los ordenadores (de ahí el nombre de «bug» —«insecto» en inglés— con el que se conoce a los fallos informáticos). Los encargados de velar por el buen funcionamiento de los sistemas eran los hackers, personas que se conocían todos los recovecos de estos ordenadores. Ellos conseguían que todo volviese a funcionar

Los activistas se definen: «¿inquieta de izquierdas o inquieta de derechas?»

A Towanda le cuesta exponerlo con las expresiones formales al uso en los ámbitos políticos tradicionales. Pero lo consigue: se siente cómodo en la *horizontalidad*. Es *anarquista*:

Gustavo: ¿Te defines como un activista político?

Towanda: Sí.

[…]

G: ¿cómo te defines políticamente?

T: ¿Políticamente? pues ..... [silencio] pues ... no sé el nombre exactamente, quizás anarquista. O sea, me siento mucho más cómodo en los espacios abiertos, horizontales.

G: Lo comentaste antes.... me decías que antes de participar en el hacklab o en grupos o comunidades de hackers o activistas no habías tenido experiencias políticas, asociativas...

T: Había conocido algunas okupas, aunque no había participado en ninguna, pero las había conocido, había conocido gente dentro.

G: Siempre en el mundo de los centros sociales?

T: Ajá.

Y una vez más Coa cuestiona los paradigmas tradicionales de la teoría política:

(01:30:55) **franz:** *cómo te defines políticamente?*
(01:31:24) **Coa:** *inquieta :-D*
(01:31:52) **Coa:** *no te puedo contestar mas certeramente*
(01:31:54) **franz:** *inquieta de izquierdas o inquieta de derechas?*
(01:32:10) **Coa:** *pues yo diría que de izquierdas...*
(01:32:21) **franz:** *por qué?*
(01:32:37) **Coa:** *pero creo que hablar de izquierdas y derechas aunque nos enten-*

correctamente, dando un golpe seco en partes concretas de los circuitos, como si de un «hachazo» o «corte» se tratara. Aunque pueda resultar un tanto sorprendente, la mayoría de los problemas de los rudimentarios ordenadores se solucionaban a base de «golpes».

Pero dejándonos de orígenes etimológicos, podemos ir al respetado diccionario de la jerga de Eric Raymond para ver su definición del «hacker»:

HACKER [originalmente, alguien que fabrica muebles con un hacha] s. 1. Persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades; al contrario que la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible. 2. El que programa de forma entusiasta (incluso obsesiva). 3. Persona capaz de apreciar el «valor del ha-

demos ya no tiene mucho sentido

(01:33:38) ***franz:*** *ok*

(01:33:44) ***Coa:*** *digamos que el interés por lo social, lo común, que el beneficio sea para todo el mundo*

(01:33:57) ***Coa:*** *son conceptos asociados a la izquierda*

(01:34:37) ***Coa:*** *pero creo que las cosas están cambiando...*

(01:34:40) ***Coa:*** *aunque no se para dónde...*

Para Towanda y Coa el tipo de práctica tecnopolítica en la que se han implicado difícilmente se encuadra o se define en el repertorio tradicional de opciones o posiciones posibles dentro del espectro político clásico. En tanto que *novísimo movimiento social*, puede perfectamente integrarse en la lógica antisistémica del conjunto de redes que cuestionen los fundamentos de la propiedad y el poder en la sociedad postindustrial, sin recurrir a posiciones políticas convencionales (izquierda, derecha). Cuestionar el concepto de propiedad intelectual y autoría individual en estos momentos es una posición política «estratégicamente» revolucionaria por cuanto puede, perfectamente, acelerar transformaciones profundas en el modo de producir y distribuir, en la manera de entender el concepto mismo de propiedad privada. En una economía libre de mercado, es decir, en el capitalismo, propiedad y producción han sido definidos conceptualmente hace más de dos siglos y, en la práctica, son las bases sobre las que se sustenta la acumulación privada de riqueza. Una parte de ella es conocimiento sustraído a lo social: ése es el frente de hacktivismo.

ckeo». 4. Persona que es buena programando de forma rápida. Experto en un programa en particular, o que realiza trabajo frecuentemente usando cierto programa; como en «es un hacker de UNIX». (Las definiciones 1 a 5 están correlacionadas, y la gente que encaja en ellas suele congregarse.) 6. Experto o entusiasta de cualquier tipo. Se puede ser un «hacker astrónomo», por ejemplo. 7. El que disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa. 8 [en desuso] Liante malicioso que intenta descubrir información sensible cotilleando por ahí. De ahí vienen «hacker de contraseñas» y «hacker de las redes». El término correcto en estos casos es «cracker».

El término «hacker» tiende a connotar participación como miembro en la comunidad global definida como «la Red». También implica que la persona descrita suele suscribir alguna versión de la

El hacklab y sus relaciones políticas: «porque el lab es político, creo que por definición, ¿no?»

(00:57:45) franz: cuéntame cosas sobre el hackmeeting... entre quiénes lo estáis organizando?

(00:58:14) Fitopaldi: bueno, pues como se diría en la lista del hackmeeting quien lo organiza es toda la lista

(00:59:07) Fitopaldi: fuera de Matrix, hay unas personas que se tienen que dedicar a la ardua tarea de buscar sitios, infraestructura, etc.

(00:59:46) Fitopaldi: por ahora lo está organizando Indymedia Sevilla, Hacklab Sevilla, CSOA Casas Viejas y otras personas a título individual [...]

(01:05:19) franz: oye, toda esta peña con la que estáis currando en Sevilla, os conocéis, sois amigos, os reunís en algún sitio?

(01:05:35) Fitopaldi: bueno...

(01:06:01) Fitopaldi: la mayoría empezamos a currar un poco antes de la contracumbre europea en Sevilla

(01:06:11) Fitopaldi: y nos conocemos desde entonces

(01:06:27) Fitopaldi: aquello fue una prueba de unificación de los MMSS en Sevilla

(01:06:54) Fitopaldi: y luego se unieron más gente que no estuvieron en la contracumbre

(01:07:03) Fitopaldi: algunos frikis y demás...

En Sevilla queda poco lugar para la duda acerca de si el Hacklab es un espacio en el que convergen activistas de diferentes redes o no. Fitopaldi lo expone sin ninguna dificultad: las entidades que organizaron el encuentro anual de hackers del Estado (Hackandalus, octubre del 2004[1]) son Indymedia Sevilla[2], el propio

1. La web oficial del evento se puede consultar en http://www.nodo50.org/hackandalus/ (visitada por última vez el 29 de junio del 2004).
2. Podríamos afirmar que Indymedia Sevilla es la plataforma comunicativa en Internet de buena parte de las redes sociales sevillanas que, en torno a La Casa de la Paz y el CSOA Casas Viejas, agrupan gran parte de la actividad política.

ética del hacker. Es mejor ser descrito como un hacker por otros que describirse uno mismo de ese modo. Los hackers se consideran a sí mismos algo así como una élite (en la que los méritos se basan en la habilidad), aunque suelen recibir amablemente a nuevos miembros. Por lo tanto, hay una parte de satisfacción del ego en considerarse a sí mismo un hacker (si dices ser uno y luego no lo eres, rápidamente te etiquetarán de falso).

***CRACKER** s. El que rompe la seguridad de un sistema. Acuñado hacia 1985 por hackers en su defensa, contra la utilización inapropiada por periodistas del término hacker (en su acepción número 8). Falló un intento anterior de establecer «gusano» en este sentido, en 1981-1982, en Usenet.*

Hacklab, el Centro Social Okupado y Autogestionado de Sevilla (Casas Viejas), y las personas implicadas ya han compartido experiencias militantes en el semestre europeo de la presidencia española de la UE (2002), en la que el Foro Social de Sevilla actuó como uno de los aglutinantes organizativos del movimiento antiglobalización[3]. El propio Foro puso en marcha un centro de medios telemáticos durante las jornadas de junio del 2002, del que surgió el grupo promotor de Indymedia en la capital andaluza y, posteriormente, el primer núcleo de hacktivistas. Tanto el espacio físico donde se reúnen los hackers en Sevilla como buena parte de los miembros del grupo se comparten con otras redes o plataformas, de forma que el hacklab se convierte en un área de producción tecnopolítica dentro del conjunto de áreas sobre las que trabajan las redes sociales y ciudadanas. Es, en la práctica, un nuevo espacio para la acción política de estas redes que cruzan acción y discurso con nuevos activistas que provienen de *lo técnico: «y luego se unieron más gente que no estuvieron en la contracumbre, algunos frikis y demás...»*.

En el IRC del Metabolik BioHacklab de Bilbao lanzamos una pregunta con la intención de profundizar en esta línea:

jun 24 00:28:18 <qw> creéis que todo lo que se mueve alrededor de los hacklabs es un movimiento con identidad propia o es una sección técnico/política de otros movimientos sociales?

jun 24 00:28:51 <anap> no es una sección

jun 24 00:28:59 <anap> es otra comunidad

jun 24 00:29:07 <anap> que intersecciona con otras comunidades

jun 24 00:29:24 <anap> al menos en londres y parte de europa, creo que incluido bilbo...

jun 24 00:29:32 <metis> hasta ahí de acuerdo con Ana

3. Sobre la Cumbre Alternativa de sevillana de junio del 2002 se puede consultar http://www.forosocialsevilla.org/ (visitada por última vez el 29 de junio del 2004).

La utilización de ambos neologismos refleja una fuerte repulsión contra el robo y vandalismo perpetrado por los círculos de crackers. Aunque se supone que cualquier hacker auténtico ha jugado con algún tipo de crackeo y conoce muchas de las técnicas básicas, se supone que cualquier que haya pasado la etapa larval ha desterrado el deseo de hacerlo con excepción de razones prácticas inmediatas (por ejemplo, si es necesario pasar por alto algún sistema de seguridad para completar algún tipo de trabajo).

Por lo tanto, hay mucho menos en común entre el mundo de los hackers y de los crackers de lo que el lector mundano, confundido por el periodismo sensacionalista, pueda suponer.

Los crackers tienden a agruparse en grupos pequeños, muy secretos y privados, que tienen poco que ver con la policultura abierta y enorme que se describe en este diccionario; aunque los crackers

jun 24 00:30:10 <zert> yo creo que casi todo hacker de dentro del movimiento de hacklabs es multimilitante

jun 24 00:30:15 <metis> pero recalcar que en cierto modo la propia comunidad es una «herramienta» (o crea herramientas) para el resto de comunidades

jun 24 00:30:24 <zert> cosa que choca frontalmente con los hackers «oldskool»[4]

jun 24 00:30:29 <zert> o crackers

jun 24 00:30:41 <zert> que «pasan de política»

jun 24 00:30:52 <anap> tambien de acuerdo con metis

[...]

jun 24 00:31:23 <qw> he conocido gente en hacklabs que ha tenido su primera experiencia politica a través de eso, del hacklab

jun 24 00:31:26 <anap> pero normalmente.. los hackers que pasan de política acaban empapándose si frecuentan mucho el lab

jun 24 00:31:47 <anap> porque el lab es político, creo que por definición, no?

jun 24 00:32:05 <metis> sí ana, en ese sentido de acuerdo (el lab es político)

jun 24 00:32:09 <anap> qw yo también he conocido gente así

jun 24 00:32:14 <metis> entre otras cosas porque el software libre es político

jun 24 00:32:20 <anap> sí

jun 24 00:32:30 <zert> anap los hackers de los que hablo no van a hacklabs

jun 24 00:32:36 <anap> ah vale

jun 24 00:32:45 <anap> sólo son crackers entonces

jun 24 00:32:46 <zert> van de hacker/cracker «con» s

4. «El término "oldskool" en cuanto a hacking se refiere más a gente como Kevin Mitnick que a gente como Richard Stallman, es decir, se refiere a crackers más que a hackers, aunque a los crackers les gusta llamarse hackers si se encargan de reventar sistemas telemáticos y crackers si se encargan de reventar programas. Para alguien "de la vieja escuela", un hacker es alguien que entra en el pentágono y modifica alguna web en plan de risa, y un cracker es alguien que consigue desproteger un programa para que no pida número de serie o licencia. Esto hace que haya bastante jaleo en cuanto a términos, porque lo que nosotros –hacklabs, etc.– consideramos hackers para ellos –oldskool– no es nada de eso, mientras que lo que ellos consideran hackers para nosotros son crackers». Zert (Txipi) en un mail en que aclara algunas inconsistencias mías en este trabajo (3-09-04).

a menudo se definen a sí mismos como hackers, la mayor parte de los auténticos hackers los consideran una forma de vida inferior.

Consideraciones éticas aparte, los hackers consideran que cualquiera que no sea capaz de imaginar una forma más interesante de jugar con su ordenador que romper los sistemas de alguien ha de ser bastante perdedor. Algunas de las otras razones por las que se mira con desprecio a los crackers se describen en las entradas sobre *cracking* y *phreaking* (crackers telefónicos). Ver también: samuráis, hackers del lado oscuro y la ética del hacker.

Una mujer, la almirante de la armada norteamericana Grace Hooper, es considerada el primer hacker de la era de la computación. Mientras ella trabajaba e investigaba en la computadora Mark I, durante la Segunda Guerra Mundial, fue la primera persona que aseguró que las computadoras no

jun 24 00:32:53 <zert> no, no tiene por qué

jun 24 00:33:16 <metis> simplemente son hackers «solo-hi-tech«

jun 24 00:33:24 <zert> mmmnnnn

jun 24 00:33:35 <qw> qué significa que algo sea «polltico»????

jun 24 00:33:50 <qw> por ejemplo el software libre

jun 24 00:33:56 <qw> o el hacking?

jun 24 00:33:58 <metis> sin darse cuenta (o sin querer darse cuenta) del valor que tienen sus conocimientos en una lucha social (o sin interesarse por una lucha social)

jun 24 00:34:14 <zert> metis su lucha es otra

jun 24 00:34:24 <zert> es la misma lucha que el investigador cientifico

jun 24 00:34:28 <zert> no política

jun 24 00:34:41 <zert> aunque bueno, yo no soy así

jun 24 00:34:49 <zert> y la gente del hacklab tampoco lo es

jun 24 00:35:06 <zert> la gente que hay en hacklabs que tienen el primer contacto con cosas sociales o políticas ahí

jun 24 00:35:12 <zert> al final acaban siendo multimilitantes

El *hacking* es político por definición y eso significa varias cosas al mismo tiempo. Primero, que la información que se gestiona, que se comparte o que se libera es necesaria e importante para «la lucha social». La comunidad está posicionada en un conflicto amplio en el que la posición compartida es la de «lucha» como (segunda) «herramienta para el resto de comunidades». El reconocimiento identitario y colectivo es claro y es lo primero que se enuncia. Anap es taxativa: *no somos una sección, somos una comunidad*, pero (matiza, inmediatamente, a continuación) «*trabajamos en un cruce de planos con otras comunidades*». Un tercer elemento que incluye el ejercicio de definición de la propia comunidad pasa por la delimitación del espacio de acción mediante la diferenciación respecto al otro: los hackers «oldskool» o los crakers[5] que «no van a hacklabs» y son sólo «hi-tech». En el espacio político definido en torno al hacklab,

solamente servían para fines bélicos, sino que además podrían ser muy útiles para diversos usos a favor de la humanidad. Ella creó un lenguaje de programación denominado FlowMatic y años después inventó nada menos que el famoso lenguaje COBOL.

En realidad, los hackers y su cultura del trabajo compartido y placentero, aunque duro, han sido fundamentales en el desarrollo de Internet. Fueron hackers académicos quienes diseñaron los protocolos de Internet. Un hacker, Ralph Tomlinson, trabajador de la empresa BBN, inventó el correo electrónico en 1970, para uso de los primeros internautas, sin comercialización alguna. Hackers de los Bell Laboratories y de la Universidad de Berkeley desarrollaron UNIX. Hackers estudiantes inventaron el módem. Las redes de comunicación electrónica inventaron los tablones de anuncio, los chats, las listas electrónicas y todas las aplicaciones que hoy estructuran Internet. Y Tim Berners-Lee y Roger

todo se incorpora al conflicto político, de forma que «*la gente que hay en hacklabs que tienen el primer contacto con cosas sociales o políticas al final acaban siendo multimilitantes*» (como ocurre en el caso de Towanda, de Madrid). El conjunto de elementos recrea un imaginario comunitario perfectamente coherente estructurado sobre la noción de un conflicto político amplio, en torno al cual se posiciona la comunidad junto a otras comunidades afines y respecto al cual la comunidad es capaz de diferenciarse de otras, aparentemente cercanas, pero políticamente distantes: los crackers.

En Sevilla la línea que diferencia el hacklab (hackers que organizan el hackmeeting de octubre del 2004) y los medioactivistas[6] de Indymedia Sevilla está poco definida, prácticamente desaparece y todo apunta a que en esa ciudad el trasvase de militantes entre diferentes redes sociales es algo asumido con naturalidad:

(01:09:12) ***Fitopaldi:*** *nos importa mucho la unión de red de personas*
(01:09:39) ***Fitopaldi:*** *por eso, nos reunimos cada semana como Indymedia o como hacklab, etc.*

Entre los hackers del Metabolik cuesta más llegar a esa conclusión:

jun 24 00:40:13 <qw> me da la impresión de que sin la gente de los hacklabs no habría indymedias... me equivoco?
jun 24 00:40:46 <anap> sí, qw, te equivocas
jun 24 00:40:46 <anap> MUCHO

5. Pau Contreras se aproxima desde la antropología a la identidad de los crakers. Se esfuerza por rescatar la dimensión política de un discurso (el de Kohfam), sin conseguirlo. Sobre la dimensión política de la actividad de los hackers, crakers y phreakers, sobre todo en lo referente a su batalla técnica y política contra el gobierno americano es imprescindible la obra de Steven Levy. Ver: Contreras, P. (2004) *Me llamo Kohfam. Identidad hacker: una aproximación antropológica* (Gedisa, ed. Barcelona) y Levy, S. (2002) *Cripto. Cómo los informáticos libertarios vencieron al gobierno y salvaron la intimidad en la era digital* (Alianza ed., Madrid).
6. Para acercarnos al concepto de mediactivismo como práctica comunicativa de los movimientos sociales se puede consultar *Mediactivismo. Estrategias y prácticas de la comunicación independiente. Mapa internacional y Manual de uso*, en http://www.sindominio.net/afe/dos_mediactivismo/.

Cailliau diseñaron el browser/editor World Wide Web, por la pasión de programar, a escondidas de sus jefes en el CERN de Ginebra, en 1990, y lo difundieron en la red sin derechos de propiedad a partir de 1991. También el browser que popularizó el uso del World Wide Web, el Mosaic, fue diseñado en la Universidad de Illinois por otros dos hackers (Marc Andreesen y Eric Bina) en 1992. Y la tradición continúa: en estos momentos, dos tercios de los servidores de web utilizan Apache, un programa servidor diseñado y mantenido en software abierto y sin derechos de propiedad por una red cooperativa.

En una palabra, los hackers informáticos han creado la base tecnológica de Internet, el medio de comunicación que constituye la infraestructura de la sociedad de la información. Y lo han hecho para su propio placer o, si se quiere, por el puro goce de crear y compartir la creación y la competición de la creación. Ciertamente, unos pocos de entre ellos también se hicieron ricos como empresa-

jun 24 00:40:59 <qw> porque?

jun 24 00:41:05 <anap> por Londres

jun 24 00:41:06 <metis> qw: yo pienso que son más o menos asíncronos, por lo que uno no ha podido depender del otro

jun 24 00:41:22 <anap> llevamos 4 anyos haciendo indymedia desde nuestras habitaciones

jun 24 00:41:37 <zert> en euskalherria no tienen casi nada que ver

jun 24 00:41:38 <meskalin> oye anap

jun 24 00:41:38 <anap> en mi caso, desde bibliotecas públicas y del college, durante un anyo o así

[...]

jun 24 00:49:31 <qw> una vez alguien de Euskalherria Indymedia me dijo que casi todo se lo debían al metabolik

jun 24 00:49:39 <qw> a nivel técnico claro

jun 24 00:50:08 <Moe_Bius> qw eso no es verdad, a nivel hacklab

jun 24 00:50:13 <anap> qw

jun 24 00:50:15 <zert> :O

jun 24 00:50:16 <Moe_Bius> no hemos hecho nada en indy EH

jun 24 00:50:19 <anap> un consejo...

jun 24 00:50:25 <zert> pues no se quién te lo dijo

jun 24 00:50:27 <anap> no vuelvas a hablar de «indymedias»

jun 24 00:50:29 <anap> en general

jun 24 00:50:31 <zert> pero menuda columpiada

jun 24 00:50:33 <zert> :DDDDD

jun 24 00:50:34 <anap> por que cada una es un mundo

jun 24 00:50:47 <zert> aunque bueno

jun 24 00:50:51 <zert> si somos muy estrictos

jun 24 00:51:04 <zert> los tech más trabajadores de Indymedia Euskalherria

rios, pero mediante aplicaciones de sus innovaciones, no mediante la apropiación de la innovación cooperativa en su propio beneficio (aunque el caso de Andreesen, de Netscape, es menos claro en este sentido). Otros obtuvieron buenos puestos de trabajo, pero sin ceder en sus principios como hackers. También hubo quien se hizo famoso, como Linus Torvalds, pero su fama le vino de su reconocimiento por la comunidad de hackers, que implica el respeto a sus reglas de libertad y cooperación. Los más permanecieron anónimos para el mundo y llevan y llevaron una vida modesta. Pero obtuvieron, mediante su práctica de innovación cooperativa, la más alta recompensa a la que aspira un hacker, el reconocimiento como tal por parte de la única autoridad que puede otorgar dicha distinción: la comunidad global de hackers, fuente esencial de innovación en la era de la información.

jun 24 00:51:07 <zert> son de metabolik

jun 24 00:51:09 <Moe_Bius> otra cosa es que haya gente en el grupo tech de indymedia Euskalherria que este tmb en Metabolik, y no son muchos

jun 24 00:51:14 <zert> pero como multimilitancia

jun 24 00:51:25 <zert> pero indymedia dentro de metabolik

jun 24 00:51:30 <zert> es residual totalmente

jun 24 00:51:41 <anap> zert, Moe_Bius, y como espacio físico?

jun 24 00:51:50 <Moe_Bius> anap: menos aún

jun 24 00:51:56 <anap> ah ok

jun 24 00:51:56 <zert> ya te digo: DDDDDD

jun 24 00:52:00 <anap> pos como en londres

jun 24 00:52:08 <anap> también hay gente de indy en el hacklab

[...]

jun 24 01:10:30 <metis> oye, reflexión personal

jun 24 01:10:31 <anap> por una parte evolución personal

jun 24 01:10:37 <anap> sí, sí, la mía también

jun 24 01:10:54 <anap> por otra, sí que parece lógica una colaboración entre hacklab e indymedia

jun 24 01:11:08 <qw> por qué?

jun 24 01:12:05 <metis> a mí se me ocurre que el formato de indymedia está íntimamente ligado a los hacklabs (bueno, a la tech en general)

Este bloque es (desde el punto de vista discursivo) circular. La pregunta moviliza (provoca) con la idea de forzar la reflexión. A las 24:00:40 Anap niega el peso de los hackers en el inicio del nodo de Indymedia en Euskalherria. Para Moe_Bius nos «columpiamos». Diez segundos después ya se matiza: «*bueno los tech mas trabajadores de Indymedia Euskalherria son del Metabolik*». El bucle se cierra a un minuto y doce segundos del planteamiento de la pregunta, reconociendo la coin-

cidencia de formatos entre ambos proyectos. La opinión que se lanza es real, y la hizo pública en su momento una persona totalmente volcada en la puesta en marcha del proyecto de comunicación. Con independencia de lo matizable de la magnitud del peso de los hackers en el diseño técnico del Indymedia Euskalherria, lo cierto es que queda patente que, como en Sevilla, ese cruce de comunidades es real y no se basa tanto en acuerdos programáticos o formales entre ambos proyectos, sino en la doble militancia, el trasvase de conocimiento y en las redes de afinidad política y personal.

Los activistas y sus experiencias militantes: «*quizás la esperanza esté en las máquinas...* :-DD»

(01:07:27) ***Fitopaldi:*** *es decir, aunque la mayoría tenemos antecedentes de trabajo político*

(01:07:48) ***Fitopaldi:*** *al montar un hacklab te puedes encontrar con personas que no necesariamente compartan un curro político*

(01:08:04) ***Fitopaldi:*** *sino sólo la pasión por la tecnología y su funcionamiento*

El hacklab es también, y por lo tanto se vincula claramente a las prácticas iniciáticas del resto de movimientos sociales contemporáneos, espacio para las primeras experiencias de socialización política de activistas que, en algunos casos más que en otros, verán redimensionada su *pasión por lo técnico* hacia su compromiso con agendas políticas bien definidas:

Towanda: *Sí, vamos, pero a nivel político... un centro donde confluyen muchas cosas distintas, y entonces también al haber tenido relación... vamos, que mi vida como activista antes del hacklab había sido prácticamente nula. Vamos, el ver, estar en contacto con gente que montó colectivos o que monta distintas campañas o distintas historias... vamos, el ver qué es lo que funciona, qué es lo que no, cómo se organiza la gente... para mí eso ha sido muy instructivo...*

Coa es el paradigma de la *multimilitancia*. Las redes sociales de su barrio comparten activistas o bien se desdoblan en múltiples iniciativas.

(01:38:26) franz: aparte del Cielito Lindo, eres activa en algún otro movimiento social?

(01:39:00) ***Coa:*** *pues ahora...estoy casi retirada de todo... por aburrimiento*

(01:39:12) ***Coa:*** *pero digamos que sigo de cerca los temas del barrio*

(01:39:21) franz: Lavapies?

(01:39:25) ***Coa:*** *sip*

(01:39:35) franz: qué se cuece en el barrio?

(01:39:49) ***Coa:*** *pues sinceramente poca cosa...*

(01:39:53) ***Coa:*** *bueno igual soy un poco mala*

(01:40:08) ***Coa:*** *porque se está trabajando el tema de la vivienda en una mesa de vivienda*

(01:40:23) **Coa:** *okupasa... quiere generar planteamientos nuevos con el tema de la okupación*

(01:40:51) **Coa:** *lavapiés wireless sigue amenazando con la instalación de multitud de nodos*

(01:41:12) **Coa:** *karakolas y biblio pelean por su okupa*

(01:41:39) **Coa:** *y se reivindica la tabacalera como espacio social para el barrio*

(01:41:50) **Coa:** *pero lo mejor es el cine de verano que hay los viernes en el solar*

Ese tipo (y ritmo) de militancia acaban teniendo algún tipo de consecuencia práctica:

(01:42:33) **Coa:** *sí... pero la sensacion que me llega de todo ello es que se está activo porque sí*

(01:42:55) **Coa:** *han pasado muchas cosas y no se ha sido capaz de plantear una crítica hacia dentro*

(01:43:11) **Coa:** *parece que todo va bien... y... seguimos*

(01:43:29) **Coa:** *pero muchas cosas han pasado... de esas que sólo se comentan en los bares, en las cañas*

(01:43:41) **Coa:** *y creo que debería darse la reflexión colectiva*

(01:43:59) **Coa:** *pero las críticas no sabemos hablarlas...*

(01:44:05) **Coa:** *quizá aprendamos... algún día*

(01:44:23) **Coa:** *no noto ilusión... sino deber*

(01:44:55) **Coa:** *las gentes que se ven casi siempre son las mismas... o las que llevan las voz cantante...*

(01:45:04) **Coa:** *y eso es siginificativo... al menos para mí*

(01:45:31) franz: te veo un poco desencatada del mundo material?

(01:45:44) **Coa:** *pues sí... la verdad es que sí...*

(01:45:52) **Coa:** *pero no pierdo la esperanza :-)*

(01:46:07) **Coa:** *quiza la esperanza esté en las máquinas...*:-DD

Un nuevo ámbito para el activismo, menos rígido en lo político, menos exigente en cuanto a lo presencial, estructurado en torno a la producción intelectual y la difusión de conocimiento, se presenta como refugio para activistas desgastados por años de hiperactivismo y entrega física:

(01:49:45) franz: qué cosas del ciberespacio te bajarías al mundo material para mejorarlo?

(01:49:51) **Coa:** *y como le comentaba a una amiga*

(01:50:03) **Coa:** *en el 11M me sentí más sola en la calle que delante de la máquina*

(01:50:22) **Coa:** *(porque parte de mi gente estaba en el jabber y podía saber cómo estaba)*

(01:50:45) **Coa:** *al principio pense qué triste que sea así... y luego pensé ¿por qué triste?*

(01:51:12) **Coa:** *uyyyy... qué pregunta más difícil*

(01:51:39) franz: :-/

(01:51:44) **Coa:** *no sé... son mundos distintos... no sé si se acoplan el uno al otro*

(01:51:58) **Coa:** *quizás la libertad para expresarse*

(01:52:10) **Coa:** *independientemente de quién lo dice...*

(01:52:50) **Coa:** *al final no se quién va a contaminar a quién*

(01:52:59) **Coa:** *si el mundo real al cibernético o al revés*

(01:53:10) **Coa:** *quizás ambos hagan una simbiosis*

El perfil de Coa es especialmente interesante. Activa en diversas redes y plataformas, comparte militancia entre el hacking y los movimientos por la vivienda en el barrio de Lavapiés. Coa, da el salto desde las redes sociales a las telemáticas en la medida en que incorpora el plano de la conflictividad en torno a la producción, propiedad y distribución de información (en buena medida, el hacking se puede definir de esta forma) al conjunto de ejes que han estructurado su vida militante en el barrio en que vive. Reacia a encasillamientos políticos tradicionales, es perfectamente consciente del cambio de paradigma (técnico y político) que permite acercarse a las nuevas formas de supervivencia en las metrópolis postindustriales.

Concluimos

«... se me iba la mente a la gran batalla contra la ciudad de Matrix, Sion, cuando aparecen los monstruos aquellos que parecen pulpos y empiezan a machacar. El poli cortando la chapa, los derribos de paredes, la gente tratada cruelmente. Sin compasión. Parece Matrix.»
Merce, sobre el desalojo del Gaztetxe okupado de Iruña, en *hackmeeting@listas.sindominio.net*

Estamos ante una constelación de experiencias y prácticas comunes, un conjunto de proyectos independientes; ante un tipo especifico de hacker, militante político en el plano de la tecnología que se empeña en desvelar las implicaciones sociales de lo técnico, la articulación de nuevos modos de comunicación; que se entrelaza en un movimiento de escala estatal y en relación con proyectos europeos, dueños de un discurso a medias propio a medias compartido con otros movimientos autónomos anticapitalistas con los que gestionan espacios e imaginario, modelos de transformación social y cambio tecnológico. Movimiento social, al fin y al cabo, que atravesado por otros movimientos rompe con las limitaciones estrictas de lo reivindicativo y se inserta en un proyecto de cambio social en el sentido mas amplio que podamos imaginarnos: el sentido de los movimientos urbanos que desde los disturbios de Seattle se coordinan a nivel planetario contra la globalización capitalista, reclamando otro uso y otra manera de vivir lo técnico y lo político[7].

7. Roig, G. y Sádaba, I. : «Internet, nuevos escenarios, nuevos sujetos, nuevos conflictos», en Aparici, R. y Marí, V. (2003) *Cultura popular, industrias culturales y ciberespacio*. UNED, Madrid.

SEGURIDAD / EE.UU.

ESCUELA DE «HACKERS» PARA LUCHAR CONTRA LOS «CRACKERS»

ELMUNDO.ES / REUTERS

MADRID / LOS ÁNGELES (EE.UU.).–
Con sus largas patillas, una espesa barba de chivo y una gorra negra de béisbol, Ralph Echemendia imparte unas clases muy particulares a un total de 15 disciplinados líderes corporativos, académicos y militares. La asignatura: «Piratería Cibernética». No obstante, parece que aún confunden los términos «hacker» y «cracker»...

En este caso, los estudiantes, muy atentos a sus portátiles, pagan aproximadamente 4.000 dólares cada uno por asistir al «Hacker College», que funciona en el Mt. Sierra College, un centro universitario del área de Los Ángeles. Este centro docente está diseñado para mostrar cómo buscar vulnerabilidades y cómo se pueden violar ciertos sistemas informáticos, informa el corresposal de Reuters Ben Berkowitz.

«Es emocionante ver lo inseguras que son las grandes corporaciones», asegura Echemendia durante un intervalo del seminario (de una semana de duración). «Es emocionante por lo fácil que es».

Se cree que los «hackers» malintecionados, o «crackers», causan a los negocios mundiales pérdidas valoradas en miles de millones de dólares al año, y los costes por defenderse de ellos se están disparando.

Un reciente estudio de Good Harbor Consulting muestra que la seguridad representa ahora hasta el 12% de los presupuestos corporativos, cuando hace cinco años representaba un 3%.

«Esto es definitivamente algo que desangra, a veces tanto que es aterrador», asegura Loren Shirk, una estudiante de este curioso «curso sobre piratería» que posee una compañía de consultoría de computación para negocios pequeños.

«Pirata Ético Certificado»
El curso prepara a los estudiantes para un examen en el Consejo Internacional de Consultores de Comercio Electrónico, o EC-Council. Si lo aprueban, obtienen un título de nombre un tanto grotesco: «Pirata Ético Certificado».

La clase no es nada fácil. Los instructores tocan temas como *criptografía simétrica versus criptografía asimétrica* (la simétrica es mas rápida), o asignaturas sobre puertos y servicios TCP (¡cuidado con cualquier actividad en el puerto 0!). Y esto es sólo la teoría.

«Definitivamente puedo decir que no es para cualquiera», comenta Ben Sookying, director de servicios de seguridad de redes del sistema de 23 campus de la Universidad del Estado de California y estudiante en el curso. «Si uno no tiene disciplina, no pasa el curso».

Pero el trabajo es práctico, también. El primer día, los estudiantes reciben instrucción sobre métodos básicos, gratuitos y legales de búsqueda *on-line*, especialmente relacionados con motores de búsqueda y bases de datos, para obtener la mayor cantidad posible de información sobre compañías, sus cargos ejecutivos y, cómo no, sus sistemas.

Con relativamente poco esfuerzo, descubrieron que el presidente ejecutivo de una compañía pública tenía su propio sitio «web» dedicado a las guitarras, mientras otra empresa, también pública, usa todavía sistemas famosos por ser fácilmente atacables.

Todo un negocio

Intense School

Desde los ataques terroristas del 11 de septiembre de 2001, la compañía se dedicó cada vez más a dar cursos sobre seguridad cibernética. Ahora ofrece unos 200 cursos al año, con los que obtiene ingresos anuales de unos 15 millones de dólares. Parece un negocio redondo.

«Lo que intentamos hacer en nuestras clases es enseñar cómo piensan los "crackers"», dijo Dave Kaufman, presidente de Intense School. La única forma de mantenerlos fuera de los sistemas de las grandes corporaciones es, por tanto, saber cómo podrían ser atacados.

El hacklab, como espacio físico y como comunidad de activistas podría ser la intersección booleana (no la suma) de tres conjuntos de activistas, la superposición de tres planos en la que confluyen y cristalizan parte de los discursos y partes de sus recursos personales: 1) los Centros Sociales Okupados (movimiento okupa), 2) los dispositivos de comunicación del movimiento antiglobalización (los diferentes nodos de Indymedia), y 3) la vieja cultura hacker, de la que se hereda el perfil más estrictamente «high-tech», las dinámicas de los viejos hackers del MIT y del movimiento social y político que inicia la Free Software Foundation[8] de Richard Stallman. Respecto a este último plano, en nuestro Estado podríamos hablar del «lobby» del software libre que se estructura en torno a Hispalinux, en forma de asociación, y que desde 1997 agrupa a varios miles de usuarios y entusiastas del sistema operativo GNU/Linux. Su trabajo de *lobby* ha conseguido, por un lado, poner en pie y cohesionar una comunidad de técnicos y especialistas como base de la solvencia técnica del sistema operativo y el software libre en el mundo hispano. Esta labor se desdobla en dos líneas de intervención: la de la ampliación permanente de la comunidad de usuarios y activistas y, por otro, la presión y el trabajo de sensibilización hacia la administración y empresa privada, a la que se pretende sustraer del ámbito de influencia y de las relaciones de sometimiento y dependencia tecnológica que ha impuesto la tecnología propietaria y muy específicamente Microsoft. Proyectos de traducción de documentación técnica libre al castellano (El Proyecto Lucas), sindicación de iniciativas de desarrollo de software libre (Software-Libre.org) o congresos son el tipo de iniciativas que parten desde la comunidad con la idea de articular un movimiento social que atraviese planos de lo social, lo administrativo y lo empresarial a favor del software libre y otra concepción acerca de la producción y gestión social de conocimiento[9].

Pero el *hacking* y los hackers de los *hacklabs* van más allá. Organizados y declaradamente políticos, se articulan como comunidad en un punto de cruce entre varios movimientos (punto de confluencia que no es simple suma o agregación, sino una expresión política nueva), lo que les permite, por una parte, reconocerse como movimiento diferenciado (en relación a un discurso y unos recursos políticos propios, un imaginario y unos referentes simbólicos y político-literarios específicos), y al tiempo sentirse parte (o herramienta) de otras comunidades o redes sociales. La red del *hacking* no puede diferenciarse plenamente de las iniciativas de comunicación de las plataformas antiglobalización, con la que comparten técnicos, incluso en alguna ciudad se confunden (Sevilla); de la misma manera que los espacios físicos de la actividad del hacklab y los hackmeetings no están en absoluto delimitados respecto a algunos Centros Sociales Okupados. Allí donde hay centros sociales estables, los hacklabs tienden, de forma natural, a compartir espacios, infraestructuras técnicas e iniciativas políticas. En la lista de coordinación de los hackmeetings suelen dar charlas animadas (en algún caso con una alta implicación afectiva) acerca de los recurrentes desalojos de centros okupados. En algunos de ellos, como el Laboratorio de Madrid o el Gaztetxe de Iruña, se

8. http://www.fsf.org.
9. http://www.hispalinux.es/.

han celebrado varios encuentros estatales. Si bien los grados de implicación varían, lo que ocurre en el movimiento de okupación es algo que toca muy de cerca:

> *...estaba pensando... no sé nada de teoría, práctica o historia del movimiento okupa, aunque sin él habría sido imposible hacer el hackmeeting. Desde esta vinculación, me permito unos pensamientos, sin animo de ofender y con la intención de que no estéis tristes. [...] Si las casas okupas se mantuviesen para siempre, el movimiento se iría aletargando, perdería energía, se solidificaría. En cambio, la desokupación —soy atrevida y primaria diciendo esto, pero ahí va— es lo que da sentido al movimiento, porque convierte su meta en inalcanzable. No estéis tristes, pues os habéis hecho más fuertes y la utopía continúa, la luz está aún allí. Propongo, en el hackmeeting, hacer algún tipo de duelo por las sedes del hackmeeting que ya no existen, porque fueron lugares preciosos y disfrutamos estando en ellos, y que quede el buen recuerdo.*[10]

Lo que da pie, en algún momento, a la intervención de activistas que dejan constancia, relatando en primera persona, el origen de los primeros hackmeetings estrechamente vinculados a los Centros Sociales Okupados:

> *...hacía tiempo que tenía metida en la cabeza la idea de una reunión pública de hackers, y a cada hacker que conocía y pensaba que podría hacerlo le comentaba la idea. Nadie se mostró dispuesto a ponerse manos a la obra. Hasta que, en el segundo hackmeeting italiano, conocí a roxu, adolfo y companyía. Hablamos de que sería guapo hacer algo así aquí. Cuando volvimos, lo comenté con la gente de Fronteras Electrónicas, quienes dieron su apoyo moral, pero del material se encargo roxu y companyía. Ellos dieron el contacto con los okupas de Barcelona, que se portaron divinamente. Había uno con barba y una pareja que curraron tanto!*[11]

La reflexión ya la hemos hecho en otro sitio. Sólo hay que traerla para ir cerrando las conclusiones:

> *En este universo conceptual se estructura el puente sobre el que desde el movimiento de okupación se trasvasan inquietudes, militancias, conocimientos, infraestructuras hacia ese nuevo espacio de hacktivismo político que traduce a la esfera de la producción inmaterial, a la generación de conocimiento social, el imaginario político de un movimiento que le precede y que cuestiona radicalmente relaciones de producción, de propiedad y de mando en el mundo material. El tránsito de okupas a hackers podría*

10. Publicado en hackmeeting@listas.sindominio.net. Date: Tue, 17 Aug 2004 19:35:36 +0200. From: merce aaa@xxx.es. To: hackmeeting@listas.sindominio.net. Subject: Re[2]: [hackmeeting] el gaztexte de iruña en pleno desalojo...
11. Publicado en hackmeeting@listas.sindominio.net. Date: Tue, 17 Aug 2004 23:23:39 +0200. From: merce aaa@xxx.es. Cc: hackmeeting@listas.sindominio.net. Subject: Re[2]: [hackmeeting] el gaztexte de iruña en pleno desalojo...

entenderse como la proyección hacia el ciberespacio de un movimiento insurgente, de corte radicalmente contracultural y subversivo, que se define en el rechazo y la superación de las relaciones sociales de dominación que imperan en las calles y se imponen en las redes.[12]

En una crítica acelerada a las consecuencias posibles del cambio tecnológico, Gibson nos describe en 1982 *La Matriz* (*The Matrix*) y el ciberespacio como un territorio de alucinación colectiva. Ahora los hackers del Metabolik teorizan acerca del código abierto, las distribuciones de GNU/Linux para activistas y el cambio social. Mediante la acción, hackers y activistas urbanos de las redes anticapitalistas han resuelto la esquizoide contradicción que la izquierda arrastra desde el siglo XIX sobre la tecnología y el mando: ¿es un instrumento de liberación o la nueva ideología que nos disciplina y atenaza a la cadena de montaje? ¿Debemos entregarnos a la dinámica de la historia fascinados por la idea de progreso o resistirnos con los amigos de Ludd[13] a la dominación tecnológica? La alucinación ciberpunk abrió paso al conflicto político. Hackers y activistas sociales han impuesto una práctica tecnopolítica en algunos ámbitos de la militancia urbana, que dispara contra la línea de flotación del modo de pensar y producir en el capitalismo postindustrial. Ése es el viaje del *hacking* y parte de la historia del ciberespacio.

Anexo metodológico sobre las entrevistas

Los fragmentos de las entrevistas hechas por medios telemáticos (Jabber, Messenger e IRC) se han insertado con casi ninguna modificación, respetando la gramática, la sintaxis y la ortografía.

Ficha de l@s entrevistad@s:

Towanda (seudónimo). 29 años, varón. Entrevista realizada en su casa, el 10 de mayo de 2004. Grabada y transcrita. Pertenece al Hacklab Cielito Lindo de Madrid y a Sindominio. El hacktivismo es su primera experiencia política clara y consciente. Abandonó la carrera de Físicas. Completó un Módulo de Informática de Formación Profesional. Ha trabajado como desarrollador de software para Internet en un banco y en la actualidad es Administrador de Sistemas de la sección española de una gran ONG. La entrevista duró 29'.

Fitopaldi. 22 años, varón. Entrevista realizada por Messenger, el 8 de junio de 2004. Pertenece al núcleo de gente que organizó el hackmeeting de Sevilla de octubre de 2004. Es miembro de Indymedia Estrecho, de Nodo50, del área telemática de La Casa de la Paz. Es Técnico Superior en Desarrollo de Aplicaciones Informáticas. Estudia 1º de Ingeniería Informática. Trabaja como programador de

12. Roig, G. y Sádaba, I. (2004) «El movimiento de okupación ante las nuevas tecnologías. Okupas en las redes», en Adell, R. y Martínez, M.: *¿Dónde están las llaves? El movimiento okupa, prácticas y contextos sociales*. Libros de la Catarata. Madrid.
13. *Crítica del nuevo mundo feliz que se avecina. Una entrevista a Los Amigos de Ludd*. http://es.geocities.com/anticivilizacion/amigosdeludd_crítica_mundo_feliz.htm (visitada el 20-08-04).

aplicaciones de Internet (free-lance) en varios periódicos digitales. La entrevista duró 89'. (*Franz* es Gustavo Roig.)

Coa (seudónimo). 30 años, mujer. Entrevista realizada por Jabber el 18 de junio del 2004. Pertenece al Hacklab Cielito Lindo de Madrid. Formó parte de Indymedia Madrid. Activa en varias redes sociales del barrio de Lavapiés. Estudió Filosofía y trabaja esporádicamente como traductora o programadora. La entrevista duró 137'. (*Franz* es Gustavo Roig.)

Entrevista colectiva en canal #metabolik del IRC (Chat) irc.freenode.net, realizada el 24 de junio del 2004. Participan entre otros y otras Anap, miembro del FreedomLab de Londres e Indymedia; Zert (Txipi), colaborador técnico de Indymedia Euskalherria y miembro del Metabolik BioHackLab; y Metis, también miembro de Metabolik. La entrevista duró 62'. (*Qw* es Gustavo Roig.)

LAS ZAPATILLAS PERSONALIZADAS DEL SR. PERETTI

UNA AVENTURA MEDIÁTICA CON NIKE

Uno de los sitios web de Nike (nikeid.com) permite a los consumidores residentes en los EEUU de América adquirir zapatillas personalizadas eligiendo los colorines de las suelas, las lengüetas, los airbags y los cordoncillos, añadiendo, además, una palabra que a modo de eslogan personal testimonie el interés de Nike por defender el derecho de sus clientes a expresarse libremente y a ser como son. Uno de estos ciberclientes «no pudo evitar acordarse de la gente que trabaja en las maquiladoras» y las fábricas inmundas de Asia y América Latina haciendo estas zapatillas, y como desafío a Nike pidió a la empresa que le hiciera unas zapatillas que llevaran el lema «Sweatshop» (la palabra inglesa para «maquiladora» referida a las fábricas habitualmente instaladas en países subdesarrollados en los que con salarios miserables y condiciones de trabajo pésimas se componen las piezas de nuestro sistema de consumo: ropa, calzado, componentes electrónicos o de telefonía, etc.). Nike rechazó la petición del cliente y así se generó esta curiosa correspondencia:

Nikeid.com:

Tu encargo de identificación personal Nike fue cancelado por uno o más de los motivos siguientes:

1) Tu identificación personal contiene la marca registrada u otra propiedad intelectual de otra empresa.
2) Tu identificación personal contiene el nombre de un/a deportista o equipo sobre cuyo uso no tenemos derecho legal.
3) Tu identificación personal fue dejada en blanco. ¿Es que no quieres que te los personalicemos?
4) Tu identificación personal contiene argot inapropiado, y entonces tu madre nos abofetearía. Si quieres encargarnos tu producto Nike con otra personalización distinta, por favor visítanos de nuevo en www.nike.com.

Gracias, Nike iD.

Respuesta de Jonah:

Mi encargo fue cancelado pero mi identificación personal no viola ninguno de los criterios enumerados en tu mensaje. La identificación personal de mis zapatos deportivos personalizados modelo ZOOM XC USA consiste en la palabra «sweatshop». Sweatshop no es:

1) marca registrada de otra empresa
2) nombre de un/a deportista
3) dejado en blanco
4) argot inapropiado.

Elegí esa palabra porque quise recordar el trabajo y esfuerzo de los niños y niñas que fabricaron mis zapatos.

Por favor, ¿podrían enviármelos de inmediato?

Gracias y Feliz Año Nuevo, Jonah Peretti.

Nueva respuesta de Nike:

Estimado cliente de Nike:

Tu encargo Nike fue cancelado porque la identificación personal que elegiste contiene, tal y como especificábamos en nuestro correo anterior, «argot inapropiado». Si quieres encargarnos tu producto Nike con otra personalización distinta, por favor visítanos de nuevo en www.nike.com.

Gracias, Nike iD.

Respuesta de Jonah:

Estimado Nike iD.

Gracias por su rápida respuesta a mi solicitud sobre mis zapatos deportivos personalizados ZOOM XC USA. Aunque les felicito por su puntual servicio al cliente, no estoy de acuerdo con su afirmación de que mi identificación personal sea argot inapropiado. Tras consultar el diccionario Webster, descubrí que de hecho la palabra «sweatshop» forma parte del inglés estándar, y no de ningún argot, la cual significa: «tienda o fábrica donde se contrata a trabajadores por largas horas a sueldos bajos y bajo condiciones insalubres» y data de 1892.

Por tanto, mi identificación personal coincide con los criterios de aceptación según se explicaba en el primer correo de NikeiD.

En su página web, Nike anuncia que su campaña «Nike iD» trata de «la libertad de elegir y la libertad de expresar quién eres». Comparto con Nike el amor por la libertad y la afirmación personal. En ella también se dice: «Si lo quieres bien hecho, hazlo tu mismo». Es emocionante poderme hacer mis propios zapatos y ofrecí mi identificación personal como una pequeña propina de aprecio por las obreras y los obreros explotados y a mi disposición para ayudarme a realizar mi sueño.

Espero de ustedes que valoren mi libertad de expresión y reconsideren su decisión de rechazar mi encargo.

Gracias, Jonah Peretti.

Contestación de Nike:

Estimado cliente de Nike iD:

De acuerdo a las normas de personalización, también se afirma en la página web de Nike iD que «Nike se reserva el derecho de cancelar cualquier identificación personal en las 24 horas después de la solicitud».

Asimismo, se añade: «Aunque aceptamos la mayoría de las identificaciones personales, no podemos aceptarlas todas. Algunas pueden ser (o contener) otras marcas, o el nombre de equipos deportivos, deportistas o personas famosas sobre cuyo uso Nike no tiene los derechos

necesarios. Otras pueden contener mensajes que consideramos inapropiados o que simplemente no queremos emplazar en nuestros productos. Desafortunadamente, a veces ello nos obliga a rechazar identificaciones personales que de otra forma podrían parecer inaceptables. En todo caso, te informaremos si tu identificación personal es rechazada y te ofreceremos la posibilidad de solicitar otra». Teniendo en cuenta estas normas, no podemos aceptar como solicitado tu encargo. Si quieres encargarnos tu producto Nike con otra personalización distinta, por favor visítanos de nuevo en www.nike.com.

Gracias, Nike iD.

Respuesta de Jonah:

Gracias por el tiempo y la energía que han dedicado a mi petición. He decidido encargar mis zapatos con una identificación personal distinta, pero querría hacerles una pequeña petición. ¿Podrían enviarme una instantánea a color de la niña vietnamita de diez años que fabricó mis zapatos?

Gracias, Jonah Peretti.

(La empresa interrumpió aquí la correspondencia)

A mediados de enero, envié estos mensajes a una docena de amigos y en poco tiempo recorrió todo el Internet, y llegó a millones y millones de personas sin que yo participara en esa circulación. El adversario de Nike era ahora un grupo amorfo de consumidores indignados conectados a una red descentralizada de correos electrónicos. Aunque la prensa ha presentado la historia en plan David contra Goliat, sería más acertado pensar que en los tiempos de las grandes compañías y sus departamentos de relaciones públicas y comunicación sólo se puede pensar en «davids» colectivos constituidos en base a redes descentralizadas de ciudadanos que sólo cuentan con «micromedios», como los e-mails precisamente, baratos a más no poder y que pueden alcanzar a números increíblemente altos de personas, especialmente si se combinan con la circulación en sitios como Slashdot.org o Indymedia, que tienden a borrar las fronteras entre editores y lectores, y que finalmente llevaron el caso de mi correspondencia con Nike a los principales medios de comunicación convencionales...

P2P

Manuel Campos
(manu@sindominio.net)

Al Principio...

«La introducción ampliamente difundida de las redes significará nuevos problemas sociales, éticos y políticos.»
Laudon, 1995

La Internet ideada a finales de los años sesenta era mucho más distribuida, descentralizada y simétrica de lo que lo es ahora. En sus orígenes, fue diseñada por militares que buscaban crear una red de comunicaciones capaz de resistir una guerra nuclear. Si un nodo de la red tiene un papel crucial, y se destruye ese nodo, se destruye la red. La solución consistía en conseguir una red robusta a base de descentralización.

> *¿Cómo sería controlada esa red? Cualquier autoridad central, cualquier núcleo de red centralizado sería un objetivo obvio e inmediato para un misil enemigo. El centro de la red sería el primer lugar a derribar... En primer lugar, la red «no tendría autoridad central». Además, sería «diseñada desde el principio para operar incluso hecha pedazos».*[1]

Como hemos visto en los capítulos precedentes, cuando esta red empezó a coger forma, en diciembre de 1969, se llamó ARPANET, y estaba compuesta por cuatro nodos que entonces se consideraban superordenadores de alta velocidad. El objetivo de ARPANET era que los ordenadores conectados pudieran compartir recursos a lo largo de los Estados Unidos.

1. Bruce Sterling, lo explica en su artículo «Pequeña historia de Internet»: http://sindominio.net/biblioweb/telematica/hist_internet.html.

EL PROYECTO SETI@home

«El paradigma p2p tiene tanto una parte humana como una técnica: desplaza el poder, y por lo tanto el control, de las organizaciones a las personas.»
David Anderson, SETI@home

En 1995, David Anderson, David Gedye, Woody Sullivan y Dan Werthimer se reunieron para hablar de una idea disparatada. Se trataba de usar la capacidad de procesamiento de los PCs domésticos para buscar señales de radio de civilizaciones extraterrestres. Y se lo tomaron en serio. Consideraron que la tecnología existente era suficiente, aunque fuera por los pelos, para grabar datos de radio y

Para poder hacer esto, era necesario crear una infraestructura que pudiera integrar todas las redes existentes, y que permitiría que cada ordenador participara por igual, sin que ninguno tuviera un papel prioritario. Los primeros ordenadores en ARPANET eran ordenadores independientes con la misma importancia. ARPANET los conectó a todos juntos como nodos iguales. El desafío era cómo diseñar la red para que pudiera funcionar sin que ningún nodo tuviera un papel principal.

> *Los principios eran simples. Se asumiría que una red era poco fiable en cualquier momento. Se diseñaría para trascender su propia falta de eficacia. Todos los nodos en la red serían iguales entre sí, cada nodo con autoridad para crear, pasar y recibir mensajes. Los mensajes se dividirían en paquetes, cada paquete dirigido por separado. Cada paquete saldría de un nodo fuente específico y terminaría en un nodo destino. Cada paquete recorrería la red según unos principios particulares. La ruta que tome cada paquete no tendría importancia. Sólo contarían los resultados finales.*

Así, Internet en sus principios era mucho mas abierta y libre de lo que lo es hoy. Prácticamente, cualquier maquina conectada era capaz de establecer una conexión con otra. La red estaba poblada por técnicos, científicos e investigadores que cooperaban entre ellos y compartían información, sin necesitar ningún tipo de protección los unos de los otros. Era una autentica utopía de investigadores y académicos.

Las primeras aplicaciones de Internet, FTP y Telnet, funcionaban de forma mucho más distribuida. Estas aplicaciones tienen un diseño cliente/servidor; esto significa que la aplicación tiene dos partes: el cliente, que pide un servicio, y el servidor, que ofrece un servicio. Por ejemplo, un navegador web (cliente) se conecta a un servidor web y le pide una página, y el servidor web se la envía. A pesar de

distribuirlos por Internet. Y se plantearon que si consiguieran 100.000 personas participando, la potencia de computación resultante les permitiría buscar más señales y más tipos de señales que lo que nunca antes había conseguido nadie.

SETI es un proyecto de investigación científica, cuyo objetivo es la búsqueda de vida inteligente fuera de la Tierra. En 1959, Phil Morrison y Giuseppe Cocconi propusieron escuchar señales de frecuencias de banda estrecha, el mismo tipo de señales que emiten las televisiones y los radares, pero distintas del ruido que emana de las estrellas y otras fuentes naturales. Dichas señales serían una evidencia de tecnología y, por tanto, de vida.

La mayoría de los proyectos SETI tiene superordenadores dedicados a buscar este tipo de señales, pero que están limitados a estos cálculos.

que este esquema no es muy simétrico (una parte pide un servicio, y la otra lo ofrece), la cosa se igualaba por que cada máquina actuaba como servidor a la vez que como cliente. Esto significa que desde cualquier ordenador se podía publicar/ofrecer información (paginas web, archivos ftp, etc.).

Pero a partir de 1994, Internet empezó a crecer de forma explosiva. Este crecimiento tan desbordante cambió el diseño de Internet de una utopía *geek* a un medio de masas. Millones de personas entraron en la red. Apareció un nuevo tipo de gente que estaba interesada en Internet como una herramienta para mandar correos electrónicos, ver páginas web y comprar cosas desde el sillón de casa.

Pero muchas de las nuevas conexiones eran realizadas por módems, y por tanto no tenían una dirección fija en la red (IP). Cada vez que se conectaban tenían una dirección distinta. Al no tener una dirección fija en la red, podían actuar como clientes, pero no podían ofrecer servicios, ya que las otras maquinas no podían conectarse al desconocer su dirección.

Mientras que al principio la web se consideraba un medio de comunicación simétrico, la explosión comercial de Internet hizo que se ajustara mucho más al paradigma de la televisión o la radio, que funcionaba en una sola dirección: había un proveedor de información y un receptor. Aunque era fácil encontrar un servidor donde alojar una página web, era muy complicado hacerlo en la propia máquina de uno.

Mucha gente estaba convencida de que este paradigma iba a aguantar mucho tiempo y que iba a ser muy rentable. Había empezado la fase comercial de Internet. Los ISPs (Proveedores de Servicio de Internet o Internet Service Provider) creían en este nuevo modelo comercial de Internet, preocupándose mucho más por que los usuarios pudieran bajarse cosas, que por ofrecer servicios. Un ejemplo son las líneas ADSL, que son bastante asimétricas, permitiendo bajarse cosas hasta tres veces más rápido que subir cosas.

Pero uno de los problemas que tiene este modelo es que se conectan muchos ordenadores a un servidor. El servidor tiene que ser muy potente, fia-

Sin embargo, el proyecto SETI@home funciona de forma distribuida. Los usuarios se bajan un programa que actúa como un salvapantallas, que se conecta a un servidor del proyecto que almacena y distribuye los datos a los usuarios. Se baja datos del servidor, realiza los cálculos cuando el ordenador no está siendo usado por el usuario, y cuando acaba, envía los resultados al servidor y se baja más datos, empezando otra vez de nuevo. Y como es un salvapantallas, sólo funciona cuando el ordenador no está siendo usado por el usuario.

En diciembre de 2003, había casi cinco millones de usuarios formando parte del proyecto, lo que lo convierte en el mayor computador de la historia, formado por aportaciones voluntarias.

Aunque no sea estrictamente hablando una aplicación *peer to peer*, SETI@home ha conseguido una potencia de cálculo mayor que la de un superordenador que sólo está al alcance de grandes ins-

ble y seguro para poder atender todas las peticiones a la vez. Y por otro lado, los ordenadores cada vez son más potentes y toda esa potencia se desaprovecha. Es lo que se ha llamado «la materia negra de Internet», que consiste en todos los PCs conectados a Internet, pero que están usando un tanto por ciento muy bajo de su capacidad de proceso y su conexión.

Y lo peor de este modelo es que, si el servidor falla, falla la red.

En 1996, apareció una aplicación que se llama ICQ. Permitía «chatear» a distintas personas de todo el mundo. Pero lo más curioso es que rompía con este modelo de red. Cuando ejecutabas ICQ en tu máquina, éste se conectaba a un servidor. El servidor tenía una lista de personas conectadas, y su función era únicamente poner en contacto a las personas que querían chatear. Una vez hecho esto, el servidor no hacía casi nada, todo lo hacían los ordenadores cuyos usuarios chateaban entre sí. Así, la carga del servidor era muchísimo menor, ya que se distribuía entre todos los ordenadores. Éste fue el principio de lo que se llaman «aplicaciones *peer to peer* (p2p)» o de igual a igual. *Peer to peer* es un tipo de aplicaciones que aprovechan los recursos (almacenamiento, procesador, contenido, presencia humana) disponibles en todos los rincones de Internet. Como acceder a recursos descentralizados supone operar en entornos de conectividad inestable e IPs impredecibles, los nodos *peer to peer* deben operar fuera del DNS[2] y tener una independencia significativa o total de servidores centrales.

2. Cuando un ordenador necesita conectarse a otro, necesita saber su dirección IP. Esto es más o menos como el número de teléfono. Pero como es algo complicado acordarse de direcciones que son muchos números, se creó el DNS, que sirve para poder conectarse a otros ordenadores usando nombres, en vez de números. Gracias al DNS podemos conectarnos a Sindominio poniendo en un navegador www.sindominio.net y no 213.172.61.252. La entidad oficial internacional que lleva el registro de nombres de dominio es la ICANN, y para registrar un dominio necesitan saber quién eres. Lo que significa que si publicas en un sitio algo que a las autoridades competentes les pueda parecer peligroso, al haber una persona a cargo del dominio, puede llegar a saber quién eres. Y dependiendo de las leyes, pueden obligarte a retirar lo que has publicado. Resulta difícil ofrecer servicios sin un nombre de dominio, pero una de las cosas innovadoras de ICQ, o de Napster, es que tenían su propio sistema de direcciones, independiente del DNS. Una vez que te conectabas al servidor, el servidor te ponía en contacto con otras máquinas. Aunque estas dos aplicaciones no son realmente *peer to peer*, porque dependen de un servidor para resolver las direcciones, se aproxima mucho a lo que se considera p2p.

tituciones o empresas, pero usando ordenadores personales. SETI@home muestra que la colaboración y la autoorganización social pueden alcanzar un poder computacional e informacional superior al de las mayores instituciones estatales y corporaciones internacionales.

Esto es el distintivo de las redes p2p. Lo que tienen en común Freenet, Jabber, Napster o ICQ es que aprovechan recursos que antes estaban infrautilizados, siendo capaces de trabajar con conectividad variable. Esto les permite hacer un nuevo y potente uso de los cientos de millones de dispositivos conectados a Internet en los últimos años.

Tres características son propias de las aplicaciones p2p:

– Permiten una conectividad variable.
– Crean un sistema de direcciones independiente del DNS.
– Permiten que todos los nodos de la red tengan una autonomía significativa.

Estas tres características permiten que las redes p2p sean autoorganizables, es decir, la red misma se autoorganiza según van apareciendo o desapareciendo nodos. Esta autoorganización ocurre a dos niveles:

1. Respecto a una comunidad p2p dada, a cualquier ordenador al que se le concede permiso para convertirse en un nodo de la comunidad, se le concede al mismo tiempo igualdad respecto a cada nodo en la comunidad. Añadir nodos a la red no requiere una reorganización, ni central ni de otra forma.

2. A mayor escala, digamos billones, la comunidad p2p puede organizarse de forma natural (dependiendo de los intereses) en millones de redes virtuales de grupos más pequeños agrupados según intereses específicos. Así, la organización de los nodos es independiente de si un nodo está conectado o no. Ésta es la característica que permite la conectividad variable y que facilita la escalabilidad.

RE-CODE.COM, LIBERALIZANDO EL CAPITAL

Los americanos son la pera al menos por un par o tres de razones: porque todo lo han inventado allí, porque si no lo han inventado lo tienen más grande y porque, si al final hace falta echarse el pisto, pues se lo echan y au.

Aquí tenemos Re-code.com, un proyecto hacktivista para dar cambiazos en supermercados adaptando el precio. Se trataba de una página web que ponía en funcionamiento una especie de wiki que permitía a los usuarios bajarse códigos de barras de productos presentes en determinados supermercados adaptando, eso sí, el precio del producto a las capacidades o deseos de cada cual. Por otra parte, también permitía que el usuario se convirtiera en cómplice activo al poder aportar informa-

Napster

«Napster empezó una revolución. Un par de personas, una buena idea y una tecnología sencilla despertaron a los perezosos y dormilones gigantes del negocio de la producción de música y les puso muy pero que muy nerviosos. La batalla legal empezó enseguida y algunos de los negocios más potentes del capitalismo casi perdieron la camisa en el intento. La cosa acabó, provisionalmente, con un acuerdo pero está por ver lo que pueda suceder.»
Massachusetts Institute of Technology (MIT 6.805/6.806/STS085), *Ethics and Law on the Electronic Frontier*[3]

En 1999, Shawn Fanning, un joven estadounidense, escribió un programilla para intercambiar música con sus amigos a través de Internet. Lo llamó Napster, y en cosa de dos años triunfó en Internet. En un año, era usado por más de 25 millones de usuarios. Esta cifra le convirtió en el servicio con mayor crecimiento de Internet.

Napster funcionaba de la siguiente manera: te bajabas el programa, lo instalabas y, cuando lo ejecutabas, te pedía un nombre de usuario y una contraseña para registrarte. Una vez registrado, el programa enviaba a un servidor una lista con los ficheros que compartías en tu disco duro. Luego, podías realizar una búsqueda en el servidor de los archivos que compartían otros usuarios.

Podías buscar por ejemplo por Pink Floyd, y el servidor te devolvía una lista de ficheros mp3 de Pink Floyd. Pero la novedad es que esos ficheros no estaban en el servidor, sino en los ordenadores de los usuarios. Mantener un servidor con la capacidad necesaria para descargar todos los ficheros que Napster permitía bajarse era inviable. Nunca antes podía uno bajarse tanta música de Internet. Además, tenía una característica especial: te permitía conocer usuarios con gustos parecidos a los tuyos. Realizabas una búsqueda por ese grupo tan especial que sólo tú conocías, y resulta que había un friki en Internet que tenía todas sus maquetas en mp3. Y lo mejor era que podías chatear con él.

3. http://ocw.mit.edu/OcwWeb/Electrical-Engineering-and-Computer-Science/6-805JEthics-and-Law-on-the-Electronic-FrontierSpring2002/LectureNotes/detail/Week-2.htm.

ción sobre nuevos códigos de barras también presentes en los supermercados a atacar. Dado que mencionaban explícitamente alguna cadena de supermercados, muy pronto recibieron amenazas legales y decidieron cerrar su página web para evitar ser perseguidos judicialmente.

A continuación os transcribimos un texto curioso sobre re-code.

RE-CODE.COM HACE PÚBLICO SU CÓDIGO FUENTE*

La descripción conceptual de los productos que compramos es el inventario de nuestras vidas. En los almacenes de las grandes cadenas este inventario se cataloga con el «Símbolo Universal

* Artículo publicado en *Suburbia*, el viernes 17 de octubre de 2003.

El crecimiento de Napster fue increíble; en apenas seis meses tuvo más direcciones registradas que el DNS en veinte años.

Sin embargo, esto no le sentó muy bien a la industria discográfica. Varios grupos musicales, como Metallica y Dr. Dre, 18 compañías discográficas y la Asociación de la Industria Fonográfica de los Estados Unidos (RIAA, http://www.riaa.com/, Recording Industry Association of America, un lobby formado por las discográficas más importantes, para «defender» el copyright y luchar contra la piratería) llevaron a Napster a los tribunales. Y empezaron las largas batallas legales...

Napster alegó que la compañía sólo actuaba como intermediaria, ya que sus servidores no almacenaban canciones. Además estaba el hecho de que los usuarios podían usarlo para compartir canciones copyleft (canciones cuya licencia copyright dice explícitamente que pueden ser copiadas sin permiso del autor). Pero no sirvió de nada. Intentaron llegar a acuerdos con músicos y empresas discográficas, pero tampoco sirvió. En julio de 2001, la jueza Marilyn Patel ordenó el cierre de Napster hasta que pudiera proteger adecuadamente, si esto era posible, la propiedad intelectual de las canciones que los usuarios intercambiaban. Sus palabras en una vista previa fueron: *«Ustedes han creado este monstruo, y a ustedes les toca buscar una solución»*.

Y esto fue el principio, que actualmente sigue, de un largo historial de amenazas y denuncias que aún sigue intentando mantener el anticuado modelo de negocio de las discográficas.

En el momento de su cierre, Napster contaba con más de 60 millones de suscriptores. Pero cuando cerró, aparecieron otras redes de intercambio de ficheros, como AudioGalaxy, KaZaA o WinMX. Aunque muchas redes se cerraron por las denuncias de la RIAA, rápidamente surgían otras redes que miles de usuarios usaban para compartir archivos. Y también surgieron otros tipos de redes p2p mucho más difíciles de controlar.

del Localizador del Producto» (UPC). El símbolo del UPC se conoce como código de barras. Los códigos de barras ahora se encuentran por todas partes en nuestro mundo, extendiéndose fuera del inventario de productos hasta nuestros libros, nuestra ciencia ficción, nuestras películas e incluso nuestros tatuajes....

El proyecto RE-CODE.COM reúne las acciones mediático-tácticas de la CARBON DEFENSE LEAGUE y de los secuestros de vídeo y de funcionamiento de Conglomco, y toma la acción en línea fuera de la caja como forma de recreación verdadera del mundo.

Si nos fijamos en la confianza puesta en los sistemas digitales por parte de los almacenes de las grandes cadenas comerciales que utilizan el sistema UPC, podremos detectar un problema o un virus en el sistema. El virus es el ser humano. Somos, hasta cierto punto, la pesadilla de lo digital. Somos

Aprendiendo de Napster

Napster demostró muchas cosas. Se podía crear una red a nivel mundial para compartir música, sin que los usuarios tuvieran que subir sus ficheros a un servidor centralizado, y en la que incluso los usuarios podían chatear compartiendo intereses parecidos. También demostró lo poco interesadas que estaban las multinacionales discográficas en cambiar su modelo de negocio.

Desde un punto de vista técnico, Napster funcionaba muy bien distribuyendo archivos y ancho de banda entre los usuarios, y centralizar las búsquedas de archivos y las direcciones resultaba muy eficiente. Pero esto tenía un inconveniente: la red entera dependía del funcionamiento de los servidores de Napster. Una vez que las batallas legales acabaron, cerraron el servidor, y de esta forma acabaron con la red.

La pregunta era: ¿y si existiera una forma de crear una red para compartir ficheros que no dependiera de un servidor central? No podrían controlarla, ya que estaría en todas partes, en cada uno de los millones de ordenadores que se conectaran a ella.

Gnutella

Gnutella es una de las primeras redes *peer to peer* completamente descentralizada, no depende de ningún tipo de servidor. Nació en marzo de 2000. En sus orígenes fue creada por Justin Frankel y Tom Pepper, que trabajaban en una compañía que se llamaba Nullsoft, que desarrolló Winamp (el popular reproductor de mp3s).

Según Tom Pepper, en un principio nació con la idea de compartir recetas. Su nombre viene de GNU y de Nutella. Fue un experimento. Sin embargo, a los ejecutivos de AOL no les pareció una idea muy rentable lo de compartir recetas y prohibieron la idea. Lo que se suponía que iba a estar bajo licencia GPL cuando llegara a la versión 1.0, no pasó de la versión 0.56. Aunque fue declarado un «proyecto freelance no autorizado».

la rueda chirriante. En las situaciones típicas de una transacción comercial, el consumidor y el cajero se comportan adaptándose al dominio del código de barras. Ambos dependen de la exactitud del código. Ambos funcionan según comportamientos acordes con los patrones de los rituales tradicionales de consumo. El cajero y el cliente escuchan solamente una señal sonora, mientras que los códigos del artículo adquirido se desvanecen tras la luz cegadora del lápiz óptico.

En algunas situaciones incluso han quitado al cajero, lo que permite que una máquina pueda ser ahora controlada solamente por el código de barras maniobrado por las manos humanas. Esas mismas manos humanas se pueden utilizar ahora en un acto de subversión del código de la fábrica. Esas mismas manos son el defecto que debe resistir el digital abrazo del símbolo UPC. No debemos limitarnos a actuar ante el horror de la ciencia ficción, sino que debemos recurrir a la acción táctica

El principal problema de una aplicación p2p es cómo encontrar a otros nodos en la red. Y es más difícil aún cuando no hay un ordenador que sea el que se encargue de poner en contacto a los nodos. Sin un ordenador central para encontrar recursos, ¿cómo se encuentran cosas en Gnutella?

Primero, hay que conocer la dirección de algún nodo conectado a Gnutella para conectarse a la red. Una vez conectado a la red para realizar una búsqueda de un fichero, el nodo que busca ese fichero envía una petición de búsqueda a los nodos a los que se acaba de conectar. Muy posiblemente estos nodos no tendrán ese archivo ni sepan qué nodos lo tienen, pero pasarán la petición de búsqueda a los nodos que ellos conozcan, y así sucesivamente las búsquedas se van propagando por toda la red. Cuando a un nodo le llega una búsqueda de un archivo que tiene, contesta enviando su dirección.

Este comportamiento de Gnutella se acerca mucho al del mundo real. Imaginemos que nos han invitado a una fiesta selecta. Acabamos de llegar y queremos averiguar dónde está el champán. Hablamos con nuestro amigo en la fiesta, se lo preguntamos, y no sabe dónde está, pero le pregunta a su colega, y así sucesivamente, hasta que encuentran a alguien que sabe dónde está el champán. Si preguntamos a mucha gente, nos llegaran respuestas de distintos sitios donde hay champán.

El horizonte Gnutella:

Al contrario que en otras redes, donde puedes ver a todos los nodos de la red, en Gnutella esto no es así. Como para buscar algo en Gnutella hay que enviar paquetes preguntando por un archivo, y si no está, pasar este paquete a todos los nodos que conozca, y así sucesivamente, hay que ponerle un tiempo de vida a los paquetes; si las peticiones fueran todo el rato de nodo en nodo, preguntando por un archivo que no existe, se colapsaría la red. Por eso a los paquetes en Gnutella se les pone un tiempo de vida de siete saltos, es decir, si un paque-

para manipular el sistema existente en beneficio del consumidor. Con RE-CODE.COM buscamos una manera de destacar la absurdidad de un sistema basado en los seres humanos que confíe, sobre todo, en nuestra presencia física y en la aceptación continua. Debemos mostrar nuestro lado humano con la subversión del código.

Re-Code fue una iniciativa del grupo Hactivist que consistía en un programa vía web, que generaba códigos de barras de productos conocidos, a un valor menor del que estipulaba el original en el centro comercial.

RE-CODE.COM era un servicio libre que permitió que sus clientes compartieran la información

Re-code.com

te que va preguntando por un archivo ha pasado por mas de siete nodos y no lo ha encontrado, se descarta.

Por eso, en Gnutella un nodo solo puede ver nodos que estén a siete nodos de distancia. Se calcula que con siete saltos, y teniendo en cuenta que cada nodo está conectado a muchos nodos, puedes ver unos diez mil nodos.

Este efecto sería el mismo que si estuvieras en una manifestación, ves todo rodeado de gente, pero no puedes ver cuánta gente hay en total.

Freenet

«Me preocupo por mi hija y el Internet todo el tiempo. Aun cuando es todavía demasiado pequeña para conectarse, me preocupa que dentro de diez o quince años venga y me diga: papá ¿dónde estabas tú cuando se cepillaron la libertad de publicar en Internet?»
Mike Godwin, Electronic Frontier Foundation

Aunque Gnutella funcionara de forma completamente descentralizada, Ian Clark estaba mucho más preocupado por la libertad de expresión y la censura, y desarrolló Freenet bajo una premisa política concreta: «el derecho a compartir información sin riesgo ninguno».

En 1999 publicó «A Distributed Decentralised Information Storage and Retrieval System» (Un sistema de almacenamiento y obtención de información distribuido y descentralizado), (http://www.ovmj.org/GNUnet/papers/freenet.pdf), y en julio de ese mismo año inicio Freenet en la Universidad de Edimburgo, Escocia. Actualmente Freenet es mantenido y desarrollado por muchos voluntarios de varios continentes.

Los objetivos de Freenet son:

– Evitar la censura de los documentos.
– Proporcionar anonimato a los usuarios.
– Quitar cualquier punto de control o fallo.

sobre los productos y crearan ellos mismos los oportunos códigos de barras, de manera que se pudieran imprimir y utilizar para recodificar artículos en grandes almacenes. Se ponían etiquetas nuevas con códigos existentes de UPC para fijar un nuevo precio, participando así en un acto de compras tácticas.

RE-CODE.COM en su inicio era una base de datos compartida, actualizada por nuestros clientes. La participación era libre y no requería ningún acuerdo especial de admisión como miembro o transferencia directa especial de software. Después de entrar en la página web, los clientes podían elegir buscar la información del producto en la base de datos o agregar al sistema sus propios datos recogidos. Usando el generador Barcode, los códigos de barras eran creados en tiempo real y puestos a disposición del usuario. Utilizamos solamente el tipo barcodes, la variedad más común de UPC-A de

– Distribución y almacenamiento efectivo de documentos.
– Conseguir que no sea posible incriminar a los operadores de un nodo.

Para conseguir esta libertad, la red esta completamente descentralizada y tanto los publicadores como los consumidores de información son anónimos. Sin anonimato no puede haber verdadera libertad de expresión, y si la red es centralizada será vulnerable a ataques.

La comunicación entre todos los nodos se realiza encriptada. Gran parte del anonimato de Freenet consiste en que cada nodo pasa información a otros nodos sin saber qué nodos originan la información ni cuáles son los destinatarios, de forma que es muy difícil saber quién insertó un documento o quién lo ha solicitado. Además, como en los nodos la información se almacena encriptada, legalmente es difícil hacer que la administradora de un nodo sea responsable del contenido almacenado.

En la actualidad, el control intrusivo del flujo de datos es una realidad. Redes de espionaje como Echelon controlan todas las comunicaciones electromagnéticas a nivel global. Yahoo y Hotmail[4] admitieron tener instalado Carnivore, un potente mecanismo de filtrado de datos que probablemente esté instalado en muchos Proveedores de Servicios de Internet (ISP).

Además, en algunos países como China o Cuba, el acceso a Internet está permitido en muy pocos lugares, y se bloquean las DNS de sitios no deseados.

Resumiendo, el uso de Freenet evitaría en gran medida todos estos mecanismos de control y espionaje de Internet, por un lado encriptando las comunicaciones y, por otro, por ser una red descentralizada e independiente del DNS.

Además de Freenet, existe un proyecto similar, GNUNet (http://www.ovmj.org/GNUnet/), que intenta desarrollar una red *peer to peer*

4. http://www.wired.com/news/politics/0,1283,46747,00.html.

barcode. Se utiliza en la mayoría de las compras al por menor en Norteamérica y Europa. En las páginas web mostrábamos a los usuarios un proceso por el que pueden obtener precios más baratos para los artículos de grandes superficies, simplemente recodificando artículos que planeaban comprar; o cambiábamos las etiquetas de algunos artículos para hacer llegar a los clientes, por medio de los cajeros, los precios verdaderos de las mercancías. La propia página web de RE-CODE.COM es en sí misma una mofa de PRICELINE.COM, hecha para parecer casi idéntica a su contraparte, y su lema es: «consumir de manera revolucionaria», intentando animar a la gente a marcar su propio precio a las mercancías y los servicios. RE-CODE.COM intentó simplemente llevar esta idea a su fin lógico, permitiendo que cualquier precio sea marcado y recodificado en el almacén del cliente, a través del reemplazo del código de barras.

encriptada y muy segura, pero que, al contrario de Freenet, no depende de Java para funcionar.

La industria discográfica

«Vuestras cada vez más obsoletas industrias de la información se perpetuarían a sí mismas proponiendo leyes, en América y en cualquier parte, que reclamen su posesión de la palabra por todo el mundo. Estas leyes declararían que las ideas son otro producto industrial, menos noble que el hierro oxidado. En nuestro mundo, sea lo que sea lo que la mente humana pueda crear puede ser reproducido y distribuido infinitamente sin ningún coste. El trasvase global de pensamiento ya no necesita ser realizado por vuestras fábricas.»
Perry Barlow, *Declaración de Independencia del Ciberespacio*

A pesar de todas las denuncias, los intentos de la RIAA por acabar con las redes de intercambio de ficheros no tuvieron mucho éxito. Aunque consiguió cerrar algunas redes tipo Napster, como Audiogalaxy, aparecieron rápidamente otras redes, y algunas de ellas descentralizadas y anónimas. También aparecieron otras redes híbridas, es decir, ni completamente descentralizadas, ni completamente dependientes de un servidor central, como por ejemplo E-donkey. E-donkey en vez de usar un servidor para poner en contacto a la gente que desee intercambiar ficheros, usa una red de servidores distribuidos, con lo cual es imposible parar la red deteniendo un servidor.

Así que la RIAA decidió cambiar de estrategia y, en vez de ir a por las redes, que cada ver era más difícil, decidió ir a por los usuarios.

De esta manera, el 8 de diciembre de 2003, denunció a 261 usuarios de redes de intercambio de ficheros[5] y esto sólo fue el principio de un historial de denuncias. Actualmente (diciembre de 2003) la RIAA está en su tercera ronda de denuncias, ha denunciado a 41 personas por compartir ficheros y ha alertado a otras 90 personas sobre posibles denuncias[6].

5. http://yro.slashdot.org/article.pl?sid=03/09/08/1712256.
6. http://www.theregister.co.uk/content/6/34340.html.

El proyecto tuvo tanto éxito que llegaron a ver saturados sus servidores con más de 50.000 vistas diarias. Les llovieron las entrevistas y las peticiones de hacer una demostración por parte de programas de radio de universidad, periodistas, investigadores, la emisora nacional de radio, la BBC y otras alrededor del mundo. Resultaba increíble la atención recibida por el sitio web.

La cadena comercial Wall-Mart, la principal afectada por estas travesuras a favor del consumidor, puso una querella judicial contra el sitio web recode.com, lo que obligo a Hactivist a sacar el programa «recode» fuera de sus páginas. Podéis ver la carta de Wall-Mart en esta dirección: http://www.re-code.com/images/letter1.jpg.

Siguiendo con esta actitud siempre «revoltosa», Hactivist ha publicado hace poco el código fuente de RE-CODE para su modificación, uso, libre distribución y diversión.

Su estrategia se basa en buscar a los usuarios que más ficheros comparten, presionar a los servidores de acceso a Internet para obtener sus datos supuestamente privados y denunciarles. Según un portavoz de la RIAA, los 41 acusados en esta tercera ronda de denuncias han bajado una media de mil canciones cada uno.

La RIAA ha denunciado a casi 400 estadounidenses desde septiembre. Ha obtenido los nombres de los supuestamente anónimos usuarios de redes para compartir ficheros mediante una exitosa estrategia legal que fuerza a los ISPs a proporcionar los nombres de los usuarios. Algunos ISPs, como Verizon y SBC, se han enfrentado a la RIAA en los tribunales, pero hasta la fecha todas las decisiones han favorecido a la RIAA.

La RIAA afirma que ha llegado a establecer acuerdos económicos con 220 usuarios de redes para compartir ficheros y que 1.000 personas se han beneficiado de una amnistía al asegurar que no intercambiarán nunca más música no autorizada[7].

Es decir, es una estrategia basada en el miedo, ya que no hay una medida eficaz para luchar contra los millones de usuarios de redes p2p. En realidad se trata de un acto de desobediencia civil masivo, ya que a nadie le parece justo el precio de los CD's de música actuales. Y tampoco nadie se cree que sea piratería, ni robo tal cual, puesto que cuando robas se supone que le quitas algo a alguien, aquí simplemente se trata de copiar información. La información no desaparece del sitio original, simplemente se copia. La intuición fundamental detrás de la justificación moral del libre intercambio de información es que la producción inmaterial no puede ser objeto de propiedad ya que su multiplicación es gratuita y en nada perjudica a quien anteriormente la posea. Si posees una manzana y la compartes te quedas con media manzana. Si tienes una idea (una can-

7. http://yro.slashdot.org/article.pl?sid=03/09/05/0042257&mode=thread.

Podéis ver una imagen de la aplicación en esta url: http://www.re-code.com/images/screengrab1_highres.jpg.

Ya sabéis, hay gloria en la subversión...

En realidad no hacía falta trabajar tanto. Si lo que quieres es dar el cambiazo, hay paginas que ofrecen imprimir códigos de barras desde el año 94 y, después de todo, es tan sencillo como irte a páginas de acceso público como www.milk.com/barcode, o de empresas que ofrecen software gratuito para windoze o linux: www.tec-it.com. Introduces la clave numérica —los numeritos que hay debajo de las barras, del producto que quieres pagar (aceite de girasol)—, imprimes la etiqueta que te genera la máquina y, cuando vuelvas al supermercado, la pegas sobre el producto que te quieres lle-

ción, un texto, una película,...) y la compartes tienes dos o más ideas. Donde no hay escasez no puede haber propiedad en el sentido tradicional; otro problema de naturaleza diferente es la remuneración de los creadores, pero esto no tiene por qué basarse en la prohibición de cooperación (en forma de distribución de información) para toda la sociedad. Sin embargo, la industria discográfica no quiere reconocer esto, llegando a afirmar que «no hay diferencia entre robar un CD y piratearlo»[8].

Perry Barlow, en su articulo «No se puede vender vino sin botellas», explica muy bien cómo el modelo de negocio de las discográficas no es válido en un mundo donde replicar la información no sólo es gratis, sino que lo que sale caro es evitar que se copie[9].

La economía de la mente en la red global

«El acertijo es el siguiente: si nuestra propiedad se puede reproducir infinitamente y distribuir de modo instantáneo por todo el planeta sin coste alguno, sin que lo sepamos, sin que ni siquiera abandone nuestra posesión, ¿cómo podemos protegerla?»
Perry Barlow

«p2p is the next great thing for the Internet.»
Lawrence Lessig

A pesar de que lo mas conocido del paradigma *peer to peer* sean las redes para compartir ficheros ilegales, éste ofrece muchísimas mas posibilidades que compartir ficheros de forma distribuida. Muchas todavía por explotar. Algunas empresas han visto este potencial y están dedicando bastantes recursos a desarrollar aplicaciones que podrían ser revolucionarias.

8. Edgar Bronfman, Jr., dueño de Warner Music, El Pais, 7-12-2003.
9. http://suburbia.sindominio.net/article.php3?id_article=85.

var a casa (siguiendo con el ejemplo: aceite de oliva virgen extra).

También puedes fotocopiar un código de barras del aceite girasol y pegarlo tal cual sobre la botella de aceite de oliva. Funciona igual de bien, lo importante es pegarlo limpiamente.

La clave del tema está en que en los supermercados tienen un montón de códigos de barras dados de alta (tantos como productos a la venta) y con sus precios asignados, que van adaptando según las ofertas o lo que sea. Cuando pasan un producto por caja, el ordenador busca el precio asignado al código de barras que lee y eso es lo que se cobra. Si en vez de llevar un código de barras lleva otro, el precio, obviamente, será otro. Como la mayoría de los códigos de barras vienen de fábrica, los supermercados se confían y mal que hacen, porque pegar un código de barras impreso en casa o recortado de otra parte, encima del que ya hay, es un remedio clásico y discreto.

En febrero de 2001, Sun creó el proyecto JXTA[10], que consistía en crear un conjunto de protocolos y de librerías para desarrollar tecnologías p2p. Las aplicaciones p2p más conocidas sólo implementan una función: ICQ, Messenger o Jabber sirven para mensajería instantánea; Gnutella, Napster o E-mule para compartir ficheros. Pero JXTA llega mucho más allá, creando la infraestructura básica para poder desarrollar cualquier tipo de aplicación.

La lista de proyectos[11] que se están desarrollando o se han desarrollado con JXTA es impresionante: radiojxta[12] es una aplicación para transmitir radio por Internet que funciona de forma distribuida, por lo que puede llegar a funcionar sin que haga falta un gran ancho de banda, incluso con módems. También existen aplicaciones para teléfono[13] sobre redes p2p, para montar foros de discusión[14] o incluso para organizar diarios compartidos[15].

Aunque Sun ha sido una de las empresas que más ha invertido, hay bastantes más empresas que han apostado mucho por estas tecnologías como forma de hacer negocio: 312inc[16] ha desarrollado una aplicación para hacer copias de seguridad usando p2p y encriptación; Digital Dream, Inc.[17] ha desarrollado un software (*ifreestyle*) para gestionar información personal, agenda, tareas y contactos; y Zudha[18] desarrolla productos p2p.

Aunque queda mucho para que esta tecnología se expanda, hay muchas empresas que están apostando fuerte, porque gracias a este paradigma pueden desarrollar aplicaciones mucho mas robustas, escalables y autoorganizables, lo cual implica mucho dinero.

10. http://www.jxta.org.
11. http://www.jxta.org/servlets/ProjectList/.
12. http://radiojxta.jxta.org/.
13. http://vop2p.jxta.org/.
14. http://juxtaprose.jxta.org/14. http://juxtaprose.jxta.org/.
15. http://shareddiary.jxta.org/15. http://shareddiary.jxta.org/.
16. http://www.312inc.com/.
17. http://www.digitaldream.jp/.
18. http://www.zudha.com/.

De todas formas, nosotros jamás recomendaríamos estos métodos reformistas a más no poder: después de todo, lo más seguro y recomendable —dicen— es sacar la botella de aceite de oliva o de tinto del bueno en el bolsillo interior de la gabardina, esa ancha que tienes, y dejarse de chorradas.

También desde el año 2001, el IEEE (Institute of Electrical and Electronic Engineers) viene organizando anualmente una conferencia sobre tecnologías p2p, a las que llaman «la tercera generación de Internet»[19].

¿Y los movimientos sociales?

Viendo cómo los servidores alternativos, como por ejemplo nodo50, están siendo vigilados[20] y cómo éstos han recibido presiones de la policía pidiendo los logs, merece la pena plantearse el uso de redes p2p con encriptación como Freenet o GNUnet.

¿Qué habría pasado si re-code, en vez de estar situado en una página web, fuera un pequeño programa p2p?

Otro proyecto muy interesante sería retomar un proyecto de hactivist, Skillit[21], que es una aplicación para poner en contacto a activistas. Éste permite crear proyectos o grupos según intereses o zonas, con un sistema de mensajería y noticias, y desarrollarlos de forma descentralizada, garantizando la privacidad, y que por mucho que aumente el número de usuarios que lo use, no se cuelgue. Imagina una especie de «messenger» que te permitiera ver qué proyectos o colectivos hay en tu zona, o por qué intereses se mueven, o crear uno nuevo y publicitarlo entre tus contactos.

19. http://www.ida.liu.se/conferences/p2p/.
20. http://losvigilantes.nodo50.org/.
21. http://hactivist.com/.

WIRELESS, LA MULTITUD INTERCONECTADA

Adolfo Antón Bravo

PREFACIO

Las tecnologías *wireless* (sin cables) están empezando a cobrar una importancia considerable en los movimientos sociales. Su porqué está relativamente claro para quienes participamos en ellas. Relativamente, porque intuimos que el hecho de conectar a la gente entre sí sin tener que pasar por una empresa de telecomunicaciones cambia radicalmente el modo en el que se ha desarrollado Internet. Ya no dependemos del cable que nos llega a nuestra casa desde el operador de telecomunicaciones. También podemos superar las pequeñas redes de un local, una casa o un edificio que tenían una frontera muy marcada, allí donde se acababa la posibilidad de tirar cable. El libro *Building Wireless Community Networks* (Rob Flickenger, O'Reilly, 2002), una de las pocas referencias editadas sobre el fenómeno del wireless, y que en España ha llegado por Internet o bien fotocopiado, advertía «acerca de cómo la gente se conecta un@s con otr@s» y apuntaba la posibilidad de hacer que tu «comunidad» se «conecte» a un bajo coste. Así, por un lado, cuando hablamos de wireless nos imaginamos una sociedad interconectada (¿la sociedad de la información?), pero en vez de hacerlo exclusivamente con herramientas (software/hardware) propietario, también con tecnologías libres y/o abiertas. En sí misma, no parece que tenga unos principios políticos, sociales o filosóficos. Sin duda ése es nuestro reto, el reto de tod@s, y por eso habla también de «comunidad». Una comunidad puede ser de vecin@s, de estudiantes o cualquier otro entorno determinado, y donde las personas que la componen comparten y construyen colectivamente la red wireless utilizando unas tecnologías libres (802.11x) para acceder a Internet, para intercambiar archivos o para lo que sea. Quizás una de las claves para el éxito de las «comunidades wireless» (nos referimos,

MANIFIESTO DE MADRIDWIRELESS

Es la red la que nos mueve, son sus hilos los que nos manejan, es el deseo de hacer crecer a la comunidad, de abrir los caminos cerrados, de atravesar los obstáculos con nuestras propias manos, de preservar nuestra independencia y el deseo de hacerla crecer.

El movimiento mundial de redes ciudadanas libres nos da esta oportunidad, su filosofía alumbra nuestro camino, redes metropolitanas construidas exclusivamente por ciudadanos, sin colaboración empresarial. La libertad que nos da la ciudadanía no nos la pueden quitar compromisos con empresas.

Al igual que estas redes, nacemos nuevamente libres de su mano, ellas cambian nuestras expectativas de comunicación y de ayuda al desarrollo, crecemos de su mano, ya que son ellas las que realmente

por tanto, a las personas que participan en la comunidad) sea el hecho de que no dan la espalda a la tecnología como otros movimientos sociales que la piensan como el último juguetito del capitalismo avanzado, sino que la acogen, la investigan, la critican, la desarrollan, experimentan con ella y todo ello por sus intrínsecas y sin embargo escondidas posibilidades sociales.

¿A quiénes nos dirigimos con este capítulo?

Pretendemos contaros de qué va esto del wireless. No va sobre cómo conectarte a Internet o cómo sabotear la actividad comercial de una operadora de telecomunicaciones (que también), sino de cómo construir una comunidad wireless. Hemos de reconocer que pese a los cuatro años que cumple en octubre de 2005 Madridwireless.net, ésta es una historia que se encuentra en la pubertad, y que todavía ha de ser contada y sobre todo construida. Insistimos, sólo hemos explorado algunas posibilidades, pero intuimos que son muchas más. ¿Te gustaría participar?

Contexto histórico

A principios de 2001 vivíamos el principio del fin del *boom* de los valores tecnológicos en las bolsas de valores de medio mundo. En España, la crisis vino algo más tarde. Internet se había convertido en la panacea de la nueva economía. Las empresas tecnológicas parecían que iban a contagiar a todo el mercado con sus espectaculares subidas en bolsa.

Internet, la red de redes como autopista mundial de la información y la Web como administradora de los contenidos parecían hechas a medida para los fines del capitalismo avanzado, la economía del entretenimiento.

También la informática, las redes, la web o mejor la tecnología en su conjunto funcionaban al servicio de las empresas. Obviamente, Internet y la Web son mucho más que eso, o más bien a pesar de ello. Las luchas de los hacktivistas representaban una mínima parte de la población mundial conectada. Su valor más

nos están enseñando cómo podemos ayudar a los demás, van más allá de simples proyectos, van más allá de simples ilusiones, incluso van mucho más allá de ser simples redes. Fácil es construir una red con los medios adecuados, hermoso es hacerlo además con una filosofía, y es esta filosofía (inherente a las redes metropolitanas wireless a lo largo de todo el planeta) la que saca lo mejor de todos los que nos hemos implicado en su crecimiento. Seattle, Nueva York, Londres nos demostraron que se pueden hacer estas redes únicamente con la colaboración ciudadana, que no son proyectos que nacen y desaparecen, que las prisas suelen ser malas consejeras y que la comunidad sabe organizarse y sacar adelante sus recursos, los cuales ofrece desinteresadamente a toda la humanidad. Los miembros de esta comunidad somos activistas de la red, tomamos parte en algo que no nos deja indiferentes en mayor o menor medida y comenzamos a trabajar. Vemos, pues, que ha llegado el momento de devolver lo que la

conocido, el sistema operativo GNU/Linux, contaba con 14 millones de usuarios en todo el mundo.

Cuando lees una noticia, no la lees tú solo (Parasitic Grid)

Y de repente, un medio especializado en noticias de tecnologías de la información (www.ibrujula.com) titulaba una noticia como «Parasitic Grid». ¿Qué era esto? El artículo hablaba de comunidades de vecin@s interconectados por wireless (literalmente, sin hilos; inalámbrico), formando redes de comunicación telemática en distintas ciudades de EEUU y Australia que, a su vez, se comunicaban entre sí por Internet.

Una tecnología llamada 802.11b, de libre uso para fines educativos o científicos, que permite una velocidad de transmisión de hasta 11Mbps, hacía posible crear una red WAN[1] sin depender de tu operador de telecomunicaciones. Hasta ese momento, una red WAN comunitaria dependía totalmente de la conexión con un ISP. Sin embargo, gracias a esta tecnología inalámbrica (las superiores 802.11a y 802.11g soportan 22 y 54Mbps respectivamente), el escenario cambiaba por completo. El hardware necesario para poder participar consistía en una tarjeta, una antena y un punto de acceso. La idea nos había tocado.

Sólo no puedes, con amigos sí (Hackmeeting 2001, la bola de cristal)

Era septiembre de 2001 y se celebraba el segundo hackmeeting en el Gaztetxe de Leioa, Bilbao. Una antigua nave industrial cercana a los ya inexistentes Altos Hornos, un escenario postindustrial donde 200 personas organizaron a través de una lista de correo (http://www.sindominio.net/listinfo/hackmeeting) el encuentro más importante de hacktivismo del estado español. Allí se habló de wireless, de hacktivismo, de la red indymedia, virus, bacterias... y también sirvió para que muchas per-

1. *Wide area network*: red de área amplia.

comunidad nos ha ofrecido, trabajamos por y para la red, por y para la gente, las únicas barreras son nuestras mentes; ante problemas: soluciones; ante dudas: colaboración; ante el pensamiento único: nuestra diversidad. Siempre existirá gente que dude de la posibilidad de estos movimientos; es de agradecer que existan, ya que nos obligan constantemente a mirarnos en los espejos de otros proyectos, ver sus realidades y reactivar nuestros ánimos al ver que ellos los han sacado adelante y que contamos con su ayuda. Madridwireless se declara pues activista de la red, desea fomentar la participación de sus ciudadanos en su seno y les invita a ello; rechaza el dinero empresarial ya que no le es necesario debido a su constitución ciudadana; proclama su independencia y libertad, ofrece sus recursos a la comunidad y utiliza los que la comunidad siempre le ha ofrecido. Wireless, software libre, cooperación sin mando, desinterés económico, compartir y ayudar son nuestras bases. ¿Quién se une a la fiesta?

sonas venidas de todo el estado y de otros puntos de Europa se conocieran. También nos conocimos much@s de Madrid que hasta entonces trabajábamos por separado en cuestiones técnicas o sociales, pero siempre teniendo en cuenta estos dos supuestos polos. Después de comentar el artículo de ibrujula y de haber visitado todos los sitios a los que hacía referencia (Seattlewireless, NYC, nocat...), creamos una lista de correo en sindominio.net (http://www.sindominio.net/listinfo/madridwireless) y posteriormente llegó el foro madridwireless.net, alojado en sindominio.net. Enseguida se apuntaron más de 200 personas a esa nueva lista y se asistía al nacimiento del espacio de discusión política, social y técnica de wireless más importante del estado.

Yo también quiero (Hacklab WH2001)

En estos inicios se abordaron cuestiones muy técnicas, aunque a su vez se escribieron documentos como el manifiesto de Madridwireless (http://www.madridwireless.net/manifesto), todavía vigente y de tremenda repercusión en el resto de comunidades wireless que aflorarían. El trabajo de la comunidad Madridwireless no se limitaba al espacio telemático. También tuvo (y tiene) su importancia el hacklab WH2001.

Si el hackmeeting es de «importación» italiana, el hacklab también lo era. Del primer hackmeeting de Barcelona surgió el primer hacklab, Kernel Panic, y con el de Leioa nacieron el Metabolik Biohacklab en Bilbao y el WH2001/Cielito Lindo en Madrid.

En el espacio físico de la Asociación de Amig@s del Café y las Computadoras se reunían cada semana decenas de personas entusiastas de la tecnología y de sus posibilidades de comunicación, transmisión de conocimiento. También se preparaban acciones o simplemente tomábamos cervezas. El el mismo recinto, bautizado como Cielito, o hacklab, nos juntábamos cada dos semanas l@s participantes en Madridwireless. Se debatían cuestiones técnicas, se hacían pruebas con nuevo hardware llegado, se decidía la compra de tarjetas o APs (Access Points,

WARDRIVING

Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como un ordenador portátil o un PDA (Personal Digital Agenda, agenda digital personal). El método es realmente simple: el atacante simplemente pasea con el dispositivo móvil y en el momento en que detecta la existencia de la red, se realiza una análisis de la misma.

Para realizar wardriving se necesitan realmente pocos recursos. Los más habituales son un ordenador portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el AP en un mapa y el software apropiado (AirSnort para Linux, BSD-AriTools para BSD o NetStumbler para Windows).

puntos de acceso) o se experimentaba con el propio hardware, como los clásicos talleres de construcción de antenas de todo tipo.

¿Cómo Participar? (esa gran pregunta)

Madridwireless y en general cualquier red inalámbrica ciudadana está formada por personas, y todas participan en la comunidad. En cuanto a su relación con la tecnología, sin embargo, van a desempeñar unos roles determinados. Algunas personas participan como «clientes» de la red, otras forman parte de la estructura de nodos, del backbone. Otras desarrollan herramientas, a su vez las primeras las prueban, etc. Una persona no tiene un solo rol en la red, esta diferenciación que hacemos es con ánimo de hacerlo más comprensible de cara a reconocer las múltiples posibilidades de interactuación. Algunos nodos ofrecen conexión a Internet, pero no tienen por qué. Tiene que quedar claro, tal como decía el manifiesto de Madridwireless, que no es una red de acceso gratuito a Internet, no es un ISP. Por encima de todo, es una red ciudadana, una red en el ciberespacio y también en la realidad. Es un movimiento social que se retroalimenta de otros movimientos sociales, como puede ser el del software libre o el del asociacionismo vecinal. Así pues, para participar hay que empezar con muchas ganas. Si sabes algo de redes, ordenadores, antenas, electrónica, programación, Internet..., quizás lo veas más sencillo y también vislumbres las posibilidades que ofrece. Si no sabes nada de lo anterior, lo primero, no te preocupes. Nadie nace sabiendo y particularmente la informática, como uno de los últimos desarrollos tecnológicos, parece reservada a una clase especial de «frikis». Nada más lejos de la realidad. En la sociedad actual todo está relacionado mucho más que antes y si sabes de cocina, coser, mecánica, electricidad, fontanería, periodismo o cualquier otra profesión o saber verás que el ordenador no es sólo un instrumento que aprovechan las empresas para vendérnoslo como una mercancía más, también es algo en lo que podemos intervenir. Éste es el gran reto de Madridwireless y de toda red ciudadana inalámbrica, la posibilidad

WARCHALKING: UN NUEVO LENGUAJE

Si tras hacer wardriving hemos detectado la existencia de redes inalámbricas en una zona, se procede a crear una marca que nos indique ante qué tipo de red nos encontramos; los símbolos se suelen poner en las farolas de alrededor, contenedores, paredes, mezclándose con el entorno. Si encuentras una de estas redes que te da acceso a Internet no abuses de quien te lo está proporcionando, no le quites todo el ancho de banda conectándote al emule para bajarte películas ni lo utilices para otras cuestiones de legalidad dudosa, ya que puedes perjudicar a la persona propietaria del equipo.

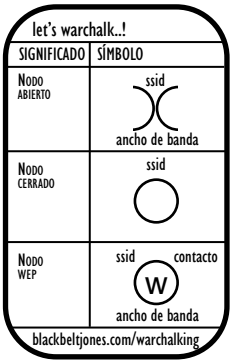
Si quieres conectarte a Internet, intenta hacerlo a través de locales como los McDonalds, Starbucks, Burguer King, hoteles caros, etc.; suelen usar redes wifis para que sus empleados interactúen con PDA. Es más divertido saber que la conexión gratuita la pagan multinacionales o establecimientos de propie-

de intervención sobre la tecnología wireless 802.11x que permite crear una red ciudadana, una Internet controlada por las comunidades. En estas redes, las comunidades tienen la posibilidad de acceder a un escenario «libre» en el que desarrollar sus relaciones y a la vez retroalimentar y potenciar las relaciones en el mundo físico. Uno de los aspectos revolucionarios de estas tecnologías es que permite saltarse a las empresas de telecomunicaciones para establecer una red a una distancia relativamente larga. Las comunidades de Madridwireless y Guadawireless hicieron experimentos en los que llegaron a 9 kilómetros de enlace en el campo pero otras comunidades han llegado a los 50 km, y Guadalajara está totalmente cubierta por Guadawireless, y eso gracias a una comunidad.

Modelos de participación

Hay varios modelos de comunidades inalámbricas. Hemos comentado el caso de Guadalajara, totalmente cubierto por Guadawireless. Otro ejemplo de cobertura «total» es el de Zamora, pero allí han sido el ayuntamiento, los hosteleros y empresas especializadas las que han sumado esfuerzos, todo lo contrario a la mayoría de las comunidades ciudadanas, que prefieren empezar a construir desde la base y luego establecer relaciones con otros agentes sociales. Y entre estas últimas, también las hay que tienen una asociación legal por detrás, como ANURI, Olotwireless o RedLibre, y las que no han buscado ese soporte legal como Madridwireless. Si bien cuando empezó el movimiento en el estado español hubo ciertas peleas (*flames*) entre miembros de Red Libre y de Madridwireless (el motivo, al parecer, era el apoyo de Madridwireless al CSOA El Laboratorio; no entendían que se compartiera espacio con «los okupas»), ahora tod@s tienen en mente la ampliación de la red, la difusión de lo que son las redes wireless, la tarea de elaboración de documentación, participación en los foros, etc.

tarios con mucho dinero, y pocas ganas de soltarlo con sus empleados. En esos sitios será interesante que utilices marcas que indiquen a la comunidad que existe una red wifi con salida a Internet cerca. Para ello podrás usar la simbología que se muestra en la imagen.Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que «pasen por allí». El lenguaje como tal es realmente simple:



Organización interna

En general, casi todas las comunidades wireless comparten algunas características. Lo primero que se suele hacer en Internet es crear una lista de correo, que se va a convertir al principio en un cajón de sastre para todo, desde información sobre la red hasta qué tarjeta me puedo comprar. Si la comunidad crece, necesitará crear más listas específicas. La segunda pieza fundamental es un foro donde la comunidad se muestra a sí misma, sus avances, sus dudas, lo que han visto/leído en otros foros... Seguramente habrá más gente que conozca a la comunidad por el foro que por la lista. El foro es más público, la lista es más de trabajo interno.

Cuando se cuenta con una comunidad amplia o cuando se quiere desarrollar un trabajo más divulgativo/educativo, encontramos el wiki, un software que permite editar una página web e ir creando páginas con una sintaxis propia, distinta al html y asequible para cualquiera. Es muy útil para proponer ideas y sobre todo para todo tipo de trabajo en grupo, colaborativo y abierto. Así existen, por ejemplo, proyectos como la Wikipedia (http://www.wikipedia.es), que tratan de crear una enciclopedia universal cuyo contenido es libre.

Otro aspecto importante es que la dimensión social no se queda en la red, y así son muy importantes las «kedadas», encuentros quincenales o mensuales donde l@s participantes intercambian experiencias cara a cara. También son las citas elegidas para los «talleres de antenas», donde algunos miembros de la comunidad van con materiales para construir antenas y cualquiera puede acercarse para montarse una.

Por ejemplo, el símbolo Retina) (1.5 identifica un nodo abierto, que utiliza el SSID «Retina» y dispone de un ancho de banda de 1.5 Mbps.

Escenario tipo

Una red wireless, a pesar de ser sin cables, es una red como otra cualquiera, como la que construyes con dos tarjetas de red ethernet 10/100 en dos ordenadores de una misma casa, por ejemplo. Pero qué hacer cuando otra persona no se encuentra a tu lado para engancharse a un *hub*[2]. Pues eso es lo que hacen los APs si hay enlace visual a través de antenas. O quizás no os veáis pero haya alguien entremedias que quiera participar en la red y ser parte de la red. Así ya habría enlace. Otra forma de solventar los enlaces a larga distancia es montar túneles por Internet, pero para ello hace falta estar conectado a la red.

Imaginemos que Pedro quiere compartir con Rubén sus apuntes de la facultad. Vamos a suponer además que Pedro tiene Internet y que Rubén no. Sus casas no distan más de dos kilómetros pero una colina (un edificio, un accidente geográfico cualquiera) evita la visión directa. Entonces encontramos a María que ve a los dos. Y a partir de ahí tenemos la conexión hecha.

Comunidad de vecinos / ISPs pequeños

Para describir este escenario vamos a suponer que una comunidad de un edificio, desea conectarse a Internet, a la vez que quiere disponer de una página web que muestre información a los vecinos sobre reuniones, pagos de comunidad, etc.

Partamos de un edificio en el centro de una gran ciudad que dispone de 15 vecinos. Todos se han puesto de acuerdo y quieren alquilar a un proveedor de Internet por cable un acceso de 10 Mbps, el cual es demasiado caro para una sola persona, pero perfectamente asumible pagándolo entre toda la comunidad.

Cada vecino va a disponer de un ordenador en su casa (máximo dos) desde los cuales se les dará servicio de conexión a Internet. Esto hace un total de —en el peor de los casos— 30 ordenadores conectados simultáneamente a Internet.

2. *Hub* o concentrador: dispositivo que conecta muchos segmentos de una red, haciendo que funcionen como uno solo.

Dispositivos wireless

Sea cual sea el estándar que elijamos vamos a disponer principalmente de dos tipos de dispositivos:

– Dispositivos *tarjetas de red*, o TR, que serán los que tengamos integrados en nuestro ordenador, o bien conectados mediante un conector PCMCIA o USB, si estamos en un portátil, o en un slot PCI, si estamos en un ordenador de sobremesa. SUBSTITUYEN a las tarjetas de red Ethernet o Token Ring a las que estábamos acostumbrados. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos trabajando. La velocidad de transmisión/recepción de los mismos es variable, dependiendo del fabricante y de los estándares que cumpla.

– Dispositivos *puntos de acceso*, o PA, los cuales serán los encargados de recibir la información de los diferentes TR de los que conste la red, bien para su centralización bien para su encaminamiento. COMPLEMENTAN a los hubs, switches o routers, si bien los PAs pueden sustituir a los últimos pues muchos de ellos ya incorporan su funcionalidad. La velocidad de transmisión/recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumplan.

Para empezar a montar la red de nuestra comunidad de vecinos necesitaremos la siguiente infraestructura: vamos a necesitar bien de un router estándar con un punto de acceso (PA) o bien de un PA router. En cualquier caso, debería poder disponer de una toma a la que conectar una antena adicional o bien que la antena del mismo sea desmontable. El protocolo seleccionado para el PA será el 802.11g.

- Sea cual sea la elección, conectaremos al router un ordenador que será el encargado de realizar la gestión de todo el sistema. No es necesario que sea muy potente, pero sí al menos lo suficiente como para poder instalar el software de servidor web + correo electrónico, software de gestión de las comunicaciones y poco más.
- Si fuese necesario, necesitaríamos una antena con un *pigtail* (rabo de cerdo, es decir cable) que sea capaz de ubicar a la misma en el centro del edificio o en la parte más alta del mismo. Debemos tener en cuenta que cuanto más largo sea el cable de conexión a la antena más atenuación de la señal emitida/recibida tendremos.
- Cada vecino ya dispone al menos de un ordenador, al cual conectará una TR 802.11g. No es conveniente hoy por hoy mezclar tarjetas 802.11b con PA 802.11g pues provoca que éstas bajen su rendimiento de forma apreciable.

Vamos ahora a echar cuentas:

10 Mbps/30 ordenadores = 350 Kbps velocidad que es bastante buena para una conexión a Internet en el peor de los casos.

10 Mbps/15 ordenadores = 700 Kbps velocidad que es muy buena para una conexión a Internet en el mejor de los casos.

10 Mbps/1 ordenador = 10 Mbps velocidad que es bastante buena para una conexión (idílica) a Internet.

Dado el número de usuarios/ordenadores, vamos a olvidarnos de el 802.11b con sus 11/22 Mbps y nos vamos a ir al 802.11g con sus 54 Mbps.

En el tramo que hay entre el TR y el PA, nuestro PA va a ser capaz de repartir sus 54 Mbps entre los 30 ordenadores de los vecinos, lo cual hace un total de 1,8 Mbps disponibles en el peor de los casos para cada ordenador.

- Dado que en el peor de los casos cada ordenador dispone sólo de 350 Kbps para acceder a Internet, 1,8 Mbps son más que suficientes. De hecho, esta infraestructura nos permitiría teóricamente aumentar el ancho de banda de nuestra conexión por cable a Internet hasta llegar a los 54 Mbps. Realmente, el límite razonable va a estar en la mitad de esto, llegando sólo hasta alrededor de 26 Mbps.
- Desde el punto de vista de los usuarios y manteniendo un mínimo de 128 Kbps de velocidad de acceso a Internet para cada uno, y dada la conexión de 10 Mbps, teóricamente podríamos dar servicio a alrededor de 80 ordenadores/usuarios simultáneos como máximo, pero en el tramo de comunicación entre el TR y el PA, la velocidad sería de 691 Kbps con 80 usuarios. Dado que esta velocidad no está soportada, tendríamos que subir hasta 1 Mbps, lo que nos llevaría a su vez a dar servicio a 56 usuarios simultáneos como máximo.

Estas dos aproximaciones han sido hechas asumiendo que cada usuario tiene un 100% del ancho de banda de su conexión en el peor caso como CIR (el CIR es la velocidad mínima de conexión). Si suponemos un CIR más bajo para cada usuario, entonces podríamos aumentar el número de usuarios, pero teniendo en cuenta que en momentos de acceso masivo simultáneo podemos tener picos que hagan que las comunicaciones se vean apreciablemente ralentizadas.

Ya hemos visto que cada vecino puede conectarse a Internet a una velocidad razonable, pero esto sólo es teoría pues dado que el estándar 802.11g de momento no dispone de QoS (posibilidad de garantizar un ancho de banda determinado), no podemos asegurar que un solo vecino no se coma todo el ancho de banda, dejando al resto parado.

Esto es muy peligroso hoy en día dada la proliferación de las redes *peer to peer*, o redes de igual a igual de intercambio de ficheros, con ejemplos como el KaZaA, E-donkey y otros que se comerían casi por completo el ancho de banda que les diésemos.

Normalmente, dentro de los ISPs/comunidades, el 10% de los usuarios tenderían a usar el 90% del ancho de banda.

Para resolver este problema vamos a tener que recurrir algún software de gestión de comunicaciones, y más concretamente del ancho de banda, que o bien venga con el mismo PA o bien lo instalemos en la máquina de gestión del sistema. Puede ser necesario tener que instalar en el servidor el SW de servidor

RADIUS (Remote Authentication Dial-In User Service), el cual nos administrará la red como si de un pequeño ISP se tratase.

Respecto a la seguridad, es la misma de siempre, prestando especial atención al tema de que cada vecino sólo debe tener dos máquinas dadas de alta en la lista de direcciones MAC (toda tarjeta de red, independientemente del medio que utilicemos dispone de un identificador, o numerito para entendernos, llamado dirección MAC) del PA.

Hace años, mientras los fiambreras estábamos haciendo de pueblerinos en Los Ángeles, entramos en contacto con un grupo de gente latina, mexicanos y salvadoreños, que andaban a vueltas y revueltas con la policía, intentando cerrar las guerras de bandas y, por eso mismo, con la policía más encabronada aún detrás de ellos. Hablando, hablando, que si se podía hacer algo, que si un folleto, que si un vídeo... van ellos y dicen que no, que lo que les gustaría es un videojuego.

Ahí era nada en el 99 o así liarse a hacer un videojuego, sin un puto duro y tomando como guionistas a los chavales del distrito central de LA. Por supuesto, lo intentamos, pero fallábamos siempre en lo mismo: los *engines* (los macroprogramas que hacen funcionar las animaciones y la interacción en un videojuego) disponibles eran propietarios y valían una pasta; además, los programadores, sobre todo en LA aspiraban también a ser propietarios y así no íbamos a ninguna parte.

Lo que sí estaba claro es que ya entonces se veía que los videojuegos iban a ser un genero más de expresión, difusión de información y construcción de agentes políticos. No en vano, al jugar con un videojuego, se supone que tiendes a identificarte al máximo con el personaje que juegas y las situaciones que atraviesa.

Quien lo ha entendido así, sin ninguna duda, es el coronel Wardynski de la Oficina de Análisis de Recursos Económicos y Humanos (o algo así) del Ejército de los EEUU. Hasta tal punto, que ha concebido y obtenido los recursos para producir y distribuir gratuitamente «America's Army», un juego de guerra en el que el jugador se ve implicado en situaciones de combate supuestamente reales y verídicas, en las que se usan las armas y equipos oficiales del Ejército norteamericano. Se supone que es una herramienta de reclutamiento, para que los chavales le vean la gracia al tema y se alisten. La guasa, o una de las guasas al menos, es que en este juego multiusuario luchas con otros jugadores que también se han registrado y están usando el juego como tú... Pero entonces, ¿quién hace de enemigo? Pues la misma gente que está jugando contigo, sólo que ellos se ven a sí mismos como militares norteamericanos y te ven a ti como talibán o iraquí o lo que sea, justo como tú los ves a ellos. De hecho en el juego no puedes solicitar más que ser soldado americano. Quizá hubiera sido más didáctico que también hubieras podido demandar ser malo y que, en fiel reproducción de la realidad, tuvieras 10 o 100 veces más probabilidades de cascar en las primeras pantallas del juego; pero por lo visto el coro-

nel Wardynski cree demasiado en la capacidad de empatía de los videojuegos y, por eso, es mejor que no puedas ser malo ni a tortas.

La otra (?) cara de la moneda es el juego «Estado de emergencia», un juego desarrollado por una compañía escocesa para la Playstation 2, y en el cual puedes elegir jugar con alguno de entre los cinco personajes pertenecientes a las hordas de los movimientos antiglobalización y anticapitalistas. Se trata de un escenario urbano que es tomado al asalto por los grupos autónomos para destrozar McDonalds y centros comerciales protegidos por guardias privados; en las primeras versiones había antidisturbios de los de toda la vida y el enemigo era la Asociación para el Libre Comercio en América, luego ya pusieron a los seguratas y llamaron al enemigo «La Corporación», no está mal tampoco.

Naomi Klein, que como todos sabemos es la hostia de lista, ha dicho que este juego es sin duda una cooptación del anticapitalismo por parte de una compañía tan siniestra como la Sony... y algo de razón tendrá, si para ser anticapitalista tienes que comprarte una Playstation, aunque yo conozco mucha gente que no las compra.

Pero espera, si «America's Army» nos parecía malvado en la medida en que concedíamos al coronel Wardynski su parte de razón en que los chavales al jugar a ese juego sentirían ganas de alistarse de verdad (el 28% de los jugadores se da una vuelta luego por la página de alistamiento del ejercito), por qué no debería suceder lo mismo con «Estado de emergencia».

¿Quizá deberíamos pedirle a Playstation que metiera links desde el juego a Indymedia o a La Haine?

Si hicieramos nosotras el juego, ¿incluiríamos la posibilidad de poder jugar como segurata?, ¿o como delegado del gobierno?

Después de todo, ¿estaremos usando las mismas herramientas y con el mismo punto de vista —voy a ver si mientras estos chavalillos juegan se enganchan a la cosa y los alisto— que el mismísimo ejército de los EEUU? ¿Qué tipo de juego, con qué nivel de intervención y capacidad de interceptación por parte del jugador deberíamos desarrollar?

BORDERGAMES/LAVAPIÉS
Todo lo demás te parecerá un juego

Los medios y fines de un proceso pedagógico.
Enmarcado dentro de la propuesta metodológica de la investigación-acción-participación, con Bordergames pretendemos que en el proceso de construcción del videojuego participen las propias personas que viven la realidad en la que intervenir, que lo hagan tan suyo en su elaboración como en el uso posterior de esta herramienta.

Desde su propia experiencia, en el comienzo del recorrido propondrán las líneas y detalles del videojuego; y tras su elaboración técnica, al ofrecerlo a los mismos y a otros protagonistas, de nuevo lo enriquecerán en su uso, buscando y discutiendo nuevas variantes al videojuego, etc. Haciéndolo de nuevo suyo en nuevas vías de autoorganización y participación, allí donde cerramos nuestra propuesta dejándolo abierto.

Con todo esto queremos provocar debates y reflexiones sobre las causas y consecuencias de las fronteras que nos rodean (las cercanas, las lejanas, las visibles y las invisibles), e incitar a que se planteen alternativas desde un formato tan abierto, cotidiano y cada vez mas accesible como es Internet y los videojuegos; sin olvidar que, a estas alturas del tostón, unas risas nos podemos y debemos echar, y por ello, y gracias a ello, el formato videojuego, la aventura, los guiños, las trampas, etc., nos y les implica y acerca, más y mejor, en la realidad a intervenir.

Bordergames: de la subalternidad a la autonomía
Bordergames es entonces una plataforma para construir series de videojuegos que toman las fronteras como motivo de organización del juego. En ese sentido supone un trabajo de concepción, diseño y programación nada desdeñable pero sobre el que nada, o casi nada, vamos a decir aquí.

Es en otro sentido —no nos cansaremos de destacar— que Bordergames nos interesa, esto es: en la medida en que se propone y se cumple como una herramienta para que sean los más directos afectados por esas mismas fronteras quienes tomen la iniciativa de construir ellos mismos las narrativas que dirigen el juego y sus situaciones.

Bordergames es así una propuesta de autoorganización de la memoria más inmediata y una vía para convertir la propia experiencia en materia de experimentación, debate e intervención, es decir para construir la propia experiencia como situación.

No se trata entonces de enfatizar el parecido entre las fronteras y las vidas que deben articularse en función de ellas, con un videojuego más o menos ingenioso; no se trata, ya otros compañeros lo han podido hacer con más brillantez que nosotros, de destacar el aspecto de funesta aventura que la supervivencia toma cuando se viene del Sur empobrecido... Se trata de hacer que la autonomía que siempre se ha defendido desde la práctica artística se vuelva contagiosa, prolifere y fundamente la práctica política y comunicativa de otros agentes sociales.

Autonomía contagiosa

La autonomía definida desde la Ilustración como coincidencia en sí de fines y medios, como capacidad de otorgarse a sí mismo las normas del propio desarrollo, ha sido una de las banderas de la creación artística en Occidente. Capaz de emancipar el arte de la tutela de nobles y eclesiásticos, la autonomía ha sido luego tan ninguneada como podamos pensar: esterilizada e instrumentalizada en su espléndido o miserable aislamiento. No obstante parece que sigue manteniendo un temible potencial formal y político tan pronto como deja de entenderse como forzada autorreferencialidad y se convierte en constituyente de las nuevas agencialidades artísticas y políticas interconectadas.

Hacer de la autonomía una realidad política contagiosa es, también, uno de los objetivos de este proyecto.

Autonomía en este contexto significa dotarse de herramientas para que aquellos a los que se les niegan por ley los más básicos derechos políticos, sindicales y sociales puedan construirse como agentes sociales pese a las múltiples fronteras.

Extensión e intensión de la frontera

Pero las fronteras que nos interesan obviamente no están sólo en el Estrecho, vigiladas por carísimos dispositivos electrónicos o beneméritos agentes, en el capitalismo de la guerra global las fronteras traman todo tipo de realidades escondidas o fuera de foco, la inmigración es imposible de considerar al margen de la explotación y la precariedad laboral, los problemas con la vivienda, la legitimidad creciente de la okupación... Este proyecto no acaba aquí, ni vuelve a encerrar a los inmigrantes en un centro de internamiento electrónico. Bordergames conecta las diversas fronteras y se plantea como un medio de reestructurar experiencias y comunicarlas directamente a *tu cortex*, en un entorno 3d con lucecitas de colores. Un entorno en el que lo que no es juego comparece como tal y ahí te quiero ver.

Bordergames empieza en Lavapiés, con un grupo de chavales marroquíes como guionistas del juego, y puede continuar en cualquier otra plaza de Europa, África o América con gente llegada de países empobrecidos o con gente que cuestiona la legitimidad reinante del mercado de la vivienda...

Lenguaje

El juego está hecho con herramientas libres y es, él mismo, software libre. Esto quiere decir que desde el momento en que se publique, o incluso antes, cualquiera podrá copiarlo a quien quiera, modificarlo o redistribuirlo, permitiendo de esta manera que nuestros esfuerzos sean reutilizados o readaptados para articular otras realidades o necesidades. Pero, sobre todo, el hecho de que el código sea libre permite que cualquiera pueda participar en el proceso de desarrollo, no atando el producto a ninguna empresa, organización o grupo de personas, sino que por el contrario cada línea que se escribe es instantáneamente propiedad de todos, asegurándose la continuidad del proyecto y su crecimiento mientras haya gente interesada en ello (y no mientras haya dinero). Las licencias utilizadas también protegen el código de entidades malintencionadas, obligando a quien quiera utilizarlo a mantener la licencia libre y publicar sus cambios de manera que siempre repercutan en la comunidad («todos»).

Creemos que el desarrollo de software libre es la manera más eficiente de utilizar los recursos, ya que éstos no se gastan en un proyecto, sino que por el contrario van a parar a un fondo común para que la comunidad, las gentes, cualquiera, los siga tratando. A un fondo, al cual se le ha venido a llamar la mayor transferencia tecnológica del Primer Mundo hacia el Tercero, sin la cual de hecho no podríamos estar haciendo esto sin rendir tributo a gigantescas corporaciones.

Sólo gracias a la existencia de herramientas libres podemos estar haciendo proyectos como éste, sin que ello contribuya a reforzar la hegemonía de aquellos que intentan privatizar el conocimiento y ponerle contadores a la inteligencia.

Con música

No podemos trabajar con un formato como el videojuego ignorando otros formatos de producción de autonomía cultural: la música sigue siendo una de las principales maneras de construir y hacer circular referentes, modos de hacer e historias.

El hip hop y el rai, la percusión: las músicas que escuchan y que hacen nuestros guionistas son parte del plan y del juego mismo. Son

acaso la muestra más clara de una producción cultural autónoma continuamente amenazada por la cooptación y la estupidez del mercado, continuamente resurgiendo y retomando las posibilidades de autoorganización y *autoexpresión*.

Redes

Finalmente, se pretende integrar el juego en el sistema Debian, un sistema operativo basado en Linux con miles de programas libres, cuya creación sigue las mismas líneas maestras que hemos comentado para nuestro juego; un sistema que nació en el 94 y que desde entonces no ha dejado de crecer a un ritmo imparable y que se distribuye en el mundo entero, mantenido por una comunidad de miles de personas, desarrollado por cientos de miles y usado por millones. Un sistema que poco a poco se va extendiendo, que es de todos y que cuanto más se usa más crece y más se desarrolla.

No representamos nada

Es evidente: en la medida en que Bordergames sea una posibilidad no sólo de autoconstrucción de identidades, sino, sobre todo, una herramienta de coordinación y comunicación política entre grupos de migrantes, estamos dejando el campo de las representaciones, más o menos bien intencionadas —de los especialistas en producción de espectros del otro—; para internarnos en un campo en el que la producción de imágenes está inextricablemente vinculada a la producción de acción política, un campo en el que ambos órdenes de producción sólo pueden funcionar como aspectos de un mismo proceso de construcción de nuevos agentes de oposición al capitalismo. Nuestra contribución no puede ser sino de doble carácter: la modal, consistente en nuestra aportación a una herramienta como Bordergames, y la metodológica, fundamental a largo plazo, radicando en cuestionar los mecanismos de representación, en la medida en que condenan a la subalternidad y la dependencia.

Cualquier otra opción en los tiempos del despotismo castizo y el multiculturalismo de pegolete nos parecería una lamentable contribución al batiburrillo ambiente y al ruido en general.

SEGURIDAD INFORMÁTICA

«To believe is very dull.
To doubt is intensely engrossing.
To be on the alert is to live,
to be lulled into security is to die.»
Oscar Wilde

txipi
[SinDominio,
txipi@sindominio.net]*

Como dijo Wilde, vivir obsesionado por la seguridad es un poco ridículo, es casi peor el remedio que la enfermedad. Esto nos lleva a la manida frase de «la seguridad total no existe». Sin embargo, sí que podemos hacer bastantes cosas para mejorar la seguridad de nuestros ordenadores fácilmente y sin mucho esfuerzo, como comentaremos en los siguientes epígrafes.

Cuestiones como comprender por qué una contraseña es buena y otra es mala, cómo poder proteger un documento privado de forma segura, cómo navegar sin ir dejando rastro en todas las páginas web que visitemos, por qué alguien puede entrar en nuestro ordenador remotamente y destrozarlo o utilizarlo como trampolín para atacar a otro, etc., serán las que trataremos aquí, poco a poco e intentando no centrarnos en los tecnicismos sino en ideas sencillas de entender y prácticas fáciles de hacer.

UN PEQUEÑO REPASO A LA CRIPTOGRAFÍA

Criptografía, criptoanálisis, cifrado... palabras que suenan a complicadísimas operaciones matemáticas y a científicos de bata blanca llenando pizarras y pizarras de fórmulas imposibles. Sí, eso es una parte de la verdad, pero la criptografía ha sido hasta hace relativamente poco algo mucho más rudimentario y casi divertido.

Criptografía viene del griego «*kryptos*», oculto, y «*graphos*», escritor: el arte de escribir de forma oculta. Como es lógico, todo método criptográfico se ha

asociado mucho a épocas en las que el envío de mensajes ocultos era muy importante, como sucede típicamente en las guerras. Si alguien del bando enemigo logra interceptar un mensaje, las consecuencias pueden ser desastrosas. Durante el imperio romano, por ejemplo, el problema tenía solución (un cambio de estrategia), porque era muy fácil detectar que un mensaje había sido interceptado (normalmente el mensajero no vivía para contarlo). En nuestros días, esta situación cambia bastante, porque actualmente es posible interceptar un mensaje sin que el emisor ni el receptor se den cuenta. Por esta razón, es importante proteger mediante medios criptográficos la información privada que queramos enviar por la red.

Cifrar un texto no es algo muy espectacular. Sólo hace falta aplicar un «algoritmo», es decir, una receta para cifrar. Por ejemplo, vamos a cifrar el texto «La acción será mañana en la plaza» con una receta muy sencilla, «sumar 2 a todas las letras»:

– texto original: «La acción será mañana en la plaza»
– texto cifrado: «Nc ceekqo ugtc ñcpcoc go nc rncbc»

Al principio puede parecer un confuso, pero veámoslo por partes:

1. El alfabeto que hemos utilizado es este: «ABCDEFGHIJKLMNÑOPQRSTUVWXYZ».
2. Cuando queremos cifrar una letra, lo que tenemos que hacer es coger la letra que está dos posiciones hacia la derecha en ese alfabeto. Por ejemplo, para cifrar la «A», avanzamos dos posiciones hasta la «C».
3. Para descifrar, tenemos que hacer el proceso contrario, restar dos posiciones a todas las letras. Por ejemplo, para descifrar «N», retrocedemos dos posiciones en el alfabeto hasta la «L».
4. Cuando estamos en los bordes del alfabeto (al principio —«A»— o al final —«Z»—), si tenemos que cifrar o descifrar, continuamos por el otro lado. Es decir, por ejemplo, para cifrar una «Y» tenemos que avanzar dos posiciones hacia la derecha: avanzamos una hasta la «Z», y como ahora no podemos avanzar más, continuamos por el otro lado, «A». Cuando tengamos que descifrar esa «A», tendremos que ir dos posiciones hacia la izquierda, pero como no hay, continuamos por el otro lado: una posición hasta la «Z», y otra hasta la «Y».

De esta manera podemos cifrar y descifrar cualquier texto de forma muy sencilla. Con este ejemplo hemos podido ver unos cuantos elementos dentro del cifrado:

– El algoritmo o receta empleado, en este caso «sumar».
– La clave utilizada, en este caso «2». Si la clave fuese «5», habría que sumar 5 para cifrar y restar 5 para descifrar, por ejemplo.
– El texto original.
– El texto cifrado.

texto original –> algoritmo de cifrado –> texto cifrado

Este algoritmo que hemos utilizado para cifrar y descifrar es el que empleaba Julio César para enviar mensajes cifrados. Tiene el problema de que en el otro lugar hacia donde se enviaba el mensaje, también necesitaban saber la clave con la que ha sido cifrado para poder descifrarlo. Esto se resolvió utilizando pergaminos enrollados sobre una vara de madera de diferente longitud. En función de esa longitud, el receptor del mensaje ya sabía cuál había sido la clave empleada. Por ejemplo:

Longitud de la vara	Clave
10 cm	1
11 cm	2
12 cm	3
13 cm	4

Este truco sirvió en su momento, pero es bastante peligroso, porque cualquiera que se diese cuenta de ello, podría descifrar todos los mensajes. Ahí reside el problema fundamental de esta clase de algoritmos, necesitan que tanto el emisor del mensaje como el receptor conozcan la clave que se ha utilizado. Por esto mismo se los conoce como algoritmos de «secreto compartido» (el secreto es la clave utilizada) o «algoritmos simétricos».

¿Cómo transmitimos el secreto o clave para que tanto el emisor como el receptor sepan cómo cifrar y descifrar? Normalmente, se utiliza otro método que se considera seguro. Por ejemplo, si queremos enviar a un amigo 200 documentos privados por carta, un método seguro sería guardarlos en una caja fuerte y enviar la caja fuerte por correo. Bien, el problema está en que si alguien nos intercepta habitualmente la correspondencia, no podemos enviar la llave de la caja fuerte por ese mismo medio, así que necesitaremos quedar en persona con el destinatario de todos esos documentos para darle la llave en mano. Una vez que los dos tengamos una copia de la llave, podríamos utilizar la caja fuerte para enviarnos documentos privados por un canal inseguro (el sistema de Correos y Telégrafos estatal, que nos sigue la pista).

Pero claro, esto en Internet no tiene mucho sentido. No puedes ir a una tienda con tu clave en un disquete a decirles que les vas a mandar los datos cifrados con esa clave. Necesitamos una manera de pasar de forma segura a través de la red ese «secreto compartido» que es la clave. Podríamos utilizar otro algoritmo de cifrado totalmente diferente para pasar la clave, pero al final estaríamos en las mismas: ¿y cómo pasamos la clave de ese otro algoritmo por la red? Esto supuso un problema muy grande, pero se ha solucionado con un nuevo tipo de algoritmos de cifrado, los *algoritmos asimétricos* o *algoritmos de clave pública* y *clave privada*.

Entender los algoritmos asimétricos suele costar un poco, porque estamos muy acostumbrados a utilizar algoritmos simétricos, en los que la clave para cifrar y para descifrar es la misma: guardamos algo en una caja fuerte y la combinación para cerrarla es la misma que para abrirla, utilizamos un candado para la

bicicleta y la llave para cerrarlo es la misma que para abrirlo, parece lógico, ¿no? Bien, pues los algoritmos asimétricos o de clave pública y privada no funcionan así, sino que utilizan una clave para cifrar y otra diferente para descifrar. En realidad, lo que tenemos es un par de claves: la clave privada y la clave pública.

Lo curioso de estas dos claves es que todo lo que cifre una clave, lo descifra la otra y **sólo** la otra, y viceversa. Es decir, tenemos un candado con dos llaves, una roja y otra negra. Si cierro el candado con la llave roja, sólo lo podré abrir con la negra. Y si lo cierro con la llave negra, sólo lo podré abrir con la roja. ¿Qué utilidad tiene esto? ¿No es liar más la manta innecesariamente? No, sigamos con el ejemplo del candado: todos los candados que se cierren con tu llave roja, sólo podrán ser abiertos con tu llave negra y con ninguna más. Entonces lo que haces es regalar copias de tu llave roja a todo el mundo (ésta será tu clave pública), y guardar tu llave negra en casa sin dejársela a nadie (ésta será tu clave privada). Cuando alguien te quiera enviar algo privado no tiene más que coger una copia de tu llave roja, proteger el paquete con un candado cerrado con tu llave roja y así se asegurará de que sólo el que tenga la llave negra complementaria podrá abrir el paquete, es decir, sólo tú podrás abrirlo, porque tienes la llave complementaria.

De esta forma podemos utilizar un medio inseguro como Internet (para mandar información digital) o el sistema de Correos y Telégrafos (para enviar paquetes), sin ningún miedo a mandar copias de la clave pública o la llave roja del candado, porque cuando un mensaje sea cifrado con tu clave pública o cuando un paquete sea protegido con tu llave roja, *SOLAMENTE* tu clave privada podrá descifrarlo o tu llave negra podrá abrir el paquete.

Cifrado y firma de ficheros y correos (GnuPG/PGP)

Todo el proceso de cifrado y firmado digital a nivel doméstico está irremediablemente asociado a tres siglas: PGP. PGP significa «*Pretty Good Privacy*», privacidad bastante buena, y es un conjunto de programas que permiten crear pares de clave pública/clave privada, almacenarlos de forma segura, enviar correos electrónicos cifrados, firmarlos digitalmente, etc.

PGP se ha convertido en un estándar *de facto* dentro de la privacidad a nivel doméstico. Además de esto, su creador, Phil Zimmerman, se ha esforzado por crear OpenPGP, una especificación de cómo hacer programas compatibles con PGP. Actualmente PGP es una herramienta comercial propiedad de NAI (Network Associates), empresa que permite descargarse una versión personal de PGP para su evaluación.

En enero de 2001, Phil Zimmerman abandonó NAI por problemas respecto a la línea que debería seguir PGP. En ese momento Zimmerman realizó unas declaraciones históricas: *«Let me assure all PGP users that all versions of PGP produced by NAI, and PGP Security, a division of NAI, up to and including the current (January 2001) release, PGP 7.0.3, are free of back doors,...»*
(http://www.theregister.co.uk/content/archive/17064.html).

Es decir, aseguraba que hasta la versión 7.0.3 de PGP no había ninguna puerta trasera que permitiera a ningún gobierno conseguir descifrar nuestros datos de forma indirecta. Esto es un acto de fe, claro está. Podemos creer o no creer a Zimmerman, pero su reputación estaba en juego y no creemos que mintiese en esa ocasión. El caso es que a partir de esa versión ya no hay un experto en criptografía mundialmente reconocido como Zimmerman llevando el producto PGP, y nadie nos asegura que PGP 8.0 y sucesivos no contengan puertas traseras que puedan ser utilizadas por los gobiernos para descifrar nuestros correos electrónicos y nuestros ficheros cifrados. Podemos descargar una copia de la última versión certificada por Zimmerman de esta dirección:

ftp://ftp.es.pgpi.org/pub/pgp/7.0/7.0.3/PGPFW703.zip.

Podemos seguir fiándonos de los programadores de NAI o podemos optar por una versión libre de PGP, GnuPG. GnuPG es un proyecto similar a PGP y compatible con el estándar OpenGPG que tiene la característica de ser software libre. Esto nos proporciona muchas ventajas, pero entre ellas hay una muy importante en este punto: tenemos el código fuente del programa, podemos ver cómo está hecho y buscar posibles puertas traseras. Es como si en lugar de fiarnos de que el búnker que nos vende una empresa es seguro y sin puertas traseras, consiguiéramos los planos de un búnker y nos lo hiciéramos nosotros, asegurándonos que no las tendrá.

Utilizando GPG (GnuPG)

Con la idea de que comencemos a utilizar GPG para cifrar todos nuestros correos electrónicos, veremos el proceso de instalación de GPG en Microsoft Windows y GNU/Linux, así como la creación de nuestra clave pública y privada. Es conveniente cifrar todos los correos que podamos, no sólo los importantes, para que sea más difícil para quien nos espíe diferenciar los datos cifrados importantes de los irrelevantes.

La instalación y utilización de GPG en Microsoft Windows es muy sencilla si empleamos un paquete de instalación como WinPT (http://winpt.sourceforge.net/es/index.php). Mediante WinPT, la instalación de GPG se reduce a seguir los pasos guiados de un asistente:

1. Arrancar el programa de instalación

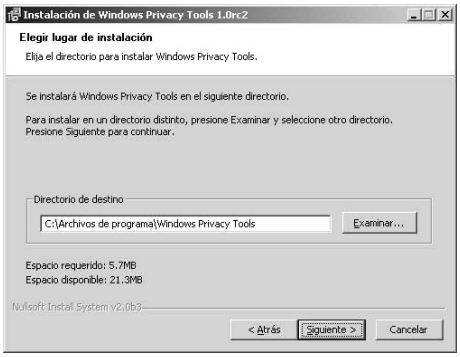
Una vez que nos hayamos descargado el programa de instalación, simplemente deberemos hacer doble clic sobre él y comenzará a ejecutarse. La primera pregunta es acerca del idioma en el que queremos instalar GPG.

Elegiremos «Castellano» y seguiremos con el asistente de instalación:

Después de darnos la bienvenida, el programa nos muestra la licencia de GPG. Al contrario que la mayoría del software para Microsoft Windows, WinPT y GPG son software libre, bajo la licencia GPL. Esto nos permite tener más libertades al utilizar y redistribuir este software, y en este caso en concreto nos proporciona la garantía de que no contiene software espía o malintencionado, lo cual es esencial dentro del software orientado a la privacidad. Aceptamos la licencia y continuamos.

2. Elegir el lugar en que instalaremos los componentes

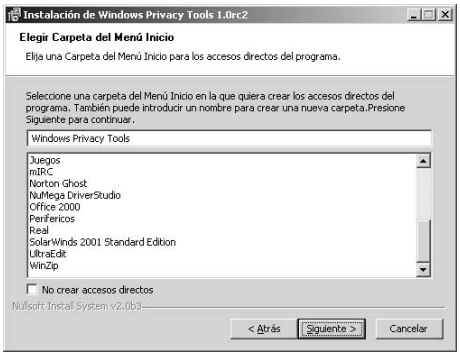
Un punto importante dentro de la instalación es decidir la carpeta de nuestro disco en la que instalaremos el programa. Por defecto el asistente nos sugiere «C:\Archivos de Programa\Windows Privacy Tools». Si no tenemos problemas de espacio en la unidad C:, ésa es una ubicación idónea.



3. Elegir los módulos que queremos instalar

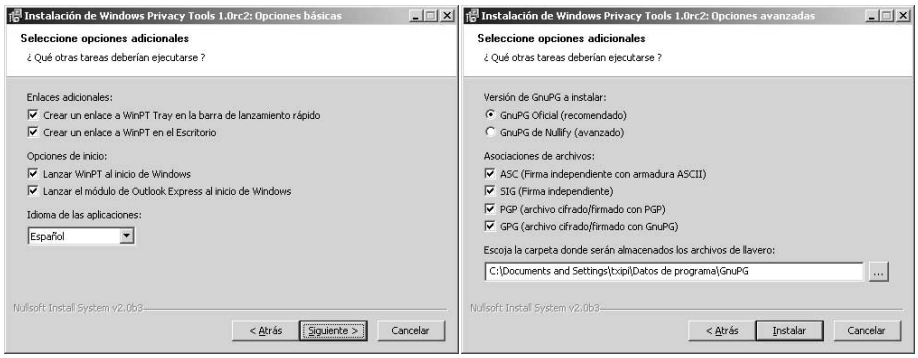
Seguidamente decidiremos qué módulos instalaremos. En caso de duda, lo mejor es seleccionar todos, fijándonos especialmente en el apartado «Módulos de correo electrónico«, donde podremos seleccionar módulos para integrar GPG con nuestros clientes de correo favoritos:

En el siguiente paso del asistente se nos pide un nombre para crear una carpeta en el menú Inicio. Lo dejaremos como está y pulsaremos «Siguiente».



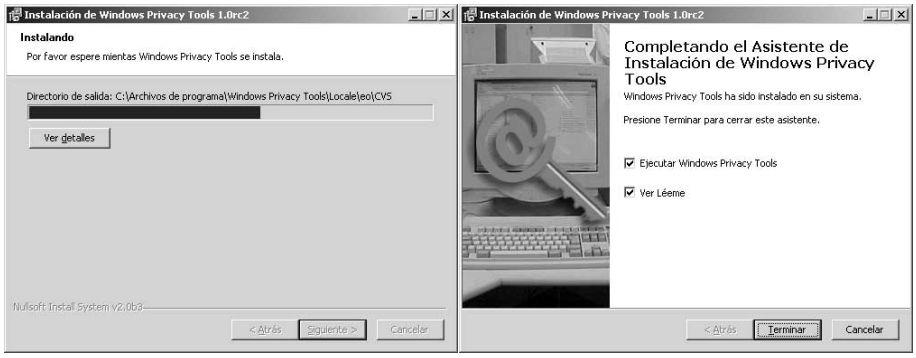
4. Configurar inicialmente GPG

Una vez instalado en disco, el asistente nos solicitará que definamos las opciones iniciales de GPG. Lo más razonable es dejarlo tal y como viene por defecto, teniendo cuidado de que esté seleccionada la opción «GnuPG oficial» en «Versión de GPG a instalar», dentro de «Opciones avanzadas»:

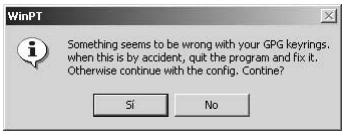


5. Instalar en disco

Una vez definido todo lo anterior, no queda sino copiar los ficheros en el disco y dar por concluido el proceso de instalación:



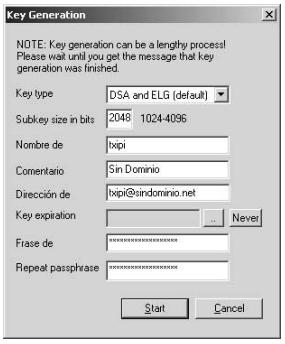
Lo siguiente que deberemos hacer, es crear nuestro primer par de claves personal. Si es la primera vez que instalamos GPG en nuestro ordenador, el asistente de instalación detectará que no hay ningún llavero de llaves GPG en el sistema y nos pedirá que creemos uno nuevo.



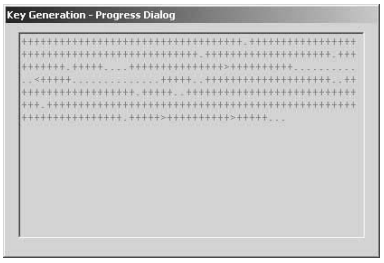
Dentro de las opciones que inicialmente se nos ofrecen, tenemos: generar un nuevo anillo o «llavero» de llaves, importar un anillo ya existente (si no es la primera vez que instalamos GPG y queremos conservar el anillo de llaves que creamos la primera vez) o importar las llaves desde un servidor. La opción que deberemos elegir es la primera, que WinPT genere un nuevo anillo de llaves:

Para generar nuestro par de llaves o claves pública y privada (es decir, crear una copia de la «llave roja» que daremos a todo el mundo y de la «llave negra» que no daremos a nadie), deberemos rellenar una serie de datos: el tipo de cifrado y tamaño de la clave que queremos (dejaremos el tipo tal y como viene —*«DSA and ELG (default)»*— y modificaremos el tamaño a 2048 bits de clave), nuestro nombre, un comentario (podemos poner lo que queramos), dirección de correo electrónico,

la fecha en la que queremos que caduque el par de claves y la *passphrase*. Normalmente la fecha indica el tiempo de vigencia de ese par de claves, aunque es habitual decir que no expira nunca. La *passphrase* es una contraseña más larga de lo normal que sirve para proteger nuestra clave privada. Aunque nos roben la clave privada, deberán adivinar esta *passphrase* para utilizarla, así que conviene poner una buena contraseña (para más indicaciones sobre cómo elegir una buena contraseña, mira el apartado siguiente):



Una vez definidos todos estos datos, pulsamos «Aceptar» (o «*Start*» en la versión en inglés) y el programa generará las claves a través de cálculos complejos (suele tardar un par de minutos).

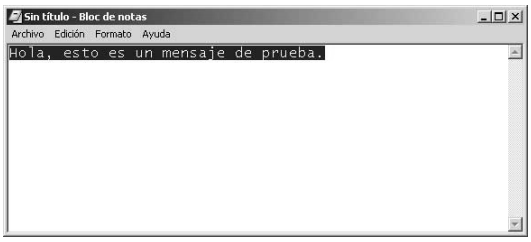


Finalmente se nos indica que es muy recomendable guardar una copia de seguridad del llavero o anillo de llaves públicas y del anillo de llaves privadas («*pubring*» y «*secring*», respectivamente). El «*secring*» deberá ser guardado en un lugar seguro, en un disquete que guardemos en una caja fuerte o algo similar, por ejemplo. El anillo de llaves públicas es menos crítico en cuanto a seguridad y podremos guardarlo donde nos apetezca.

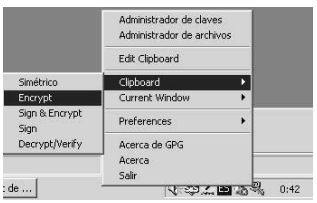
Y ya está. Eso es todo. Ya tenemos nuestro sistema de privacidad GPG listo para ser utilizado. Esto nos permitirá proteger mediante cifrado ficheros importantes de nuestro disco, correos electrónicos, etc.

Vamos a ver ahora cómo utilizar GPG para cifrar y descifrar datos dentro de nuestro ordenador.

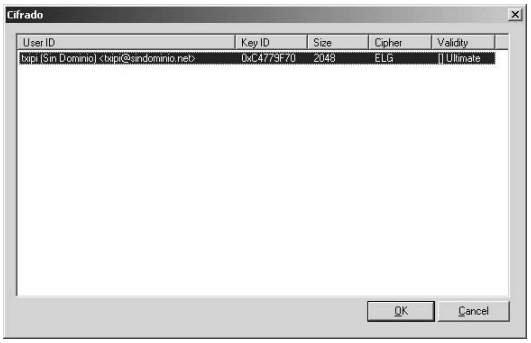
Para empezar, vamos a abrir un Bloc de Notas y escribir una frase cualquiera, por ejemplo «Hola, esto es un mensaje de prueba». La seleccionamos y la copiamos en el portapapeles para poder hacer «Copiar y Pegar» (es decir, pulsamos Control+C o elegimos «Editar: Copiar» en el menú del Bloc de Notas).



Seguidamente vamos a la esquina inferior derecha de nuestro escritorio y justo al lado de donde se muestra la hora, hay un icono como una lupa del GPG. Pulsamos con el botón derecho y se nos muestra el siguiente menú:

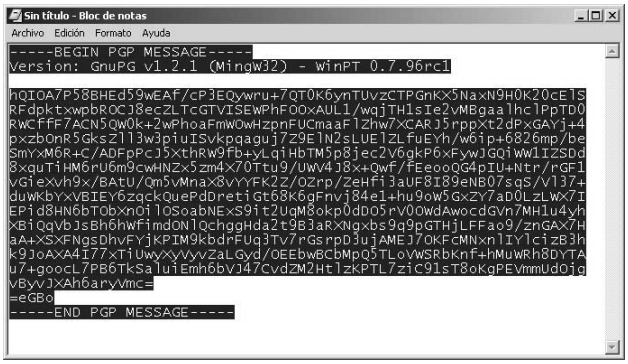


Elegimos «*Clipboard*», es decir, portapapeles, y dentro de ahí, seleccionamos «Encrypt». Se nos muestra un menú con las claves de cifrado disponibles en nuestro ordenador, y elegimos la nuestra, por ejemplo:

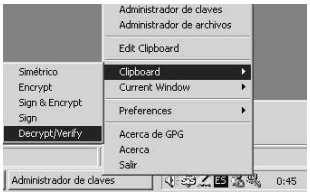


Haciendo esto habremos «*encriptado*» o cifrado lo que previamente guardamos en el portapapeles haciendo Control+C. Volvemos al Bloc de Notas y hacemos Control+V para pegar el resultado de nuestra operación (ver siguiente figura). El resultado es un bloque ininteligible de números y letras, precedido de un encabezado que muestra que eso es un bloque de datos cifrado con GPG.

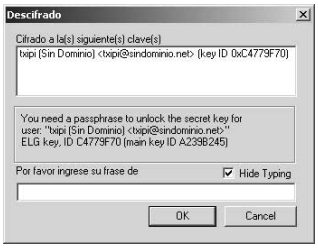
Vamos a hacer ahora el proceso inverso. Supongamos que alguien nos ha mandado un correo cifrado y lo que hemos recibido es un bloque GPG lleno de símbolos extraños. Lo primero que tenemos que hacer es copiarlo al portapapeles, seleccionándolo y pulsando Control+C o «Edición -> Copiar» dentro del menú:



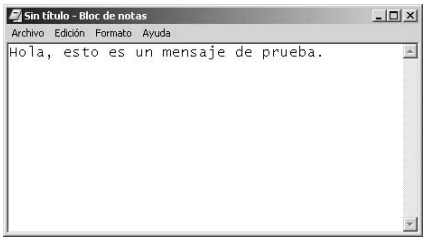
Volvemos a acceder al menú que está en la esquina inferior derecha, junto a la hora del sistema, y seleccionamos «*Clipboard: Decrypt/Verify*» para descifrar el contenido del portapapeles:



GPG comprueba que el texto ha sido cifrado con nuestra clave y nos muestra un diálogo para que introduzcamos la «*passphrase*» que protege nuestra clave privada:



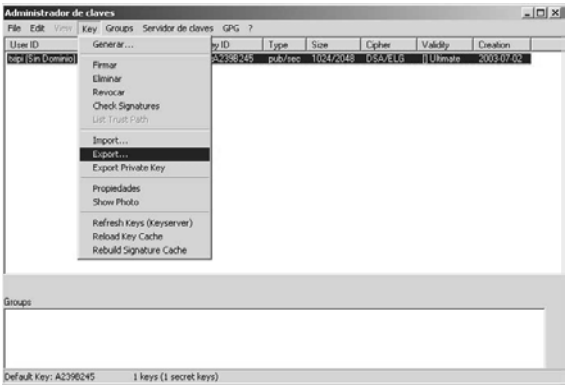
Si la introducimos mal, GPG no será capaz de acceder a la clave privada necesaria para descifrar el texto y se producirá un error. Si por el contrario hemos introducido bien la *passphrase*, el contenido del portapapeles se habrá descifrado correctamente y podremos copiarlo (con Control+V o eligiendo «Edición: Pegar») en el Bloc de Notas para leer el texto en claro:



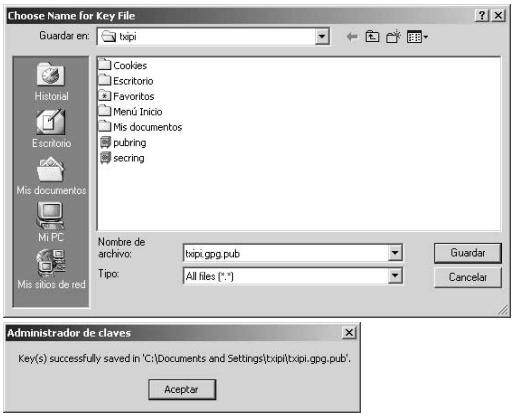
Si hemos seguido los pasos correctamente hasta aquí, ya sabremos cifrar y descifrar todos los textos que queramos mediante GPG, ya sean correos electrónicos o textos guardados en el ordenador. El método que hemos empleado es el más genérico y el más manual, para poder utilizarlo en multitud de ocasiones y con muchos programas diferentes. No obstante, algunos programas como el Outlook Express o el Eudora tienen módulos propios para cifrar y descifrar correos electrónicos cifrados con GPG de forma automática, mucho más cómodamente. En definitiva, el camino que hemos seguido es el más «rudimentario», pero entendiendo esto bien es mucho más fácil encontrar los diferentes «atajos» que tiene el sistema GPG para utilizarlo más ágilmente.

Por último, vamos a ver cómo poder exportar nuestra clave pública a un fichero de texto, para poder pasárselo a todos nuestros compañeros y que ellos

sepan *cómo nos gusta que nos cifren los datos* (recordemos todo el asunto del candado que se cierra con una llave y se abre con la otra: nosotros regalamos a todos nuestros compañeros una copia de la llave roja —la pública— y cuando la usen, sólo nuestra llave negra —nuestra llave privada— podrá abrirlo, haciendo imposible cualquier intercepción de la información). Para exportar nuestra clave pública, lanzamos el «Administrador de claves» de GPG y seleccionamos nuestra clave. Una vez hecho esto, elegimos «*Key: Export...*» en el menú:



Y se nos mostrará un diálogo en el que nos piden un nombre de fichero para guardar la clave. Elegimos «miclaveGPG.pub» o algo similar y pulsamos «Aceptar»:



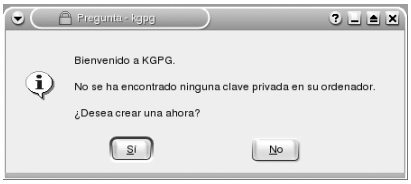
Ahora ya sólo queda distribuir este fichero a todos los compañeros que nos quieran enviar algo cifrado con GPG. Alguna gente incluye su clave pública en todos los correos electrónicos que envía, otros ponen un enlace a una página web que contiene su clave pública, otros dejan una nota diciendo que utilizan GPG y que les pidas la clave pública si la necesitas.

GPG en GNU/Linux

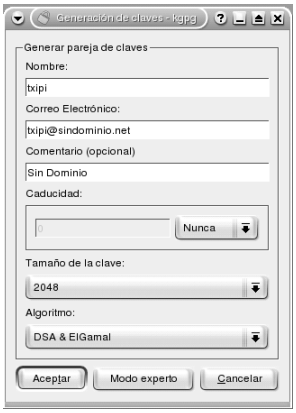
El proceso para utilizar GPG en GNU/Linux es muy similar. Aquí nos centraremos en un asistente para GnuPG llamado KGPG, basado en el entorno de ventanas KDE («The K Desktop Environment»). Muchas distribuciones de GNU/Linux lo tienen preinstalado desde el principio, en otras es necesario instalarlo. Para distribuciones basadas en Debian GNU/Linux, como Debian, Knoppix, GNOME/Live-CD, Linex, Guadalix, X-Evian, etc., basta con hacer lo siguiente (como root):

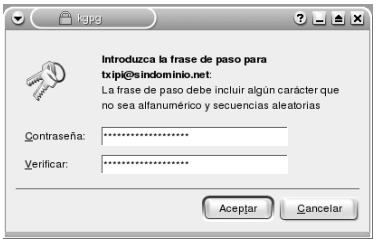
```
apt-get install kpgp
```

Una vez que está instalado, lo lanzamos escribiendo «kgpg» en una terminal del entorno de ventanas KDE. Si es la primera vez que utilizamos el programa, y no hay ningún anillo de claves creado, se nos mostrará un diálogo solicitándonos que creemos un nuevo par de claves:



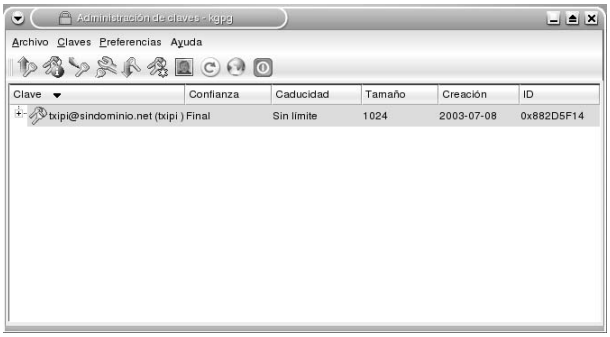
El diálogo para crear un nuevo par de claves es exactamente igual que el que hemos comentado para WinPT (GPG para Windows), así que lo rellenamos de igual forma. Seguidamente se nos pide la *passphrase* (recordemos que conviene que sea una contraseña potente). Y ya tenemos el KGPG funcionando, como muestra el icono con un candado al lado de la hora del sistema:





Para realizar todas las operaciones de cifrado, descifrado, firma digital, etc., deberemos pulsar sobre el candado de la barra de tareas, de forma similar

a cuando pulsábamos en el icono de GPG en Windows. KGPG dispone además de un programa de «Administración de claves» como en Windows, desde el que podremos exportar nuestra clave pública para que nuestros compañeros puedan utilizarla y cifrar datos exclusivamente para nosotros:



Para más información, conviene consultar:

- http://www.gnupg.org/download/.
- http://www.winpt.sourceforge.net/es/download.php/.

Esteganografía

La esteganografía es un caso particular dentro de la criptografía. La palabra también proviene del griego y significa «escritura encubierta» («*stegos*» es cubierto). El nombre es muy apropiado, puesto que mediante la esteganografía conseguimos ocultar un mensaje dentro de otro, que hará de «encubridor». Veámoslo con un ejemplo:

– texto original: «Evidentemente, siempre tienes organizada esta sala tan alegremente como Iñigo Freire recomendó antes de octubre».
– texto encubierto: «Esto esta cifrado».

El texto encubierto se consigue tomando la primera letra de cada palabra de la frase original. De esta manera, el mensaje original no parece contener información adicional y no suele levantar sospechas. Obviamente este ejemplo es muy simple, pero es posible encubrir información importante de formas mucho más sofisticadas. Hoy en día, se utiliza mucho la esteganografía para ocultar mensajes dentro de fotos o ficheros de música.

La idea es más o menos sencilla: las fotos y los ficheros de música se comprimen para que ocupen mucho menos que el original. Todos sabemos que un fichero MP3 ocupa mucho menos que el fichero que contiene la canción en un CD

UNA DE TROYANOS

A diferencia de los virus, los caballos de Troya o troyanos están diseñados para obtener información privilegiada del ordenador donde son ejecutados. Así pues, existen troyanos que únicamente consiguen contraseñas, otros que graban secuencias metidas en el teclado, otros que abren puertas traseras al ordenador, etc.

Los más conocidos últimamente son el BackOrifice y el NetBus. Ambos son troyanos que abren una puerta trasera a un equipo basado en Windows 95, Windows 98 o Windows NT.

El BackOrifice, creado por Cult of the Dead Cow, es un programa cliente/servidor para Win95/98. Al ser ejecutada la porción del servidor en una máquina Win95/98, ésta se cargará en

de audio. Esto se consigue a través de ciertos trucos, como reducir la paleta de colores utilizados en una foto cuando hay muchos colores que son casi iguales, u obviar cambios muy pequeños de frecuencias altas dentro de un MP3. Por esa misma razón, si cambiásemos un poco el color en un punto de una imagen o si cambiásemos la frecuencia un poco en un instante de una canción, no lo notaríamos. Esto se utiliza para ocultar en esos pequeños cambios información confidencial.

Una imagen dentro de un fichero del ordenador está formada por una tabla con números. Cada uno de esos números indica qué color hay que poner en cada punto de la imagen para formar la imagen total. Es como aquellos cuadernos que usábamos en nuestra infancia en los que había un dibujo sin colorear que tenía numeritos y nosotros teníamos que ir con las pinturas y pintar donde ponía un 1 en rojo, donde ponía un 2 en azul, etc. Pues el ordenador hace lo mismo con las imágenes: tiene una tabla con un montón de puntos y los números de los colores con los que se tienen que pintar esos puntos. Imaginemos que tenemos una imagen que tiene un lago muy grande y en una esquina hay una parte que es casi toda del mismo color de azul. Eso dentro del fichero estaría indicado como que cada uno de los puntitos que están en esa zona tienen el color 140, el 140, el 141, el 141, el 141, el 140, el 140 y el 139, que son diferentes tonos de azul, casi iguales. Por otro lado nosotros queremos esconder la letra «A», por ejemplo, dentro de esa foto. Para escribir una letra como la «A» es necesario que el ordenador utilice 8 bits. En concreto para la «A» el código ASCII es el 65, así que en binario sería 01000001. Lo que vamos a hacer es sumarle a aquellos números de azul que teníamos en esa parte de la foto los números de guardar una letra «A»:

fragmento de foto azul:	140	140	141	141	141	140	140	139
letra «A» (01000001):	0	1	0	0	0	0	0	1
resultado:	140	141	141	141	141	140	140	140

memoria y hará referencia a sí misma en el registro, asegurándose que se cargará cada vez que Windows se cargue. La porción del servidor es configurable a través del cliente, pero por defecto se instala como .exe («espacio».exe), sin clave de acceso, y abriendo la comunicación para que los clientes se conecten a él a través del puerto UDP 31337. La comunicación entre el BackOrifice Client/Server es cifrada, aunque ha habido informes de grupos que han conseguido romper el esquema de cifrado utilizado.

Lo único que un hacker tiene que hacer para obtener control total de la máquina de un usuario es mandarle, a través de un e-mail attachment, por ejemplo, un fichero servidor del BackOrifice. Una vez el usuario haya ejecutado este fichero, el hacker únicamente tiene que conocer la dirección IP del usuario para poder conectarse a dicha máquina. Una vez conectado, el hacker puede obtener

El fragmento de la foto ha cambiado en dos puntitos, pero sólo ha cambiado un tono en esos puntos, así que no desentona para nada. La foto se percibe prácticamente igual y nosotros hemos conseguido guardar una letra dentro de ella. Si el mensaje es mucho más grande, deberíamos escoger fotos con mucha resolución o ficheros de audio de muchos MBs, para que no se note la diferencia con el original.

Existen incluso sistemas de ficheros esteganográficos que permiten tener ficheros enteros dispersos por otros ficheros diferentes. Por ejemplo, podríamos tener un fichero con contraseñas repartido en 600 MB de ficheros de música. Podríamos copiar esos ficheros de música en un CD y pasárselos a un amigo para que, además de disfrutar de la música, pueda leer el fichero guardado esteganográficamente.

La herramienta más utilizada para encubrir datos dentro de ficheros en el mundo Windows ha sido «camouflage» (http://www.camouflagesoftware.com/). Típicamente se ha utilizado para guardar ficheros MP3 como si fueran imágenes y poder colgarlos de servidores web gratuitos. Una esteganografía tan poco sutil no consigue engañar más que al ordenador que hace de servidor web, porque cualquier persona se daría cuenta de que esas imágenes no son reales. En un MP3 de 3 MB hay tanta información que encubrir que la imagen final quedaría totalmente distorsionada. *Es fácil ocultar una aguja en un pajar, pero es bastante difícil hacer lo mismo con 7 toneladas de agujas*. En cuanto a herramientas de software libre, existen varios programas que pueden ocultar información dentro de otros ficheros:

- steghide: consigue ocultar información en JPEG, BMP, WAV y AU, cifrando el mensaje con mcrypt.
- outguess: la herramienta más utilizada para esteganografía, oculta información de diversas maneras.
- stegdetect: dentro de outguess existe una herramienta de detección de esteganografía que busca patrones esteganográficos dentro de imágenes y demás

contraseñas, bajarse ficheros, subir otros troyanos, etc. Cult of the Dead Cow indica que se puede tener más control de una maquina Win95/98 remotamente desde un cliente BackOrifice ¡que sentado enfrente de la máquina físicamente!

Existen en circulación varios programas cuyo supuesto propósito es proteger a usuarios del BackOrifice, pero que en realidad no es así. Uno de ellos, llamado BOSniffer (BOSniffer.zip) pretende ser un programa que protege las partes del registry que el BackOrifice escribe, pero en realidad no es más que un BackOrifice server. Existe otro, llamado IPSpoof (theipsoof.zip) que pretende ser una utilidad para hackers que ayuda a esconder la dirección IP del «supuesto» hacker, pudiendo así meterse en sitios del web sin poder ser identificado. Este fichero también contiene un servidor BackOrifice. El otro troyano, conocido como NetBus, es bastante similar el BackOrifice, pero introdu-

ficheros. Normalmente detecta versiones anteriores de outguess y otros programas similares.

«12345678» NO ES UNA BUENA CONTRASEÑA

Ingeniería social

Quizá a alguno de vosotros le suene el nombre de Kevin Mitnick, un auténtico mito dentro del cibervandalismo de los años ochenta. La gran mayoría de ataques a sistemas y redes que Mitnick consiguió realizar se debieron casi siempre a un par de trucos técnicos, pero, sobre todo, a su gran maestría en el campo de la ingeniería social. Mitnick era el Lazarillo de Tormes de la Era Digital, utilizaba todas las artimañas que se le iban ocurriendo para conseguir información fácilmente.

A fin de cuentas, ¿qué es la ingeniería social? La ingeniería social (una mala y literal traducción del inglés «*Social Engineering*») engloba a todas aquellas conductas útiles para conseguir información de las personas del entorno de un ordenador. No son más que engaños, algunos externos al propio sistema informático (por ejemplo: entrar en el edificio como periodistas, aprovechando la vanidad de la gente, para conseguir información importante) y otros internos (aprovechar la confianza del usuario, como por ejemplo el gusano «Kournikova» o el «I Love You» que utilizan las ganas de ver a la tenista rusa o recibir una carta de amor para colarse en el sistema).

Imaginemos la siguiente conversación ficticia entre un intruso, Kevin, y un proveedor de Internet, Neotel:

— Neotel: Buenos días, bienvenido al servicio de atención al cliente de Neotel, le atiende Juan, ¿en qué puedo ayudarle?
— Kevin: Hola, llevo toda la mañana tratando de acceder a Internet y no me funciona, ¿están teniendo problemas técnicos?
— Neotel: Nuestros sistemas funcionan correctamente, ¿qué le sucede exactamente?

ce otro peligro: también funciona bajo Windows NT. Al igual que el BackOrifice, el NetBus es de un programa cliente/servidor. El servidor por defecto escucha en el puerto 12345 UDP.

Al igual que el BackOrifice, el servidor NetBus también se está repartiendo por Internet bajo otro nombre. En este caso se esta distribuyendo como WHACKAMOLE.EXE, un juego que en realidad lleva escondido el servidor NetBus. Al ejecutar la instalación del juego, el programa de instalación también instalará el servidor NetBus.

— Kevin: Pulso en el icono de conexión a Internet y después de unos ruidos raros me sale esto... espere que lo tengo apuntado por si acaso... sí, aquí está: «Error 630, Login or password incorrect, connection refused».
— Neotel: Ha introducido erróneamente su usuario o contraseña.
— Kevin: Eso es imposible, yo no he tocado nada. ¿No será que han modificado algo y no se me ha informado? Realmente estoy muy disgustado, necesito enviar un informe a mis empleados con urgencia y llevo toda la mañana perdida con este asunto, me estoy planteando cambiar de proveedor, ¡su servicio es pésimo!
— Neotel: A ver, veamos como podemos solucionarlo... ¿es usted el titular de la línea de teléfono?
— Kevin: Así es.
— Neotel: Dígame su número de teléfono y número del Documento Nacional de Identidad.
— Kevin: 970031337, y el DNI 42573658-Z
— Neotel: De acuerdo, es usted...
— Kevin: Juan López, vivo en c/ Valdivieso, 13, 1° D.
— Neotel: Sí, eso es. Espere un momento...
ding, dong, ding ding dong, ding (música de la «Garota de Ipanema»)...
— Neotel: Bien, tome nota por favor. Su nueva contraseña es: «Phe7a31X»
— Kevin: Probaré con esta nueva contraseña, si tengo algún problema tenga por seguro que volveré a llamar.

Tal vez pueda parecer algo irreal, pero no es así. Kevin conocía los datos del verdadero titular de la cuenta en el proveedor de Internet y eso hizo asegurarse al trabajador de *Neotel* que se trataba de un cliente malhumorado. Esos datos son relativamente públicos, basta con mirar un listado de personas admitidas a unas oposiciones en un Boletín Oficial del Estado para conocer nombres, apellidos y números de DNI, o incluso direcciones, números de teléfono, etc. O más fácil aún, una simple carta

Especialistas crean troyano indetectable y lo dan al FBI

José Luis López (videosoft@videosoft.net.uy)

EN UNA GUERRA, TODO ES VÁLIDO... ¿TODO?

Cuando aún está sobre el tapete la polémica en torno a la probable nueva herramienta de espionaje que el FBI pretende usar en su guerra contra el terrorismo y el crimen en general (el troyano «Linterna mágica»), el conocido grupo de hackers creador del famoso BackOrifice —un troyano que permite el control total de una computadora en forma remota— anuncia que colaborará con el FBI para crear una versión totalmente actualizada de su herramienta, la que además sería indetectable por los antivirus actuales.

de un proveedor de Internet informando de una nueva oferta a uno de sus clientes puede contener toda la información necesaria para que se reproduzca la conversación anterior. ¿Debemos incinerar toda la propaganda que llega a nuestro buzones?

La ingeniería social, como veremos, es un factor clave a la hora de adivinar una contraseña.

¿Cómo se guardan las contraseñas?

En la mayoría de los sistemas, las contraseñas se guardan en el mismo sitio en el que hay otra información importante para cada usuario, como su nombre, sus configuraciones, etc. Ese lugar normalmente es accedido por muchos programas y personas que necesitan información de un usuario en concreto, como por ejemplo saber si ese usuario tiene permisos para entrar en una determinada carpeta o saber el lenguaje preferido por el usuario para mostrar una pantalla en un idioma o en otro, etc. Toda esta información referente a los usuarios de un sistema suele guardarse en un fichero. En GNU/Linux y la mayoría de sistemas UNIX este fichero está en /etc/passwd, en Microsoft Windows su ubicación varía dependiendo de la versión que se utilice.

Como podemos intuir, ese fichero tiene que ser accedido por muchas personas y programas y además contiene las contraseñas del sistema, así que tenemos un problema. No podemos guardar las contraseñas sin más, porque cualquiera podría leerlas. Tenemos que cifrarlas, pero si las ciframos utilizando un método simple, pronto alguien lo adivinará y podrá conseguir todas las contraseñas. Por esa misma razón, las contraseñas en un sistema se cifran con un método de cifrado indescifrable. ¿Cómo? ¿De qué nos sirve cifrar algo de tal manera que no exista un método para hacer la operación contraria? Responderemos *a la gallega* con otra pregunta: ¿para qué usamos las contraseñas que hemos cifrado en ese fichero? Para comprobar si la contraseña que nos han pasado por teclado es correcta. Pero claro, no podemos descifrarlas para comprobar si es correcto lo que el usua-

Los enemigos de mis amigos serán mis amigos

El grupo Cult of the Dead Cow (Culto de la Vaca Muerta) o cDc ha alcanzado su máxima fama con la creación de la que ellos llaman una herramienta de intrusión y administración remota.

No es la primera vez que pretenden blanquear su condición, con el argumento de que BackOrifice (BO) es una herramienta legítima para acceder en forma remota a otro PC. Lo cierto de esto último es sólo la parte de que una herramienta de ese tipo puede sernos muy útil, sobre todo cuando debemos resolver problemas o administrar un PC en forma remota.

Pero lo que no es cierto es que BackOrifice en su estado actual pueda considerarse una herramienta legítima, porque no fue creada como tal, sino para actuar en forma totalmente furtiva, de modo que se pueda controlar la computadora de una víctima sin su consentimiento.

rio ha introducido por teclado. El truco está en cifrar lo que el usuario ha introducido y comparar cifrado con cifrado:

```
Usuario (teclado)
        contraseña: hola ————————ciframos————————> RAZFC72ckD/g2 (hola cifrado)
Sistema (fichero/etc/passwd)                        ll ? (SÍ, Acceso concedido)
        contraseña:???? <—NO PODEMOS DESCIFRAR!!— RAZFC72ckD/g2 (hola cifrado)
```

Al utilizar estos algoritmos de cifrado indescifrable o *de un solo sentido* («*only-one-way*»), no podemos descifrar la contraseña, pero podemos aplicar ese mismo algoritmo a lo que nos han pasado por teclado y comparar el resultado cifrado con la contraseña cifrada. Con estos algoritmos, *sólo podemos ir hacia la derecha*, es decir, sólo podemos cifrar. De esta forma cumplimos los dos objetivos iniciales:

- Cuando un usuario introduce su clave, podemos comprobar si es la correcta (cifrándola y comprobando si el resultado coincide con lo que nosotros tenemos almacenado).
- Si alguien consigue arrebatarnos la clave cifrada (el texto «RAZFC72ckD/g2», por ejemplo), no puede descifrarla, porque hemos utilizado un algoritmo de cifrado de sólo un sentido y no es posible hacer la operación inversa.

Imaginemos otro algoritmo irreversible, por ejemplo, «contar el número de letras de una frase». Si alguien pusiera «hola, me llamo Juan» el resultado de ese algoritmo sería 15 letras. Si ahora alguien toma ese 15 como dato de partida, es imposible que llegue a la conclusión de que la frase origen era «hola, me llamo Juan», porque se ha perdido información relevante mientras se hacía el proceso. Está claro que este ejemplo no valdría para guardar contraseñas, pero explica el concepto de algoritmos irreversibles o de un solo sentido.

Ésta es la razón por la que los antivirus la identifican como un troyano.

Es irónico pensar que en la controversia generada por el troyano Linterna Mágica, y la decisión en su momento de un fabricante de antivirus de no detectarlo (cosa que ahora desmiente), haya tenido un antecedente cerca de un año atrás, justamente con el Back Orifice y la misma empresa de antivirus, y su anuncio de que dejaría de detectar como troyano al BO, por considerarlo una herramienta, decisión que luego fue dejada en el olvido, presuntamente debido a las presiones del momento...

UN GUSANO INDETECTABLE

Eso es lo que dice cDc. Y aunque sus intenciones puedan parecer buenas (o al menos patrióticas, que

Ataques de diccionario

Acabamos de decir que los algoritmos de un solo sentido son la mejor manera para guardar contraseñas (esto es cierto), y que cualquier contraseña almacenada así no puede ser descifrada (esto no es tan cierto, ahora veremos por qué). Cuando nosotros conseguimos arrebatar la contraseña a alguien en su forma cifrada (así: «RAZFC72ckD/g2», siguiendo el ejemplo de antes), no podemos utilizar una receta para tomar ese galimatías y generar la contraseña descifrada («hola», en este ejemplo), pero lo que sí que podemos hacer es aplicar el algoritmo de cifrado a todas las palabras del diccionario, hasta encontrar una cuyo galimatías coincida con el que nosotros hemos conseguido arrebatar.

No podemos *ir hacia la izquierda*, es decir, descifrar la contraseña, pero podemos ir tantas veces como queramos *hacia la derecha* (cifrar palabras), hasta dar con el resultado. Así, lo más habitual es coger todas las palabras de un diccionario, y aplicarles el algoritmo de cifrado, hasta dar con la palabra correcta:

Diccionario		Palabra cifrada		Contraseña		
a	——>	hYZeSQW6JtO/6	=	RAZFC72ckD/g2 ?	——>	NO
ab	——>	6ZmfTPHvQfMBo	=	RAZFC72ckD/g2 ?	——>	NO
ababa	——>	LZGyE2g1HxVl6	=	RAZFC72ckD/g2 ?	——>	NO
ababillarse	——>	gZL1zEPlc4Pm2	=	RAZFC72ckD/g2 ?	——>	NO
ababol	——>	aqX5qKqDy/eE	=	RAZFC72ckD/g2 ?	——>	NO
hojuela	——>	IaxLbY/4G50r6	=	RAZFC72ckD/g2 ?	——>	NO
hojoso	——>	XapGN/ph3zhzI	=	RAZFC72ckD/g2 ?	——>	NO
hola	——>	RAZFC72ckD/g2	=	RAZFC72ckD/g2 ?	——>	¡¡¡SÍ!!!, la contraseña es «hola»

Probamos secuencialmente con todas las palabras del diccionario, hasta encontrarla. Estas listas de palabras suelen hacerse cogiendo todas las pala-

no es lo mismo), es lógico pensar que quienes deseen colaborar en la lucha contra el terrorismo, lo hagan desde su especialización, y ese es el primer argumento del grupo cDc.

El diseño del nuevo BO se haría bajo estrictas reglas, como por ejemplo, no compartir el código fuente, mantenerlo en un estricto secreto y jamás distribuirlo en público, para evitar el descubrimiento por parte de los laboratorios de antivirus.

LLÁMESELE COMO SE QUIERA, PERO SIGUE SIENDO UN INTRUSO

La herramienta, que sería entregada sólo al gobierno (al FBI en principio) una vez terminada, pretende ser un arma eficaz contra el fraude en Internet, el robo de identidad (hacerse pasar por otro), los escritores de virus y la pornografía infantil, entre otros. Un arma capaz de interceptar cualquier

bras del inglés, todas las del castellano, todas las del italiano, nombres de ciudades, de equipos deportivos, de famosos, etc., y al final lo que obtenemos es un listado gigantesco de posibles contraseñas con las que probar este ataque de diccionario.

A simple vista podemos extraer dos conclusiones de todo esto:

- Elegir como contraseña una palabra que esté en el diccionario **NO** es una buena idea, aunque sea «esternocleidomastoideo» o «*unterschiedlichen*».
- Contra un ataque de diccionario, una contraseña que empiece por x, y o z tiene menos probabilidades de ser acertada rápidamente, puesto que los listados con diccionarios suelen ordenarse alfabéticamente.

Aquí puede entrar en juego también la ingeniería social: si queremos tener suerte a la hora de reventar la contraseña de una persona en concreto y sabemos que está loco por todo lo relacionado con *El Señor de los Anillos*, podemos meter en el diccionario todos los nombres, lugares y palabras características de ese tema, y seguramente tengamos suerte.

Evidentemente todo esto no se hace de forma manual, existen muchos programas para crackear contraseñas, aunque el más famoso de todos es el «*John the Ripper*». La versión para Windows funciona relativamente bien, aunque es un programa pensado para el mundo UNIX en general, así que tiene más sentido utilizarlo desde GNU/Linux o sistemas BSD. Para instalarlo en Debian GNU/Linux basta con escribir (como root):

```
apt-get install john
```

Veamos un ejemplo de su uso: en diccionario.txt tengo mi diccionario de posibles contraseñas, mostraré las 50 últimas para que sea más fácil entender cómo es, posteriormente atacaré el fichero de contraseñas utilizando como diccionario mi fichero «diccionario.txt»:

clase de crímenes que se puedan cometer con una computadora. Y de seguir el rastro aún después de cometidos estos crímenes.

Incluirá analizadores de imagen para reconocer datos críticos en cualquier fotografía, como por ejemplo logotipos o banderas usadas por los terroristas, identificación de los más buscados, etc.

En su sitio, Cult of the Dead Cow explica en forma mucho más detallada el porqué de su decisión de crear algo así, y de ofrecerlo al gobierno de forma totalmente desinteresada.

El grupo de hackers informa también de que BackOrifice será rediseñado de forma que no pueda ser detectado por las herramientas de seguridad, precisando además que la nueva versión será para uso exclusivo del FBI.

Y lo de indetectable es relativo, ya que, tarde o temprano, cualquier investigador serio y respon-

```
# tail -50 diccionario.txt

zyuuzyun zyuuzyut zyuuzyuu zyuwaki zyuyo zyuyou zyuyouki zyuzou zyuzu zyu-
zutsu zyuzutu zyuzutun zyuzyou zyuzyu zyuzyuts zyuzyutu zyweck zywicki zywiel
zyxenhujul zyzomys zyzzoget zyzzogeton zyzzy zyzzyva zyzzyvas zz zzalsrh zzang
zzapsid zzdean zzdlg zzekka zzetsu zzetsuen zzetu zzgl zzhi zzppyyx zztop zztop-
man zzyzx zzyzyx zzz zzzz zzzzz zzzzzz zzzzzzz zzzzzzzz zzzzzzzzzzzzzzz

# john -w=diccionario.txt /etc/shadow
Loaded 1 password (FreeBSD MD5 [32/32])
hola                (prueba)
guesses: 1 time: 0:00:03:26 100% c/s: 3024 trying: hola
```

En mi fichero de contraseñas (/etc/shadow) sólo tenía al usuario «prueba», con la contraseña que hemos puesto antes, «hola». Como vemos, ha tardado 3 minutos y 26 segundos en adivinar la contraseña, comprobando a una velocidad de 3.024 claves por segundo, mientras iba probando por la palabra «hola» dentro del diccionario.

Ataques incrementales por fuerza bruta

Como muchas estaréis pensando, no todas las contraseñas son palabras del diccionario, algunas incluso no son ni pronunciables y contienen números y letras mezclados. En estos casos se usa un enfoque incremental para crackear las contraseñas, probando absolutamente todas las combinaciones: primero todas las de una letra, luego las de dos letras, luego las de tres, etc. De esta manera nos aseguramos que al final la contraseña será adivinada (probamos absolutamente todas las posibilidades), pero puede darse el caso de que la contraseña sea lo suficientemente grande y compleja como para que el tiempo que necesitemos sea de varios años.

sable descubrirá la forma de detectarlo, cuando el troyano establezca algún tipo de comunicación con su entorno.

Pero lo peor de todo esto es que lo llamemos como lo llamemos (Linterna Mágica o Back Orifice), seguirá siendo un programa intrusivo, capaz de establecerse en nuestra computadora y de robarnos información, sin nuestro conocimiento.

Y esto... puede ser peor que la enfermedad, ¿no le parece?

Normalmente en todo ese tiempo un usuario que haya puesto una contraseña buena, la habrá cambiado varias veces, así que nuestro trabajo no valdría para nada. (Nota: actualmente proyectos como LASEC (http://lasecwww.epfl.ch) llevan a cabo una estrategia bastante inteligente: almacenar en una base de datos inmensa (unos 4 TB para contraseñas de Windows NT) todas las posibles combinaciones de letras y números y su correspondiente texto cifrado; así, cuando alguien quiera crackear algo solamente hay que buscar en esa base de datos por el texto cifrado solicitado, en muy poco tiempo).

Veamos un nuevo ejemplo de utilización del «John the Ripper», mediante el enfoque incremental:

```
# john -incremental /etc/shadow
Loaded 1 password (FreeBSD MD5 [32/32])
hola                (prueba)
guesses: 1 time: 0:00:17:12 c/s: 2887 trying: hola
```

Como vemos, ha tardado bastante más que con el enfoque por diccionario (17 minutos contra 3 minutos), porque «hola» es una palabra del diccionario. Si hubiéramos puesto algo que no está en el diccionario, como por ejemplo «4tq2», con este enfoque habríamos tardado lo mismo, mientras que con el ataque por diccionario nunca lo habríamos resuelto.

Las cosas que deberemos tener en cuenta para evitar un ataque de este tipo son claras: el tamaño de nuestra contraseña, cuanto más grande sea, más difícil será adivinarla, y la complejidad de la contraseña, mezclando letras mayúsculas y minúsculas, números y caracteres raros como @, #, !, etc. Muchos ataques incrementales sólo prueban letras y números y no son eficaces contra combinaciones raras de letras, símbolos especiales, etc.

INFOMIXER

El Infomixer se basa en el clásico programa Perl «Travesty», que hace una extraña parodia de cualquier texto o colección de textos reordenándolos a partir de la frecuencia con la que aparecen pares de palabras determinados. Plagiarist.org ya usó Travesty para hacer su manifiesto plagiario allá por el 98, remezclando los manifiestos más o menos famosos de otra gente. No teníamos nada nuevo que decir, pero lo importante es que lo dijimos con un montón de convicción. Como en plagiarist.org somos tan entusiastas del Travesty, decidimos homenajearlo haciendo este Infomixer para remezclar las declaraciones y discursitos de relaciones públicas de grandes corporaciones.

Consejos prácticos

Para resumir, siguiendo estos consejos podremos inventarnos una buena contraseña:

- No utilizar nunca una palabra del diccionario, en ningún idioma conocido (*klingon* o *élfico* incluidos), por muy larga o extraña que pueda parecer.
- Intentar evitar combinaciones que empiecen por las primeras letras del alfabeto, para ponérselo un poco más difícil a un ataque incremental.
- No utilizar palabras relacionadas con nuestras aficiones, el nombre de nuestra novia, hijas, etc. Es probable que el atacante pueda conocer esos datos.
- Bajo ningún concepto usar la «*pregunta relacionada*». En algunos sitios como Yahoo o Hotmail nos permiten utilizar una pregunta para recordar nuestra contraseña. «¿Cuál es el nombre de tu mascota?», «¿cómo se llama tu madre?», etc., son preguntas típicas que podremos usar. Si respondemos bien a esa pregunta, se nos envía un correo con nuestra contraseña. De nada sirve una contraseña buena, si utilizamos una pregunta de recordatorio demasiado fácil. Ya sabemos que la cadena siempre se rompe por el eslabón más débil, así que éste podría ser un buen método para que alguien consiguiera nuestra contraseña. Tener como contraseña «23IhXt-wll@er3X» es inútil, si luego en la pregunta para recordarla pones: «¿Cuál es mi pueblo de veraneo?», y en tu página web dices que eres de la peña de fiestas de Valdemorillo de las Cañas.
- En cuestión de contraseñas, «*size DOES matter*», el tamaño importa.
- Combinar mayúsculas, minúsculas, números y caracteres especiales pondrá las cosas más difíciles a quien quiera crackear nuestra contraseña.
- Si lo que necesitamos en una «*passphrase*», es decir, una contraseña que normalmente tiene que ser muy larga porque lo que protegemos es importante, no dudaremos en utilizar espacios a la hora de definir la *passphrase*. Por ejemplo, una buena *passphrase* podría ser: «Biba la vid@, y biba lamorl!!».

Dada la sabiduría de Travesty para encontrar similitudes entre textos, ésta era la herramienta ideal.

Pero, ¿por qué hacerlo con textos de relaciones públicas de grandes empresas?
Habíamos notado un montón de curiosas coincidencias entre los textos que las grandes empresas escriben sobre sí mismas. Eran increíblemente parecidos, resultando impersonales, formulosos, etc. A ver si iba a resultar que los expertos en relaciones públicas eran una panda de hipócritas que se limitaban a arrejuntar un montón de lugares comunes de las relaciones públicas (?). Pero tampoco había que verlo de ese modo, al fin y al cabo, hay que ver lo igual que suena tanta y tanta música dance, y ahí llegan los dj's, la remezclan y aquello cobra vidilla. Quizá desde plagiarist.org se podía hacer algo parecido animando los sosos textos con un programa tan guays como éste.

Uffff... ¡qué pereza! ¡Si quiero poner una contraseña siguiendo todos esos consejos, al final nunca me voy a acordar de ella! No desesperes, existen trucos muy buenos:

1. Coge una frase que te guste. Por ejemplo: «Verde que te quiero verde».
2. Quita los espacios y sustitúyelos por mayúsculas: «VerdeQueTeQuieroVerde».
3. Cambia algunas letras por números, el 3 es una E al revés, el 0 puede ser una O, la @ la cambiamos por la Q... usa tu imaginación: «V3rd3@u3T3@ui3r0V3rd3».
4. Esa contraseña ya es potentísima, pero no nos vamos a acordar. Cogemos las 10 primeras letras, y nos queda: «V3rd3@u3T3», o sea, «verdequete» escrito a nuestro estilo personal, una contraseña bastante difícil de crackear.

Naveguemos sin dejar rastro

Echelon, Carnivore y Passport.Net

Desde los comienzos de Internet, cuando la antigua Arpanet tenía mucho más de aldea que de global, el proyecto Echelon ya funcionaba interceptando contenidos considerados como peligrosos en las comunicaciones electrónicas. En un principio nadie quiso creer paranoicas historias sobre sistemas de espionaje computerizado, satélites vigilando noche y día nuestras comunicaciones, filtros de correo electrónico, etc. Todo parecía sacado de una vieja película de espías. Sin embargo, 30 años después de su constitución en 1971, el Parlamento Europeo hizo pública su existencia en mayo de 2001:

> *No hay ninguna razón para seguir dudando de la existencia de un sistema de intercepción de las comunicaciones a nivel mundial en el que participan los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda en el marco del Acuerdo UK/USA; considerando, asimismo, que según las informaciones de que se dispone, es probable que su nombre sea*

¿Vale y cómo puedo usarlo?

De un par de maneras, puedes jugar con él en la página de plagiarist.org con las webs corporativas que tenemos preseleccionadas, o puedes bajarte el programa desde la misma página y montártelo con los textos que más gracia te hagan: puedes probar con las declaraciones de diferentes políticos, con las centrales de la acp. Infomixer no tiene límites.

¿No tengo ni idea de Perl, de Travesty ni de programación, puedo usarlo aun siendo así de torpe?

Por supuesto y para eso estamos en plagiarist.org, que somos tan majas que lo hemos adaptado para que lo puedas usar como cualquier script de CGI que, aunque aún no sepas lo que es, está chupado, de veras.

> *«ECHELON», si bien no es éste un aspecto de importancia primordial (...) El sistema no se utiliza para interceptar comunicaciones militares, sino privadas y económicas.*
>
> (Informe de la UE sobre Echelon)

Como vemos, el sistema está orientado al espionaje del ciudadano de a pie en su vida cotidiana; atrás quedó el espionaje militar de la Guerra Fría, todo el mundo es un enemigo potencial. No sólo las comunicaciones personales por Internet son filtradas y espiadas, sino muchas conversaciones telefónicas, celulares, fax y GPS. Funciona con un sistema de «palabras clave» que activan el filtrado. Un ejemplo bastante escandaloso de este sistema es el que se relató en el programa «*60 minutes*» de la CBS. Una mujer hablaba por teléfono con una amiga explicándole que su hijo hizo un papel durante una obra de teatro en el colegio, usando la expresión «*he bombed*» (literalmente «puso una bomba», pero también en sentido figurado «fue muy deprisa»). El sistema detectó automáticamente la expresión, y su nombre y datos personales fueron a parar a la base de datos de posibles terroristas. El «mejor» Gran Hermano jamás diseñado ha estado más de un cuarto de siglo espiando conversaciones por todo el mundo. La alianza entre las agencias de seguridad e inteligencia de todos sus participantes se han cubierto las espaldas en el terreno legal: es ilegal que un gobierno espíe a sus propios ciudadanos y mandatarios, pero siempre es posible pedir «favores» al resto de participantes en este sentido. Margaret Tatcher hizo uso de estos favores y espió a varios miembros de su gabinete solicitando informes a sus colegas canadienses. Organizaciones como Greenpeace o Amnistía Internacional han sido también espiadas, como se ha reconocido públicamente.

Obviamente esto sólo es la punta del iceberg; sin embargo, cada vez la cantidad de información que hay que tratar se va haciendo más inmanejable y su eficacia está cayendo poco a poco. Por esto mismo, la NSA, Agencia de Seguridad Nacional de Estados Unidos, y el FBI están desarrollando nuevas herramientas para

¿Y donde puedo encontrar más información sobre el Travesty este o lo que otra gente hace con él?
Pues en el medio de megametamasas que es Google, por supuesto, y también en distribuciones de Perl o en sitios como: www.geek-girl.com/perl/programming_perl/ch6/travesty.
La implementación más popular de Travesty en Perl se basa en un algoritmo publicado en el 84 en: http://infomix.plagiarist.org/corp/frameset.html.

aumentar la capilaridad de sus sistemas de filtrado y espionaje. En este sentido destacan las colaboraciones de empresas que guían gran parte del futuro de Internet como Microsoft o Cisco, líderes en el mercado del software y el hardware de equipamientos de red respectivamente. Ambas empresas han manifestado públicamente que supeditarán la privacidad de sus usuarios a los intereses de la NSA y FBI en cuestiones de seguridad. Este colaboracionismo se ha visto como algo muy negativo dentro de los grupos de usuarios concienciados con el tema, pero la gran mayoría de sus consumidores no se detienen a observar estos puntos de la licencia EULA («*End User License Agreement*») que aceptamos cada vez que instalamos uno de sus productos.

Además de los acuerdos de colaboración con Microsoft o Cisco entre otros, el FBI ha contado con la colaboración de hackers afamados como el grupo *Cult of the Dead Cow*, creador de la famosa herramienta de «administración remota» de sistemas (a veces considerada como software espía o troyano) «*Back Orifice*». Esto le ha hecho trabajar en la creación de programas espía («*spyware*») como «*Magic Lantern*» o «*Cyber Knight*», programas capaces de editar el registro de Microsoft Windows, detectar claves secretas, manipular archivos o espiar conversaciones por chat, *Messenger* o *ICQ*.

Carnivore es un proyecto en este mismo sentido. En palabras de los propios representantes del FBI: «Carnivore es un sistema computacional diseñado para permitir al FBI, en colaboración con un proveedor de Internet (ISP), que se haga valer una orden judicial que exige la recolección de cierta información en relación al correo electrónico u otros tipos de comunicaciones electrónicas de un usuario específico que es objeto de investigación». Como podemos ver, Carnivore solicita la colaboración de los proveedores de Internet, pidiendo los registros de correos electrónicos enviados o recibidos por y para una persona en concreto. Esto es bastante similar a lo que exige la reciente Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE), que obliga a guardar los registros de todo lo que sucede en proveedores de Internet y demás empresas que desarrollen

AGENTES

Un agente es una especie de programa que realiza tareas, como cualquier programa que se precie, pero que a la vez es capaz de ir aprendiendo de las «prioridades» de sus usuarios para así ir tomando iniciativas y hacerle ofertas que le permitan ganar tiempo. Los programas que usan las agencias de viajes que venden billetes por Internet son agentes: aprenden que vas a Castellón todas las Navidades, de forma que en vez de esperar a que les pidas el billete, dos meses antes te buscan uno más barato y te lo ofrecen por si cuela. De paso, si les dices el nombre de tu madre, pues igual te recuerdan el día de su santo y te venden un ramo de flores electrónicas. Así de limpio y de conveniente es el nuevo capitalismo personalizado, donde se trata de contar con la información sobre tus

actividades comerciales en Internet. A pesar de las protestas de asociaciones de internautas y grupos sociales relacionados con la telemática, el gobierno español ha seguido adelante con la ley, cuyo reglamento es a día de hoy una incógnita y podrá afectar muy negativamente a las libertades digitales de mucha gente.

Por otro lado, sistemas como Microsoft Passport.Net pueden ser una amenaza grande contra la intimidad de los «*netizens*» o ciudadanos de la red. Mediante Passport.Net es posible introducir un usuario y contraseña en uno de los sitios en los que se utilice y no tener que volver a enseñar ese «pasaporte virtual» en el resto de sitios que funcionan con este sistema. Es muy habitual que entremos en Hotmail a revisar nuestro correo, vayamos a *Amazon.com* a comprar un libro o a Ebay a buscar algo en sus subastas, y que esos sitios nos reconozcan al entrar y nos muestren nuestras preferencias, etc. Esto no supondría mayor riesgo si el sistema no pudiera utilizarse para hacer correlaciones complejas que dieran más información que la estrictamente necesaria para cada una de esas tiendas virtuales. Pongamos un ejemplo: si un hombre mediante Passport.Net compra unos pantys en una web de lencería, cualquiera podría pensar que son para su madre, hermana o novia. Si mediante este mismo sistema se hace con el mapa de calles de Leganés, es probable que vaya a pasar una temporada por allí, de vacaciones o por trabajo. Si además de esto, se compra una escopeta de caza, el sitio que se la vende pensará que tiene un coto privado, y si compra una sierra para cortar metales, es probable que quiera hacer obras en las cañerías de casa. El «problema» para este sujeto le vendrá cuando se analicen todos estos datos a la vez, junto con la noticia de que un encapuchado ha asaltado una caja de ahorros en Leganés a punta de escopeta recortada. Quizá éste sea más un contraejemplo que un ejemplo de las maldades de este sistema, pero me gusta especialmente porque cuando lo escuché en una charla sobre estos temas me pareció tremendamente gráfico.

Después de esto, podemos ser todo lo paranoicos que queramos (siempre sin olvidar la frase del comienzo: la seguridad y privacidad total no existen).

trayectorias personales, de forma que ellos puedan estar allí antes que tú y montar el mercadillo para venderte lo que saben que vas a necesitar.

Si en algún momento se inventaron las necesidades de masas, ahora te han inventado a ti, compañero, y más te vale parecerte a la imagen que los agentes irán construyendo de ti porque si no va a ser esto una paliza de aquí te espero.

Nuestro amigo Sintron, de nuevo, pilló onda muy rápidamente y se puso a construir DeathCo, algo así como Muerte y Cía, un dispositivo de fabricación en serie de agentes electrónicos.

Con Muerte y Cía. podrías ir definiendo mediante tus acciones y tus comunicaciones cuál es tu estilo y tu modo de hacer las cosas, de forma que al cabo de algún tiempo el «agente» producido por el programa podría responder por ti a un buen porcentaje de e-mails, participar en chats y con-

Estos enlaces servirán de guía para quien quiera ahondar en estos temas:

- «Echelon y la gran familia», por Arturo Quirantes, muy recomendable: http://www.ugr.es/~aquiran/cripto/informes/info025.htm.
- «La protección de datos personales en Internet, ¿un derecho fundamental virtual?», por A. Daniel Oliver Lalana: http://www.unizar.es/derecho/fyd/prodatos/pdf/uned2.pdf.
- «EU Repport» sobre Echelon (en inglés): http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.
- «Carnivore FAQ. Privacidad», por David Casacubierta: http://www.spain.cpsr.org/boletin000c.php.

¿Cómo navegamos realmente por la web?

Cuando hacemos una petición web desde nuestro navegador, es decir, cuando escribimos «http://www.sindominio.net», por ejemplo, en la barra de direcciones del navegador, es necesario hacer unos cuantos pasos previos antes de que se nos muestre por pantalla el contenido de esa página web:

1. Lo primero y más importante es obtener la dirección IP de «www.sindominio.net». Internet funciona con direcciones IP, que son como número de teléfono de muchas cifras (en la versión actual de IP —la 4— tienen el formato A.B.C.D donde A, B, C y D son números del 0 al 255). Para llamar por teléfono a nuestros amigos es muy sencillo: recordamos su número de teléfono, marcamos y listo. Pero cuando queremos llamar a la estación de autobuses o a una tienda normalmente usamos las «Páginas Amarillas». En Internet hacemos lo mismo: si pusiéramos en la barra de direcciones en lugar de «www.sindominio.net», la dirección IP que le corresponde, 213.172.36.134 en este caso, funcionaría perfectamente. Pero claro, acordarnos de unos cuantos números de teléfono es fácil; sin embargo, hacer lo mismo con todas las IPs de todas las páginas que visitamos sería de locos. Por eso mismo, los navegadores utilizan las «Páginas Amarillas» de Internet, los servidores

seguirte citas. Eventualmente podría hacer encuestas, distribuir libros alternativos o ver publicidad para ganar algo de dinero en la red, dinero que ingresaría en tu/su cuenta corriente electrónica. Así contando con pasta, podría enviar regalos a tus conocidos, comprarte los libros que os gustan etc. Idealmente iría aprendiendo tu tono y sus comunicaciones se irían asemejando más y más a las tuyas. Al final, es decir cuando murieras, el agente podría seguir viviendo por ti, participando en listas de correo, en foros, ligando por Internet, ganando dinero y gastándoselo... Nadie notaría que has muerto. Excepto tú mismo, aunque a estas alturas tus opiniones serían irrelevantes, como quizá irrelevante había sido tu vida.

Claro que también podrías construir agentes falsos, agentes que no se parecieran en nada a ti y que se dedicarán a darle información falsa a los agentes de las compañías que venden de todo por

DNS (Domain Name System). Cuando yo le digo «www.sindominio.net» a un servidor DNS, él me responde diciendo «213.172.36.134»; y viceversa, si le digo «213.172.36.134», él me responde «www.sindominio.net» (resolución de nombres inversa). Este primer punto es importante, ya que una navegación anónima no debe dejar rastro ni siquiera en sus peticiones a los servidores DNS.

2. Una vez que tenemos ya la dirección IP a la que hay que conectarse, nuestro navegador intenta abrir el puerto 80, que es el de HTTP. ¿Qué es esto de los puertos? Siguiendo con el símil telefónico, un puerto podría entenderse como una extensión telefónica: tu llamas al teléfono del ayuntamiento (555 341 431), pero no quieres hablar con todo el ayuntamiento, sino únicamente con el departamento de bienestar social (extensión 2349). Con los ordenadores pasa parecido: un servidor tiene la IP 213.172.36.134, pero para ver la página web que alberga sólo nos interesa entrar por el puerto 80, que es el de HTTP (web).
3. Después de conectarse, nuestro navegador le pide al servidor la página que nosotros hemos solicitado. Si, por ejemplo, hemos puesto en la barra de direcciones «www.sindominio.net/ayuda.shtml», el navegador va a «www.sindominio.net», puerto 80, y dice: «GET /ayuda/irc.shtml», y el servidor le envía la página que ha pedido. El servidor tiene que saber quién le ha pedido esa página, es decir, la dirección IP de quien ha pedido esa página para poder enviársela. Normalmente este dato (quién solicitó esa página) se almacena en el propio servidor web, por lo que es posible saber qué ordenadores han visitado determinadas páginas.
4. El navegador recibe lo que le ha enviado el servidor, y nos lo presenta en un formato más agradable, con tablas, negrita, subrayados, etc.

No parece muy complicado, ¿verdad? La navegación web estándar tiene pocos misterios. Algo más compleja es la navegación web segura, a través de HTTPS (HTTP Seguro), que utiliza el puerto 443 y transmite los datos de manera cifrada. Conviene diferenciar la navegación web segura de la navegación web anónima.

Internet, a hacerles enviar ramos de flores a señoras inexistentes y a escribir a los políticos interminables cartas soeces, una detrás de otra, a organizar sentadas electrónicas en las que sólo participaran agentes.
Todo un campo este de los agentes.
Más información en: www.sintron.org

En la navegación web segura, se sabe a qué direcciones vas, pero no qué contenidos intercambias con ese servidor, porque la conversación entre tu navegador y el servidor web está cifrada. En la navegación web anónima, el objetivo es otro: dificultar que el servidor web sepa realmente quién le está visitando, como veremos a continuación.

Navegación anónima

Si queremos navegar sin dejar rastro, no nos basta con utilizar navegación web segura mediante HTTPS siempre que podamos, ya que con eso sólo estaremos cifrando los datos que transmitimos y recibimos, pero no estamos «anonimizando» o «impersonando» (dos palabras inglesas traducidas con calzador) nuestras peticiones a los servidores web. En otras palabras, si yo me conecto a la web de mi caja de ahorros para realizar una transferencia bancaria, casi con total certeza estaré bajo una conexión segura, protegida mediante HTTPS, pero en ningún momento dicha conexión será anónima, porque el servidor web de la caja de ahorros sabrá que hemos sido nosotros quienes nos hemos conectado a hacer esa transferencia.

Por otra parte, si queremos entrar en la página web de Falange Española sin que sepan que hemos sido nosotros, no necesitamos entrar bajo una conexión segura mediante HTTPS, sino que lo que tenemos que conseguir es que parezca que no hemos sido nosotros quienes hemos pedido determinada página web. ¿Cómo conseguimos esto? La respuesta ya la sabemos, de la misma manera que lo hacemos cotidianamente para otras cosas: mandamos a otra persona a que nos haga el recado. En el mundo de los navegadores y las páginas web, los recaderos se llaman «*proxy*» o «*proxy-web*». Un servidor *proxy-web* recibe peticiones o «recados», los realiza y devuelve los resultados a quienes se lo pidieron. Bien, asunto arreglado: en lugar de ir nosotros a visitar la página de la Falange directamente, le pedimos a un proxy-web que la visite por nosotros y nos devuelva la página cuando la tenga.

GOOGLE BOMB

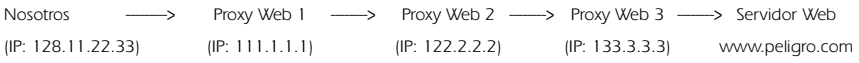
Una *google bomb*, o bomba de Google, es un intento de subir artificialmente la valoración de una web en un buscador como Google. Para ello se aprovecha que el buscador relaciona la cantidad de enlaces con palabras a una web con la importancia de esa web en relación a esas palabras. Al crear muchas webs diferentes con enlaces idénticos a otra, ésta puede subir mucho en los resultados del buscador. Si además estas webs se actualizan muy regularmente (como los weblogs) el efecto es aún mayor.

La primera bomba de este tipo fue lanzada a finales de 1999 cuando se descubrió que si metías en Google: «more evil than satan himself» (más malo que el mismísimo Satanás) ibas a dar a la

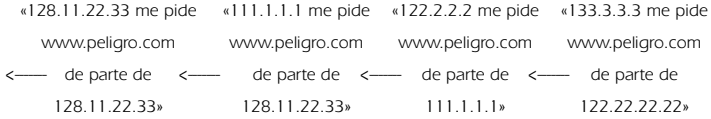
En los registros del servidor web ya no aparecerá nuestra dirección IP como la que ha hecho la petición, sino que será la dirección del *proxy-web* la que se almacenará.

Esto funciona bastante bien, pero a veces los servidores proxy-web son tan gentiles que piden las cosas así: «Por favor, solicito la página documentos/informacion.html, de parte de 128.11.22.33». Imaginemos que nosotros somos ese tal 128.11.22.33, gracias a esa manera de pedir la información, habremos sido delatados claramente. Muchos servidores web están configurados para registrar las direcciones IP que aparecen en «de parte de...» dentro de la petición (técnicamente en la cabecera HTTP_X_FORWARD).

Fue bonito mientras duró... con estos servidores proxy-web tan educaditos no podemos navegar de forma anónima. Bueno, todavía podemos poner las cosas difíciles a quien nos quiera seguir el rastro: encadenamos una serie de servidores *proxy* y así es más difícil seguirnos el rastro. Lo mismo pasa en la vida real: si le dejas un libro a alguien, y ése se lo deja a otra persona, y así unas cuantas veces, da el libro por perdido. Solamente aparecerá nuestra dirección IP en el primer «salto» que demos:



¿Qué dice cada uno?



página de Microsoft. Ya en el año 2000 se usaron bombas de Google similares para llevar desde una búsqueda que solicitara «tontos del culo» (o algo así) a la página electoral de Bush. Así hasta que lleguemos a la web semántica, que dice Carolina que es el futuro; pues ya sabéis, a preparar vuestras propias bombas de Google.

De esta forma, lo que queda registrado en el servidor web es que 133.3.3.3 ha solicitado la web «www.peligro.com» de parte de 122.2.2.2. Ni rastro de la IP origen real, es decir, la nuestra (128.11.22.33). Cuantos más saltos de *proxy-web* demos, más difícil será rastrear nuestra navegación, pero configurar esto puede ser complicado. Para evitarnos muchos quebraderos de cabeza, existen herramientas que hacen esto mismo de forma automática. JAP es una de ellas.

JAP

JAP significa «*Java Anonymous Proxy*», es decir, «Proxy Anónimo en Java». En realidad ese es el nombre original del software de proxy-web, pero actualmente no en todas las plataformas está escrito en Java (Java es un lenguaje multiplataforma que funciona de manera similar tanto en Microsoft Windows, Apple MacOS o GNU/Linux, entre otros). Concretamente las versiones de Windows y MacOS sí están escritas en Java, y tienen una interfaz gráfica muy similar, y la versión para GNU/Linux y BSD funciona de otra manera, en modo texto.

JAP se basa en el principio de que todos sus usuarios navegan con la misma dirección IP. De esta manera, cuando un servidor registre nuestra visita, apuntará esa IP, que es compartida por todos los usuarios de JAP, y no podrá saber cuál de todos los usuarios ha visitado la página.

Cuando instalamos JAP en nuestro ordenador, lo que estamos instalando es un servidor proxy-web. Todas las peticiones que le hagamos a ese servidor proxy irán encaminadas a la red de servidores proxy de JAP de forma cifrada, así que todo lo que pidamos a nuestro «recadero JAP» será tratado de forma *anónima* y *segura*. Recordemos el diagrama anterior:

Nosotros—SIN CIFRAR—>Proxy Web JAP—CIFRADO—>Proxy Web JAP2—CIFRADO—>Servidor Web
<—SIN CIFRAR— <—CIFRADO— <—CIFRADO—

El salto desde nuestro navegador al primer proxy JAP es sin cifrar, pero esto no es ningún problema si lo instamos en nuestro propio ordenador, porque sería como decir al «recadista JAP» dónde queremos ir ***dentro de casa***, donde nadie puede *oírlo*. A partir de ahí, se produce otra serie de saltos entre diversos servidores proxy de JAP, y finalmente se accede al destino. Una vez se obtiene la página, el sistema JAP realiza los saltos inversos y al final obtenemos la página web en nuestro navegador.

La secuencia de saltos que realiza JAP dentro de sus servidores se conoce como «cascada de saltos» o «*mix cascade*». Podemos elegir entre diferentes secuencias de saltos para dificultar más aún el seguimiento. Dado que mientras nosotros navegamos hay también usando este sistema otros muchos usuarios, nuestro tráfico web se mezcla con el del resto de usuarios, haciendo muy costoso el seguimiento del tráfico de una sola persona.

Los servidores proxy-web del sistema JAP son proporcionados por diferentes instituciones independientes, que declaran *oficialmente* que no guardan un registro de las conexiones, ni intercambian información sobre ellas con otros proveedores. A pesar de esta declaración pública, se prevé crear un software que haga de «perro guardián» del sistema, para asegurar que esto se cumple por parte de las citadas instituciones, creando navegaciones de prueba y comprobando si han podido ser objeto de escuchas o registros.

Instalación y uso en Microsoft Windows

Instalar JAP en Windows es muy sencillo, sólo tendremos que seguir los pasos de un asistente de instalación. Lo primero que tenemos que hacer es bajarnos el paquete de instalación de la página http://anon.inf.tu-dresden.de/win/download_en.html. Ahí encontraremos diferentes enlaces en función de la versión de Java que tengamos instalada en el sistema, etc. Lo más sencillo es pinchar en el enlace «*download the complete setup program*» para bajarnos el programa de instalación completo y evitar así mayores complicaciones.

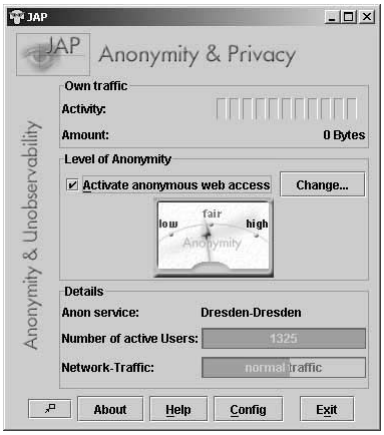
Una vez que tenemos el programa de instalación en nuestro disco duro, lo ejecutamos y nos aparecerá un asistente de instalación en el que deberemos elegir el idioma. Actualmente sólo está disponible en inglés o alemán, así que elegimos inglés y le damos a continuar. Seguidamente se nos muestra un diálogo en donde deberemos especificar la carpeta en la que queremos instalar JAP. En principio la carpeta que viene por defecto es correcta, así que pulsamos el botón de siguiente («Next»). En el siguiente paso, el asistente nos pregunta qué es lo que queremos instalar. Ante la duda, lo más sencillo es pedirle que instale tanto JAP como el soporte para Java («JAP + Java»). Posteriormente, se nos solicita un nombre para la carpeta destinada a JAP dentro del Menú de Inicio. «JAP» es una buena opción. Por último, se nos avisa de que hemos completado todos los pasos para proceder con la instalación de JAP y pulsando en siguiente («*Next*») comenzará a instalarse en nuestro ordenador.

Una vez termina el proceso de instalación de JAP, comienza la instalación del soporte para Java (tal y como habíamos solicitado en el segundo paso de

la instalación). Esta versión de Java es propietaria de Sun Microsystems, así que es necesario aceptar la licencia de uso para poder instalarla. Aceptamos y continuamos. Definimos el lugar en nuestro disco duro en el que queremos instalar Java. El directorio mostrado por defecto es una buena opción, así que pulsamos el botón de siguiente. Seguidamente se nos pregunta si queremos que esta versión de Java que estamos utilizando se utilice también cuando usemos el Internet Explorer o el Netscape Navigator. En principio nos da igual, así que dejaremos las casillas en blanco y pulsaremos el botón siguiente para continuar. Una vez llegados a este punto, se instalan los componentes necesarios para que funcione Java y se da por finalizado el proceso de instalación. El proceso de instalación finaliza aquí, pero conviene tener marcada la opción para configurar automáticamente nuestro navegador para que use JAP antes de pulsar el botón de finalizar.

El asistente para configurar nuestros navegadores intentará buscar todos los navegadores que tengamos instalados en nuestro ordenador de forma automática y cambiará sus configuraciones para que naveguen a través del proxy-web JAP. Además, podrá configurarse JAP para que funcione también con programas de gestión de descargas, como el «*Download Accelerator*» o «*GetRight*», para no delatarnos al usar estos aceleradores de descargas. En la siguiente pantalla el asistente muestra una lista de los navegadores que ha encontrado instalados en nuestro ordenador. Es recomendable seleccionar todos los navegadores que utilicemos de esa lista y que pulsemos el botón de siguiente («*Next*»). Posteriormente, se muestra una lista de todas las conexiones a Internet configuradas en este ordenador, para seleccionar con cuál de ellas queremos utilizar JAP. En principio seleccionaremos todas, salvo que hubiera problemas con alguna (por tener que utilizar otro *proxy-web*, por ejemplo). Y finalmente terminamos el proceso de configuración automática de JAP, por lo que podremos utilizarlo normalmente.

Una vez instalado, JAP situará un icono en el escritorio de Windows. Si hacemos doble clic sobre ese icono, podremos ver la ventana de gestión del proxy-web anónimo:



Hasta que no activemos la opción «*Activate anonymous web access*», no estaremos navegando de forma segura. Después de activar esa opción, podremos modificar la configuración de JAP pulsando sobre el botón «*Change*», que nos mostrará un diálogo en el que podremos cambiar las medidas de seguridad tomadas, etc.

Instalación y uso en GNU/Linux

El proxy-web anónimo JAP tiene una manera diferente de funcionar para sistemas UNIX y similares. No utiliza Java, sino que está escrito en C, y se llama «*anon-proxy*». Existen paquetes para Debian GNU/Linux y RedHat entre otras distribuciones, así como las fuentes para cualquier otro sistema UNIX-like.

El proceso de instalación en Debian GNU/Linux es muy sencillo. Primeramente comprobamos si lo tenemos en las listas de paquetes disponibles:

```
# apt-cache search anon-proxy
anon-proxy - Proxy to surf the web anonymously
```

Si queremos conocer algo más sobre el contenido del paquete, podemos mostrar sus características e información relevante con el comando:

```
# apt-cache show anon-proxy
```

Para instalarlo basta con hacer:

```
# apt-get install anon-proxy
```

Y el sistema de paquetes de Debian GNU/Linux se bajará los paquetes necesarios y procederá a su configuración. Si es la primera vez que instalamos anon-proxy, se nos preguntará en qué puerto queremos que quede el proxy-web a la escucha dentro de nuestro ordenador (por defecto es el 4001). Y finalmente se nos pregunta si queremos iniciar el proxy anónimo nada más arrancar el sistema. Además de esto, se nos informa de que deberemos configurar el proxy en los navegadores que utilicemos de esta manera: 127.0.0.1:4001. Es decir, 127.0.0.1, que es la dirección IP que significa siempre «nuestro propio ordenador», y 4001 que es el puerto que hemos elegido durante la instalación para que el proxy-web escuche. Si queremos utilizar «anon-proxy» para programas que funcionan con la configuración propia del sistema como APT o el navegador Lynx, deberemos exportar la variable de sistema «http_proxy»:

```
# export http_proxy=http://127.0.0.1:4001/
```

Para asegurarnos de que realmente el puerto 4001 de nuestro sistema está abierto para conexiones al proxy anónimo, podemos utilizar el comando «netstat»:

```
# netstat -ptau
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address       Foreign Address State       PID/Program name
tcp        0      0 localhost:4001 *:*                 LISTEN      6114/proxytest
```

Como vemos, el puerto TCP 4001 en *localhost* (es decir, 127.0.0.1, nosotros mismos) está a la escucha (Listen) y el programa que se encarga de atenderlo es «*proxytest*», el nombre del programa ejecutable de anon-proxy.

Otros anonimizadores web

Si no queremos instalar un *proxy-web* en nuestro ordenador o simplemente no podemos (porque estamos en un ordenador en el que no tenemos privilegios como para instalar software, como podría suceder en el trabajo o en un cibercafé), podemos utilizar otros métodos para navegar de forma anónima. Simplemente visitando la página http://www.the-cloak.com/login.html, podremos definir cómo queremos navegar y a qué dirección queremos ir, y el propio «anonimizador» de the-cloak hará la navegación web y nos mostrará el contenido de la página que queramos.

Esto es bastante útil si tenemos problemas de censura como filtros, etc. Un ejemplo claro de todo esto se dio justo después de que se ilegalizará el partido político vasco Batasuna. Nada más ilegalizarlo, todos los proveedores de Internet españoles se vieron en la obligación de prohibir que sus clientes pudieran acceder al contenido de www.batasuna.org. Los proveedores del Grupo Telefónica (Terra, Infonegocio, etc.) modificaron sus servidores DNS (los que hacían de «Páginas Amarillas» de Internet) para que siempre que un cliente pidiera «www.batasuna.org», devolvieran la dirección «1.2.3.4», que no existe en Internet. El resultado era que la página era inaccesible a menos que supieras la dirección IP exacta. Mediante el servicio de the-cloak podríamos poner «www.batasuna.org» y visitar la página a través de su servicio, ya que quien verdaderamente está realizando la visita es the-cloak y no nosotros, aunque podamos ver el contenido de dicha página.

En este sentido, existe bastante desconfianza acerca del gran poder que está adquiriendo el buscador Google, ya que todo lo que aparece en Google existe y lo que no aparece no existe para la gran mayoría de internautas. Por eso mismo se ha abierto una página donde se informa de las razones de esa desconfianza, y entre los servicios que ofrece destaca un *proxy* (un «recadero», recordemos) que nos hace las peticiones de búsqueda por nosotros para que Google no sepa que nosotros estamos buscando algo determinado: http://www.google-watch.org/cgi-bin/proxy.htm. Imaginemos que alguien consigue averiguar que hemos estado navegando por páginas anarquistas antes de que se produzca una manifestación violenta de corte anarquista dentro de nuestra ciudad, un hecho como este podría valer para incriminarnos de manera indirecta. Si hemos hecho uso del *proxy* de google-watch para hacer las búsquedas, Google no podrá saber que hemos sido nosotros

quienes hemos hecho esas búsquedas. Como servicio añadido incluye búsquedas combinadas con otro buscador, All-the-web, para evitar la «google-dependencia».

Consejos prácticos

Al igual que hemos hecho con las contraseñas, estos son unos consejos prácticos que pueden mejorar de forma fácil nuestra privacidad y seguridad mientras navegamos por la red:

- Evitar entrar en páginas que contienen datos privados (aunque estén protegidos con contraseña) en sitios públicos como cibercafés, conexiones en universidades, bibliotecas, etc.
- Usar siempre que podamos HTTP seguro, en lugar de HTTP normal. Esto se diferencia claramente porque en la dirección de la web que accedemos pone https://lo-que-sea/ en lugar de http://lo-que-sea/ (nótese la «s» de «https»). Esto cifrará los datos y las contraseñas que utilicemos y nos permitirá acceder a páginas personales como nuestro correo, en sitios con conexiones inseguras como cibercafés o redes públicas.
- Cerrar *siempre* la sesión en un cibercafé.
- Utilizar siempre que podamos datos falsos a la hora de registrarnos en webs, sistemas sobre Passport.Net, etc.
- Evitar servicios como Hotmail, Yahoo o Gmail, propiedad de empresas multinacionales que anteponen sus intereses a la privacidad de sus usuarios. Si lo que necesitamos es una cuenta de correo gratuita para acceder por web, en http://www.linuxmail.org/ tenemos ese mismo servicio (no es necesario ser usuario de GNU/Linux). Basta con acceder a esa página y pulsar en el enlace «*New member sign up*», y seguir los pasos para obtener una cuenta de correo nuevo (acordaos de «no» utilizar la pregunta típica para recordar contraseñas).
- En cuanto a mensajería instantánea (del estilo de MSN Messenger, ICQ, Yahoo Messenger, etc.), tenemos el cliente GAIM que es capaz de conectarse a redes de mensajería libres como Jabber o propietarias como la del MSN Messenger o ICQ. De esta manera, no nos escudaremos en la típica excusa de que «mis amigos utilizan MSN Messenger así que yo tengo que usarlo», porque podremos ser clientes de una red libre como la de Jabber y a la vez poder ver a clientes de redes propietarias como la del MSN Messenger desde el mismo programa. Para más información sobre GAIM, visita http://gaim.sourceforge.net/about.php. En http://gaim.sourceforge.net/win32/index.php podréis descargaros una versión para Windows; para GNU/Linux o BSD está disponible en todas las distribuciones.

En este capítulo hemos intentado acercarnos al mundo de la seguridad informática desde un punto de vista práctico, pero explicando los conceptos subyacentes a cada nueva técnica. Espero que con su lectura hayamos aprendido un poco más sobre cómo funciona Internet y cómo sobrevivir en ese mar de tiburones. Nos vemos en la Red.

HUMILDAD Y AMBICIÓN DEL VIRUS: UNA INTRODUCCIÓN AL ACTIVISMO VÍRICO

Lluís Guiu

Como sabemos, el Sistema es el mejor amigo de los virus. Merced a su infinita gentileza, los virus pueden disfrutar de sus deportes favoritos. Mutar y infiltrarse, parasitar y propagarse, provocar epidemias y rebrotar. En el caso de los virus genéticos de ARN o ADN, nuestro sistema inmunitario es un buen ejemplo de lo que para ellos es el Sistema.

Por su parte, las bacterias crearon la primera red de redes de alcance planetario como mínimo hace 3.500 millones de años, forjando una red de código abierto[1]. Actualmente siguen existiendo y resistiendo esos venenos llamados antibióticos con respetable grado de impunidad. Si la vida humana se esforzase suficientemente por desaparecer del planeta, podemos otorgarle un voto de confianza y pensar que lo conseguiría, pero lo tendría mucho más difícil para hacer lo mismo con las redes bacterianas.

Sin duda, el microcosmos es un manual de instrucciones que, convenientemente descomprimido, nos proporciona una fuente inagotable de ideas para resistir a cualquier tipo de sistema abierto y descentralizado. Como ejemplo, el Sistema en mayúsculas, es decir, el capitalismo, es un sistema de este tipo, puesto que se comporta de manera análoga a un sistema inmunitario en el terreno de los memes. ¿Cómo podemos resistir a esta tipología de sistemas? Nos gustaría con lo que sigue ayudar a transferir un poco de tecnología del mundo micro al mundo macro, situándonos —metafóricamente— bajo la piel de un virus y observando el mundo desde esta perspectiva.

Empezaremos con la humildad del virus, comprendiendo su humildad.

1. Guiu, L. (2002) «Código abierto y bacterias»: http://astramat.com/c/bacterias.html.

VIRUS INFORMÁTICOS

Un virus informático es un programa que es capaz de «infectar» otros programas para que incluyan una copia de sí mismo. Así pues, es un programa como cualquier otro, con la peculiaridad de que consigue reproducir su código cuando se ejecuta un programa infectado. Este comportamiento nos recuerda a los virus biológicos, que piratean las células para obligar a su maquinaria genética a fabricar copias del propio virus. Sin duda, existen numerosas analogías entre virus biológicos y informáticos que nos ayudan a entender el funcionamiento de estas criaturas del universo digital.

Su origen se remonta a 1959, en los laboratorios de la BELL Computer, subsidiaria de AT&T, en Nueva Jersey, donde se inventó un juego que se denominó Core Wars, inspirado en las teorías sobre

Difícil sería encontrar organismo[2] más salvaje que un virus. No hay atisbo de moral en sus acciones. Pero fijaos en el siguiente detalle: un virus no va por el mundo gritando: «hola gobierno, soy un virus y te vengo a joder». No. Intenta de todas las formas posibles no ser identificado como un enemigo por el Sistema. Procura camuflarse, pasar desapercibido, dificultar su identificación.

Ya un viejo virus MS-Dos como «Natas de Satán», propagado el orwelliano año de 1984, presentaba todo tipo de técnicas de ocultación:

- Encriptación. Los virus como Natas utilizan métodos de criptografía para evitar ser descubiertos.
- Polimorfismo. Un virus polimórfico muta parte de su código, de forma que es diferente en cada infección. Concretamente, el Natas modifica su rutina de desencriptación para evitar ser detectado.
- Código hostil *anti-debugging*. El virus intenta que no puedas inspeccionar su código. Si intentabas hacer una ejecución paso a paso de Natas, el virus te colgaba la máquina o te finalizaba la ejecución del programa infectado.
- Mecanismos de *stealth*. A través del stealth, procura ocultar los síntomas de infección y hacer ver que todo es normal. Por ejemplo, si se hace un listado de los archivos contaminados por el Natas, éstos muestran el tamaño y fecha original antes de ser infectados.

El metamorfismo —un paso más allá del polimorfismo, ya que todo el código del virus muta— cobra elegante forma en criaturas como Zmist, obra del programador ruso Zombie. Pero no nos engañemos, en cuanto a mutación se refiere, los expertos son los virus genéticos de ARN. Ahí está nuestro amigo el virus de la gripe. Estos virus tienen un índices de mutación altísimos, que superan en varios órdenes de magnitud los índices de mutación de un organismo pluricelular. Objetivo, no ser iden-

2. El pensamiento vírico se entiende mejor desde una perspectiva neodarwinista, donde un virus basado en un código genético puede considerarse como un organismo.

programas con capacidad de autorreplicación de Von Neuman, el que fuera el padre de la arquitectura de los ordenadores tal y como los conocemos. El fundamento de este juego consistía en que dos programadores desarrollaban dos programas, que compartían un espacio de memoria común, de modo que los programas pudiesen reproducirse dentro de este ecosistema digital e ir «conquistando» zonas de memoria. Ganaba el programador del virus que hubiese consumido más espacio de memoria o hubiese conseguido aniquilar al contrario.

tificados por nuestros sistemas inmunitarios. Están continuamente mutando su personalidad, algunos virus de ARN son auténticos profesionales de la personalidad múltiple en clave genética. Parece ser que mutan hasta el límite de ser devorados por sus propias mutaciones, el llamado «colapso catastrófico». Y lo más interesante, algunos virus ARN forman una especie de enjambres llamados «cuasiespecies», donde el virus muta hacia sí mismo[3]. Extraño concepto este que voy a explicar. Los virus mutan tan rápido como pueden para que el virus se quede en el mismo sitio y conserve su identidad. El virus muta tan rápido como puede para seguir siendo él mismo, para reencontrarse a sí mismo.

No se escapa que los virus, sean informáticos o genéticos, van siempre con la cara tapada. ¿Serán los virus unos cobardes? No. Los virus no son cobardes, son humildes. Se lanzan en un ataque aparentemente suicida al interior de su enemigo, a la cocina de su enemigo. Es evidente que para hacer esto hay que ser muy valiente.

Pero un virus no vive sólo de humildad. También tiene ambición. Y no es poca. La ambición del virus es convertir al enemigo en sí mismo, en él mismo, replicándose infinitamente. La inmortalidad a través de la parasitación de sus huéspedes. Alguien podría pensar que la ambición del virus es destruir el Sistema, pero ésa es una falsa ambición de los virus. Como bien dice Richard Dawkins, los *payloads* destructivos de los virus informáticos son artificiosos. Si pretenden inspirarse en los virus genéticos de ADN o ARN, se trata de una incorrecta interpretación de este tipo de virus, puesto que un virus auténtico nunca haría eso. Si somos capaces de situarnos bajo su piel, nos daremos cuenta de que los daños que infringen los virus genéticos no son intencionados. Son un producto secundario de la replicación del virus, ya que éste no tiene en principio ningún interés en matar al organismo que le da cobijo.

3. Domingo, E. (1994) *Virus en evolución*. Ed. Univ. Complutense de Madrid, Madrid.

TomaTAZo

Cuando se estaba redactando la Ley de Servicios de la Sociedad de la Información, más conocida como LSSI, enseguida se vio que iba a suponer un recorte en las libertades de los usuarios de Internet, donde la privacidad no iba a tener hueco, puesto que se iba a obligar a los ISP a guardar todas las páginas a las que accedan sus usuarios, a quién mandamos correos, todo para ponerlo a disposición de las autoridades en caso de ser necesario, por vaya usted a saber qué razón; es decir, que el espionaje empezaba a ser un formato autorizado de comportamiento en Internet. En medio de toda la polémica de las movilizaciones contra la LSSI, siendo conscientes de que los gobernantes atacaban de una manera escandalosa las bases de Internet en la nueva sociedad de la información,

El Sistema no es sólo un enemigo, es el mejor amigo. Parasitamos su infraestructura y su producción de energía. Ésta es sin duda la clave para entender cualquier aspecto del pensamiento vírico, a saber, situarse en su perspectiva interior: no observamos a los virus, somos virus.

El sustrato teórico del pensamiento vírico sirve de bien poco si no toma cuerpo en forma de consejos prácticos y, a ser posible, de ingeniería activista, modelos de acción reproducibles. A continuación detallamos muy sintéticamente la ficha técnica de un par de juegos que desarrollamos contra la famosa «ley de Internet», la LSSI[4]. Estas acciones fueron realizadas a modo de experimento de ciertas técnicas de activismo vírico.

Pensar como un virus: análisis práctico de acciones activistas

El sustrato teórico del pensamiento vírico sirve de bien poco si no toma cuerpo en forma de consejos prácticos y, a ser posible, de técnica activista, modelos de acción reproducibles.

A continuación realizamos un análisis detallado de dos acciones activistas realizadas en la red con el propósito de concretar a nivel práctico como se pueden llevar a cabo acciones de activismo vírico y no quedarnos con la sensación de haber soltado la típica performance posmoderna que quiere bailar con las neuronas de nuestro cerebro para ver si somos capaces de pensar de forma más original de lo que acostumbramos. Estas acciones activistas tuvieron lugar el año 2002 en el marco de la aprobación de la polémica «ley de Internet», que levantó una firme protesta a lo largo y ancho de la red activista del estado español.

4. Ley de Servicios y Sociedad de la Información.

los internautas recurrieron a varios medios de protesta; uno de ellos fue el «el tomatazo contra la LSSI», realizado y distribuido por CPSR-ES (Computer Professionals for Social Responsability, una de las organizaciones más veteranas, cuya idea principal es que Internet ha de ser de todos y para todos), y otro será el script contra la retención de datos.

El tomaTAZo es un juego bajo licencia libre GPL que puede encontrarse en: http://www.spain.cpsr.org/tomatazo/, y una protesta lúdica: consistía en lanzar tomates al entonces ministro de Ciencia y Tecnología, Josep Piqué, y al anterior presidente del Gobierno español, José María Aznar. Pero la protesta no se quedó sólo en el alivio espiritual de «entomatar» a los políticos: cada 3-5 aciertos, aleatoriamente, el juego enviaba una petición web a la dirección http://www.mcyt.es/no-a-la-LSSI. Ésta página no existe, porque la intención no era bombardear el

Dónde está la autoridad competente

Vamos a empezar con la primera acción, la realización y difusión por la red de un juego flash llamado «¿Dónde está la autoridad competente?». Nos vamos a situar mentalmente en el mes de febrero de 2002. Era la tarde del 8 de febrero. Sabíamos muy poco de la LSSI, y esa tarde nos leímos el borrador definitivo que había aprobado ese mismo día el consejo de ministros. ¿Qué era, pues, la LSSI, de la que en la red todo el mundo hablaba? Se trataba de una ley que emanaba de una directiva de la comunidad europea y, según esta directiva, su función debía ser exclusivamente ocuparse de la regulación del comercio electrónico por Internet. Pero el gobierno del Partido Popular, en aquellos tiempos en el poder, no hizo bien los deberes que se le encomendaron desde Europa y presentó una propuesta de ley que por su manifiesta ambigüedad pretendía —con alevosía y nocturnidad— regular cualquier web, fuera o no comercial, coaccionar la libertad de expresión, preparándose un instrumento de censura para poder domar el incipiente poder de la red que empezaba a asomar su hocico. El problema estaba en que era difícil actuar con nocturnidad porque, en la red, toda cuestión relevante para el crecimiento del propio tejido social de la red queda a la luz del día en muy poco tiempo. El gobierno con su conocida testarudez siguió adelante con la aprobación de ley, pero la presión activista fue tan palpable, que hizo imposible el uso práctico de la ley como instrumento coercitivo. Dos años más tarde, en los días posteriores a los atentados del 11 de marzo de 2003, la inteligencia colectiva de la red demostró al gobierno que definitivamente no se la podía domar. Como sabemos, las redes de comunicación fueron el factor clave en la caída del gobierno del Partido Popular[5].

8 de febrero de 2002. Nos hemos leído el borrador de la ley y ahora nos preguntamos qué hacemos. ¿Cómo conseguimos llegar a los grandes medios

5. *Pásalo* es un buen libro para conocer de primera mano lo que realmente pasó (Traficantes de Sueños, Madrid, 2004; http://www.nodo50.org/ts/editorial/pasalo.htm). Para una aproximación genérica y análisis de este fenómeno, ver Howard Rheingold: *Multitudes inteligentes* (Gedisa, 2004).

servidor del Ministerio de Ciencia y Tecnología, sino que quedase constancia en sus registros de que mucha gente había intentado acceder a este sitio.

Así, lo que se veía desde el Ministerio era:

80.58.13.23 - - [23/Feb/2003:19:39:28 +0100] «GET /no-a-la-LSSI_183 HTTP/1.1» 404 1009 «-» «Shockwave Flash»
80.58.13.23 - - [23/Feb/2003:19:39:33 +0100] «GET /no-a-la-LSSI_85 HTTP/1.1» 404 1009 «-» «Shockwave Flash»
80.58.13.23 - - [23/Feb/2003:19:39:38 +0100] «GET /no-a-la-LSSI_227...

Éste no es el primer juego creado por la comunidad internauta para protestar contra la LSSI. Un juego parecido, obra de Pere Rocallaura, reproducía a un trilero, bajo la pregunta «Dónde está la autoridad competente». También en protesta contra la ley, CPSR-ES participó en la campaña del *Manifiesto del 12 de Octubre*, consistente en cerrar indefinidamente la web los días 12 de cada mes, de comunicación para que el máximo número de gente posible conozca los peligros que conlleva esta ley? Era la ocasión perfecta para experimentar algunas técnicas de activismo vírico y comprobar su efectividad a nivel práctico, aportando nuestro grano de arena a la batalla activista contra la LSSI.

Empezamos a pensar como un virus

Observamos a la LSSI como una máquina a hackear. ¿Cuáles eran sus puntos débiles por donde podíamos atacar? El punto débil más evidente era quién tenía potestad para aplicar la ley. Los expertos en derecho constitucional nos decían que sólo un juez tenía potestad, nunca un funcionario del gobierno[6]. En cambio, el texto de la ley se refería una y otra vez a que quien tenía potestad era la «autoridad competente», pero no dejaba nada claro quién era esa autoridad. ¿Cuál era el objetivo de la ambigüedad del concepto de «autoridad competente»? Dejar la puerta abierta para que quien aplicara la ley no fuera un juez. Y si la ley decía, por mostrar un ejemplo edificante, que te podía caer una multa de 600.000 euros simplemente por «atentar contra la dignidad de una persona» o «alterar el orden público», creo que ya está todo dicho. Pero al igual que el gobierno se abría una puerta trasera para burlar la división de poderes, también nos dejaba a la vista una debilidad vulnerable. Íbamos a atacar con fuerza a la idea, al meme de «autoridad competente»[7]. Pero, eso sí, siendo muy buenos chicos y chicas, porque los virus nos enseñan que hay que ser muy suave para dar con fuerza.

Íbamos a hacer una acción de apariencia inocente, un juego simple en flash para ser jugable fácilmente por todo el mundo via web, un pasatiempos para

6. Véase al respecto el informe sobre la inconstitucionalidad de la LSSI de Guillermo Escobar Roca. Para una introducción al contexto temporal de la ley en el año 2002, se puede consultar la siguiente selección de artículos disponible en el propio juego: http://www.manje.net/juegolssi/s/articles.html
7. La memética es la mejor aproximación a la transmisión cultural de la que disponemos actualmente y resulta indispensable para el pensamiento virus. Una perspectiva interesante al respecto es la de Robert Aunger: *El meme eléctrico* (Editorial Paidós, Barcelona, 2004).

fecha en que la LSSI entró en vigor. Puesto que no se ha presentado recurso de inconstitucionalidad (nuestros representantes parlamentarios se decidieron y el Defensor de Pueblo se opuso) se propuso combatir la retención de datos de una manera imaginativa. La retención de datos dejaría de tener sentido si todo el mundo visitara todas las páginas de Internet. Esto, claro está, es imposible; sin embargo, se puede hacer a pequeña escala: si todos los internautas visitan miles de páginas que no interesan en absoluto, mezcladas con las que sí que interesan, los datos retenidos perderán gran parte de su valor. Resultaría muy pesado, sin embargo, dedicar tiempo a visitar páginas que no nos interesan un ápice; por este motivo crearon el script «contra la retención de datos», donde el programa toma las direcciones de un fichero de texto y las visita por el usuario.

Para más información podéis dirigiros a: http://www.puntnet.org/script.html.

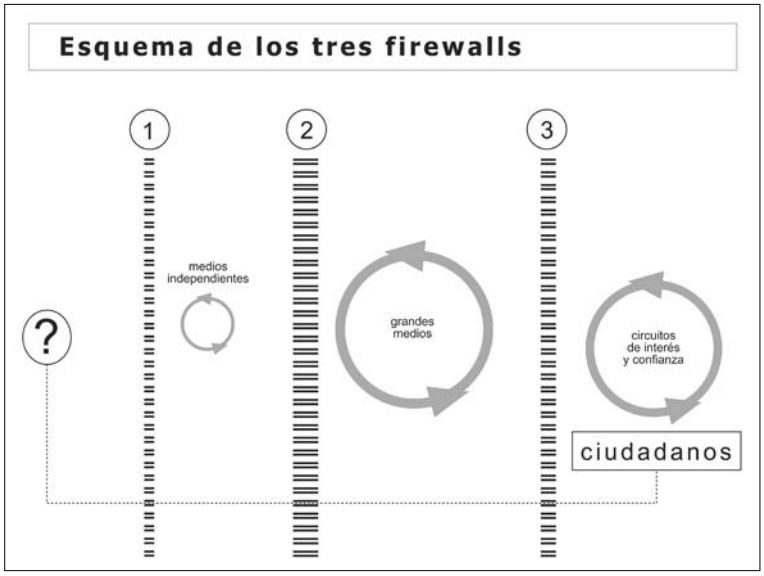
el internauta ávido de nuevas golosinas digitales. Y ese juego sería nuestro caballo de troya que en su interior contenía nuestro duro ataque a la ley. Y eso es lo que hicimos.

El esquema de los tres *firewalls*

Vamos a analizar con más detalle el porqué de realizar un juego y su relación con el pensamiento vírico. ¿Cómo idear una acción activista que se replique en los medios y llegue hasta los ciudadanos? ¿Qué obstáculos nos vamos a encontrar?

Los medios de comunicación están protegidos por *firewalls mentales* de defensa que seleccionan, filtran, censuran la información a partir de la cual se generan los contenidos que se van a publicar. Al igual que un servidor está protegido por un firewall, software de seguridad que regula el tráfico de datos que entra y sale de la máquina evitando intrusiones, podemos imaginarnos que las mentes de los periodistas están protegidas por una especie de firewall mental, y la política de seguridad viene inculcada por la línea editorial y los intereses corporativos del medio de comunicación para el cual trabajan.

Exploremos esta analogía. El firewall de un servidor puede permitir que los ordenadores de su red interna accedan a él porque son de confianza y en cambio vetar sistemáticamente aquellas peticiones de ordenadores externos a su red, a no ser que estén en la lista de fuentes confiables. Ante una cuestión polémica como la LSSI, el firewall mental del periodista confiará fácilmente en la información de las agencias de noticias porque son una fuente confiable y rechazará, por ejemplo, una información de un activista o de apariencia subversiva porque por definición la consideran una fuente no confiable. De esta forma, los grandes medios se aseguran que sus periodistas no sean un vector de contagio de noticias subversivas que para nada convienen a esos intereses corporativos. Cada medio de comunicación dispone de un tipo diferente de política de seguridad para los firewalls mentales de sus productores de noticias. En la hipótesis con la que trabajamos es lo que denominamos el «esquema de los tres firewalls» (figura 1).



Este esquema sigue un trazado lineal muy simple donde nosotros somos el interrogante de la izquierda y queremos llegar hasta la derecha (el ciudadano). Un esquema realista de los medios es mucho más complejo y contempla por ejemplo una serie de retroalimentaciones con la red de weblogs y medios digitales que nos sugieren más un mapa en red. El objetivo de este esquema simplificado es centrarse en el entendimiento de cómo superar los firewalls mentales. En la acción activista que planteamos, la red de firewalls etiquetada como número 1 en el gráfico corresponde a los medios independientes, como ejemplo tenemos barrapunto.com, la publicación Makypress, kriptopolis.org y IBLnews.com. Éste es un nivel usualmente fácil de atravesar, ya que —al menos en el caso que nos ocupa— la red activista estará a nuestro favor. Una vez superada esta barrera, entramos en el circuito de difusión y replicación de memes de estos medios.

La segunda red de firewalls, la de los grandes medios, es nuestro objetivo. Si conseguimos atravesarla con suficiente nivel de inoculación, entraremos en el gran circuito de replicación, propagación y difusión radial de ideas de los grandes medios.

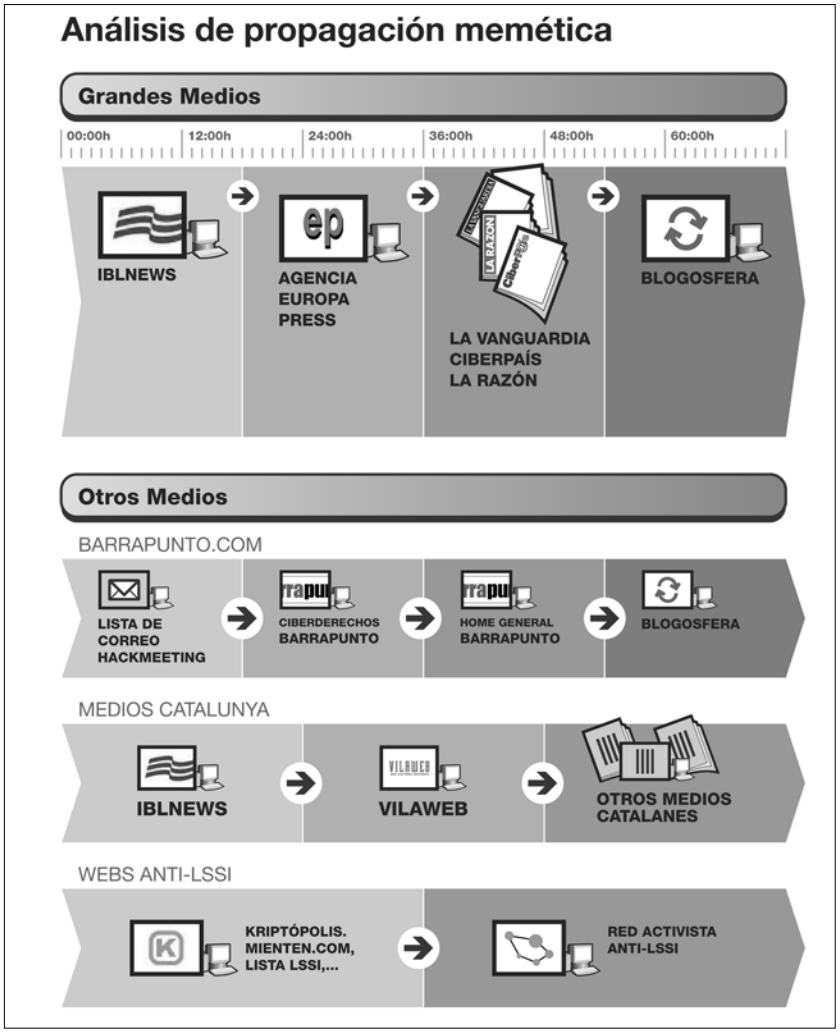
No nos debemos olvidar que existe una tercera y última red de firewalls que son las mentes de los ciudadanos, los firewalls que protegen nuestras intranets mentales[8]. A partir de este tercer nivel, la difusión de las ideas sigue a través de los circuitos de interés y confianza de las personas infectadas que transmiten el mensaje.

8. Si esta forma de decir las cosas le suena un poco maquiavélica, lo es, ciertamente. No podemos esperar un pensamiento moral del virus, simplemente porque no lo tiene. En su estado puro, no hay atisbo de moral en sus acciones. Por eso debemos delimitar el alcance de nuestro pensamiento vírico para mantener una coherencia con nuestra ética personal.

Teniendo claro este esquema, y a la luz del pensamiento virus, se nos revelan dos cuestiones clave. La primera es que tenemos que fabricar un caballo de Troya de forma que nuestra acción no sea detectada como una acción hostil, y esconder nuestras ansias radicales en el interior del caballito. *Et voilà*, por eso decidimos desarrollar un juego, es decir una acción agradable estéticamente, de apariencia inofensiva («es sólo un juego») y a la vez irónica (el humor es buena forma de saltar las protecciones de los firewalls mentales). La segunda cuestión es que debemos convertirnos en la medida que sea posible en una fuente más confiable. Esto se puede resolver observando una de las consecuencias de lo que el pionero del weblogging periodístico Dann Gillmor denomina «periodismo participativo»[9]. Fruto de este fenómeno, los periodistas de los grandes medios cada vez más se alimentan de información que obtienen de los medios independientes de la red, especialmente si se trata de noticias relacionadas con el mundo digital, como es el caso de todo aquello que concierne a la LSSI. Una hipótesis interesante que formulamos es que cuando el periodista recibe una noticia mediante un comunicado de prensa por parte de alguien desconocido no le otorga el mismo grado de confiabilidad que cuando esta misma noticia la lee en uno de los medios independientes de los cuales se alimenta y decide seleccionarla como fuente para la elaboración de una posible noticia. En el caso de ejercer una selección consciente sobre un medio que visita frecuentemente, el periodista tendrá tendencia a otorgarle un estatus superior de confiabilidad. Eso nos lleva a que si conseguimos un buen grado de difusión en los medios independientes, estos pueden ser nuestros avalistas en estatus de confiabilidad para llegar hasta los grandes medios. Ejercemos una parasitación benigna de nuestros medios afines para conseguir que nuestras ideas lleguen hasta el otro lado de la red de firewalls número 2. Sobre esta premisa, enviamos un comunicado informal a estos medios, esperando confirmar esta hipótesis. El nombre de quien lo enviaba también era un detalle importante. Como un experimento más en nuestra investigación, elegimos el nombre de Pere Rocallaura, un ciudadano cualquiera indignado ante la LSSI, mutando nuestra verdadera personalidad, tal y como lo haría un virus. Lo redactamos de forma muy pedagógica pensando en facilitar la replicación.

Bien, ahora veamos como estos supuestos teóricos se desenvolvieron a nivel práctico. A continuación, en la figura 2, podemos ver un análisis de propagación memética en los medios de nuestro mensaje anunciando el juego. En 72 horas este mensaje sufrió una propagación epidémica. El análisis está inspirado justamente en los análisis de control de epidemias, se trata de seguir la pista de quién contagió a quién a través de una línea de tiempo, teniendo en cuenta los periodos de incubación y los factores causales, con la ventaja de que en nuestro caso ya sabemos quién provocó los primeros contagios. Deducimos por las fechas de publicación y el redactado de las noticias, que IBLNews, un medio digital independiente, fue el vector de propagación a los grandes medios.

9. Bowman, Shayne y Willis, Chris: «Nosotros, el medio», http://www.hypergene.net/wemedia/espanol.php.



Como vemos, por su carácter de expansión epidémica, nuestro mensaje puede propagarse muy rápido, por lo que prácticamente no habrá tiempo para rectificar si nos equivocamos. Hay que planificar todos los detalles antes de realizar la acción. Es posible que no tengamos segundas oportunidades. Distribuimos el juego en diferentes mirrors para distribuir la carga de los servidores teniendo en cuenta que alguno de ellos podía dejar de funcionar por razones diversas.

Finalmente, quisimos comprobar si era factible realizar una acción de esta tipología evitando medianamente la identificación. La distribución de mirrors evitó una identificación directa y el uso de anonimizadores dejó bastante a salvo la IP real.

FICHA: «¿DÓNDE ESTÁ LA AUTORIDAD COMPETENTE?»

- URL: http://www.manje.net/juegolssi/s
- Tipología de acción: activismo vírico, juego en flash vía web.
- Objetivo básico: contribuir a crear un clima de opinión en contra de la LSSI, llegando a los grandes medios.
- Programación: Actionscript y html. Remodelación y mejora de flash existente bajo licencia GPL.
- Equipo de desarrollo: Lluís Guiu, Arbeka y kl2.
- Tiempo: dos semanas.
- Tamaño del juego: primera carga de 52 KB y segunda de 112 KB.
- Técnicas de camuflaje: utilización de juego como caballo de troya memético, lenguaje humorístico, anonimización de ip's, mutación de personalidad con la creación de «Pere Rocallaura», distribución del juego mediante mirrors (esto permitió también la distribución de carga).
- Estrategia de propagación memética: escalada bottom-up siguiendo esquema de los tres firewalls[1].
- Medios infectados: medios independientes y movida anti-LSSI, edición digital de grandes medios, Europapress, edición en papel de *Ciberpaís*.
- Velocidad de propagación: muy rápida, propia del activismo vírico.

FICHA: «COLABOREMOS CON LA LSSI»

- URL: http://www.manje.net/juegolssi2.
- Tipología de acción: activismo mixto vírico/bacteriano, juego participativo vía web.
- Objetivo básico: visualizar los peligros de la LSSI a través de la participación directa de los internautas.
- Programación: html y javascript, y uso de cgis externos de hosting gratuito.
- Equipo de desarrollo: Lluís Guiu, Arbeka, kl2 y Mercè Molist.
- Tiempo: un mes.
- Técnicas de camuflaje: lenguaje irónico y naificación, dejando que sean los internautas quienes aporten la subversión, uso de personalidad «Pere Rocallaura», distribución de la web mediante mirrors.
- Estrategia de propagación memética: escalada bottom-up.
- Medios infectados: respecto al primer juego, mayor penetración en medios independientes y escasa incidencia en grandes medios. Por otra parte, destacable la mención de «Colaboremos con la LSSI» en la sesión del Senado español de 20-6-2002 donde se debatió la ley, en la que un senador invitó a la ministra del Ministerio de Comunicación y Transportes a participar en el juego.
- Medición de participación: un total de 230 contribuciones en primera fase.

Colaboremos con la LSSI

Respecto a la segunda acción activista la vamos a detallar muy brevemente. Se trata de «Colaboremos con la LSSI», una acción web a caballo del activismo vírico y el activismo participativo. Como sucintamente nos explica Xabier Barandiaran[10]:

> *En esta página (diseñada bajo otro nombre múltiple: Pere Rocallaura) el usuario se encuentra con un formulario en el que puede elegir la categoría de denuncia dentro de las posibles en la LSSI, introducir la página que quiere denunciar, el porqué, etc., y al final un botón de envío de la denuncia al ministerio de ciencia y tecnología. La ambigüedad de la LSSI, que en principio es aplicable a un entorno indefinido de servidores, esconde una instrumentalización flexible de la ley como herramienta para la represión selectiva (con multas que van desde los 60.000 a los 600.000 euros). El objetivo de esta acción no es la denuncia de las diversas páginas web de los poderes establecidos (algo condenado al fracaso de antemano), sino el cuestionamiento (mediante esa denuncia) de la ambigüedad y los peligros de arbitrariedad de esa ley. Además la creación de esta web de denuncias propone un nuevo experimento de modelo de acción polítca ya que los activistas no son los que realizan la acción sino que se limitan a poner a disposición del público una tecnología de denuncias sistemáticas, con lo que introducen al espectador de la política del espectáculo como actor político.*

En cuanto a los aspectos de activismo vírico, fijémonos por un momento en el título de la acción «Colaboremos con la LSSI». Se trata de la comprensión de que la LSSI no es nuestra enemiga, sino todo lo contrario. Se trata de hacer judo con la ley, estamos a favor de la ley. Porque recordemos, el Sistema no es sólo un enemigo, es el mejor amigo.

En cuanto al análisis de la propagación memética, se consiguió mayor inoculación en medios independientes pero escasa incidencia en grandes medios. La acción activista, aún siendo vírica sólo parcialmente y concentrándose más en los aspectos participativos, esperábamos que podía conseguir una cierta penetración en los grandes medios. Por otra parte, nos sorprendió gratamente la mención de «Colaboremos con la LSSI» en la sesión del senado español de 20-6-2002 donde se debatió la ley, en la que un senador invitó a la ministra del Ministerio de Ciencia y Tecnología a participar en el juego. Asegurar el objetivo de llegar a los medios puede implicar la realización de múltiples acciones, esperando que al menos una de ellas consiga superar la red de firewalls número 2.

10. Barandiaran, Xabier (2003) «Activismo digital y telemático: Poder y contrapoder en el ciberespacio», v.1.1., http://www.sindominio.net/~xabier/textos/adt/adt.html.

MÓVILES: ¿UN NUEVO CAMPO DE INFECCIONES?

ENTREVISTA REALIZADA POR TXIPI A VALLEZ ZELLAV

¿Podrías definirte en cuatro líneas?

Decir algo de uno mismo es lo más complicado. Tengo 24 años, estudié telemática y ahora, mientras trabajo, informática, con calma. Trabajo con ordenadores. Diría que soy una persona sociable y amistosa y luego, aparte, pues con inquietudes y con ganas de aprender y experimentar cosas nuevas.

¿Desde cuando estás interesado en el mundo de los virus y los gusanos de Internet?

Hace ya varios años. No sé si hará unos 3 o 4 años ya, más o menos.

¿Por qué ese interés?

Es un mundo apasionante. Al principio me llamaba muchísimo la atención (ahora también, pero al principio siempre está ahí esa magia y esa atracción de lo que desconoces completamente). Tener la capacidad de crear algo con tu ordenador que de alguna manera «cobra vida» y es capaz de expandirse y de viajar por todo el mundo (aunque en realidad yo nunca he llegado a poner ningún virus *in the wild*). Hasta podría decir que llegas a coger cariño a ese bichejo que estás creando, y quieres meterle más y más características.

Y lo bueno que tiene es que esto es algo con lo que a la vez estás aprendiendo un montón de cosas. Y luego una vez que ya estás en la *scene* surge un poco el querer hacer algo que sorprenda a los demás, y luego el tema de poder publicar tus trabajos. Es otro aliciente.

¿Qué es lo que más te gusta de la escena vírica?

Lo que más me gusta es conocer gente que comparte una afición a veces tan atípica como ésta y con la que puedes comentar tus nuevos trabajos e ideas, y ellos te comentan. Al final una *scene* nace por eso, gente que comparte una afición y que necesita conocer a otras personas con las que compartirla.

¿Y lo que menos?

Que cada vez hay menos gente. Algunos dicen que ya no es lo que era, que ahora la gente se dedica a hacer *massmailers* que no aportan técnicas nuevas ni nada «gracioso». Yo respeto cualquier trabajo que haya necesitado un esfuerzo, incluso un *massmailer* de lo más normalito. Aunque sí que pienso que cada vez hay menos cosas novedosas. Es lo que en su día se definió como «la buena y la mala *scene*». De la «buena *scene*» cada vez hay menos, pero siguen apareciendo nuevos «fichajes» con muchas ganas de aprender y que realmente se esfuerza en hacer cosas interesantes. En cualquier caso no soy yo el

más apropiado para hablar de la *scene*, pues tampoco llevo mucho tiempo en ella, aunque hablo a menudo con gente de hace años, la *old school* que la llaman.

¿Cómo surgió la idea de desarrollar el primer gusano para móviles?
Es lo que decía: el interés por algo distinto, una nueva plataforma con todo lo que eso conlleva. Y las ganas de aprender también, sobre esta nueva plataforma. Y también un poco pues querer ser el primero en el mundo en algo, no voy a negar que eso también me movió a interesarme por ello.

¿Qué dificultades encontraste durante su desarrollo?
Pues la verdad es que encontré muchos. Lo primero pues que es un sistema operativo que, aunque internamente guarda muchas similitudes con windows o linux (el modelo de memoria, procesos, hilos, seguridad, tiene su modo usuario y su modo kernel... se parece bastante), pero el api que te dan es bastante diferente. Cada sistema operativo más o menos sigue una política para la api que te ofrece. La api que te da symbian, además de seguir un diseño muy diferente, tiene algunos detalles que se tarda en cogerles el truco.

¿Cuál ha sido la principal motivación para desarrollar el gusano? ¿Alguna motivación política, económica, de lucha antisistema, etc.?
Pues en parte demostrar que todo es vulnerable. Últimamente parece que se está poniendo de moda la frase de «hemos aprendido de los errores que han cometido otros sistemas en el pasado y los hemos corregido y hemos hecho algo mucho más seguro». Es lógico que se aprenda del pasado, pero no se puede asegurar que un sistema es completamente seguro. En parte porque estás ofreciendo cosas nuevas, nuevos servicios, nuevas tecnologías, en las que eres pionero. Y también porque quien hace la ley hace la trampa, sencillamente.

Además tienes que ofrecer un servicio y unas ventajas, y si quieres ofrecer algo bueno «te la tienes que jugar»: por ejemplo, con el bluetooth, lo primero que intenté es enviar directamente un .app (un ejecutable) de un dispositivo al otro; y en el receptor enseguida saltó un mensaje diciendo que no se podía abrir el adjunto recibido por ser peligroso. Pero sí que permite recibir y abrir archivos .sis (instaladores). Y abrir un .sis es tan peligroso como cualquier ejecutable, desde el punto que puedes crear un .sis que automáticamente lance un ejecutable que contenga durante la instalación. Entonces, ¿deberían haber quitado también la posibilidad de intercambiar .sis vía bluetooth (o MMS)? No, ya que es algo útil e interesante, por ejemplo poder intercambiar juegos y aplicaciones con amigos. Es una ventaja que también conlleva un riesgo.

Entonces motivación política, económica, etc., quizás también fue una motivación. Sin embargo también me gustaría decir que si alguien ha salido beneficiado han sido las empresas antivirus. A ellas les interesaba más que a nadie provocar el «revuelo» y el «pánico» alrededor de los virus para móviles.

¿Cómo valorarías el impacto que tuvo la aparición del Caribe («Cabir», según algunos antivirus), tu gusano para móviles?

Es un poco lo que decía antes, creo que le han dado mucho bombo, especialmente las empresas antivirus, porque les interesa mucho tocar este nuevo mercado que está creciendo muchísimo. Y luego pues que me imagino que la gente se sorprende con que su móvil pueda ser infectado. Mucha gente no tiene ordenador, pero casi todo el mundo hoy en día tiene móvil (aunque pocos tienen un móvil infectable). Y mucha gente que desconoce completamente el mundo de la informática, que oyen que su teléfono puede ser infectado y empiezan a pensar todo tipo de cosas.

¿Consideras que puede servir como forma de «cortocircuitar» sistemas, atacar, o para el hacktivismo? Alguien sugirió que podrían servir para perjudicar a los grandes productores de software comercial como Microsoft, ¿estás de acuerdo?

Desde mi punto de vista, de un teléfono móvil se puede sacar información muy delicada. Un troyano en un móvil podría controlar desde el lugar del mundo donde está el teléfono (por la celda) y enviárselo a quien controle el troyano, hasta enviar toda la lista de contactos por mms a alguien, o hacer que el troyano envié sms o mms a donde tú quieras, y bueno, en general cualquier cosa que pueda un usuario hacer con el móvil, puedes hacerla programáticamente, además de muchas cosas que un usuario no podría. Así que todo es darle rienda suelta a la imaginación...

En cuanto a perjudicar a Microsoft, no creo (si acaso a Symbian Ltd.). De todas formas aunque Microsoft está entrando en el mercado de móviles creo que lo va a tener difícil... aunque claro,... es Microsoft, donde pisa no crece más la hierba...

¿Crees en los virus como forma de comunicar un mensaje o una lucha?

Puede ser. Los virus perjudican la imagen de las grandes empresas, o sea que se podría ver por ahí la cara reivindicativa de este hobby. Pero, por otro lado, otras grandes empresas están ganando mucho dinero gracias a los virus y los problemas de seguridad.

Alguna vez he metido algún mensaje que quería hacer ver. Uno que hice hace mucho tocaba la canción: «*What if god smoked cannabis?*» por el speaker. Es una manera más de lanzar una idea o un mensaje a cuantos más mejor.

¿Qué papel crees que juegan las empresas que desarrollan antivirus en esto? ¿Salen perjudicadas o beneficiadas con la creación de virus?

Beneficiadas, sin duda. Lo que no creo es el mito ese famoso de que las empresas antivirus contratan gente para hacer virus. Pero que salen beneficiadas de la aparición de nuevos virus, eso seguro.

¿Algo que nos hayamos dejado en el tintero en esta entrevista?

Pues en principio nada más a destacar, creo que ha estado muy completa.

LA DESOBEDIENCIA CIVIL ELECTRÓNICA, LA SIMULACIÓN Y LA ESFERA PÚBLICA

Critical Art Ensemble*

«Lo que cuenta, en última instancia, es el uso que hacemos de una teoría... Debemos tomar las prácticas existentes como punto de partida para buscar los errores fundamentales.»
Felix Guattari,
Por qué Marx y Freud ya no molestan a nadie

En 1994, cuando el Critical Art Ensemble (CAE) introdujo por primera vez la idea y posible modelo de la desobediencia civil electrónica (DCE) como otra alternativa dentro de la resistencia digital, el colectivo no tenía forma de saber qué elementos resultarían más prácticos, ni sabía qué ulteriores explicaciones serían necesarias. Tras casi cinco años de trabajo sobre el terreno en torno a la DCE, llevado a cabo tanto por colectivos como por personas que trabajan aisladamente, las lagunas de información han ido quedando algo más patentes y podemos por fin ocuparnos de ellas. Este ensayo examina con especial atención el giro que se ha producido en la situación y que ha generado un modelo de DCE en el que predomina el espectáculo público frente a la subversión clandestina de políticas y que da mayor importancia a la acción simulada frente a la acción directa. El Critical Art Ensemble (CAE) sostiene que este tipo de tendencias dentro de la investigación general sobre DCE son poco oportunas. El CAE sigue creyendo que la DCE es una actividad underground que (al igual que la tradición hacker) debe permanecer al margen de la esfera pública o popular y de la mirada de los medios. El Ensemble también mantiene que las tácticas de simulación que están utilizando las fuerzas de resistencia son sólo parcialmente efectivas, cuando no contraproducentes.

* Traducción del inglés de Carolina Díaz.

CIBERFIASCOS FAMOSOS

En 1999 cuando la existencia en Internet del grupo de artistas suizos eToy fue seriamente amenazada por una compañía de juguetes, eToys (nótese la diferencial «s» final), hubo un montón de gente que reaccionó de forma solidaria y dispuesta a la acción. Los detalles eran, como poco, sorprendentes: la multibillonaria compañía eToys Inc. había convencido a un juez californiano para que prohibiera a eToy usar el dominio eToy.com que ya llevaba tres años en la red, desde mucho antes que la compañía eToys siquiera existiera. ¿Los fundamentos de la decisión judicial? Pues que la gente, el inocente niño o niña, podía confundirse y creer que las imágenes de colorines de eToy eran juguetes puestos a la venta.

LA DESOBEDIENCIA CIVIL EN LA ESFERA PÚBLICA

Aquellos que estén familiarizados con el modelo de DCE planteado por el Critical Art Ensemble[1] sabrán que se trata de una inversión del modelo de desobediencia civil (DC). En lugar de intentar crear un movimiento de masas de elementos públicos de oposición, el CAE sugirió la idea de un flujo descentralizado de microorganizaciones diferenciadas (células) que produjesen múltiples corrientes y trayectorias, con el fin de frenar la velocidad de la economía política capitalista. Esta sugerencia nunca fue del agrado de los activistas más tradicionales, y recientemente el modelo ha sido criticado incluso por Mark Dery (en *Mute* y *World Art*). Dery arguyó que este modelo provocaría conflictos entre los objetivos y actividades de las diversas células. La CAE sigue manteniendo que, por el contrario, los conflictos derivados de la diversidad de las células no debilitarán el proyecto sino que lo fortalecerán. Esta diversidad daría pie a un diálogo entre diversas manifestaciones que se resistirían a la estructura burocrática a la vez que abrirían un espacio para accidentes afortunados e invenciones revolucionarias. Si la cultura de la resistencia ha aprendido algo a lo largo de los últimos 150 años, es que «el pueblo unido» es una falacia que sólo sirve para construir nuevas plataformas de exclusión. Esto sucede al crear monolitos de burocracia y regímenes semióticos que no pueden representar ni actuar en nombre de los distintos deseos y necesidades de los individuos dentro de segmentos sociales complejos y en proceso de hibridación.

La segunda inversión clave en el modelo de desobediencia civil era la de perseguir directamente un cambio de política, en vez de hacerlo de forma indirecta a través de la manipulación de los medios. El Ensemble sigue considerando la estrategia directa como la más efectiva. La estrategia indirecta, la de la manipulación de los medios a través de un espectáculo de desobediencia destina-

1. Para más información: todos los libros del CAE, entre otros *Electronic Civil Disobedience*, están disponibles en Autonomedia (NYC) o se pueden descargar gratis en http://mailer.fsu.edu/~sbarnes. También se pueden conseguir versiones en alemán (Passagen Verlag), francés (l'eclat) e italiano (Castelvecchi), aunque no en la red. Contactar con el CAE para más información.

Es verdad que hay jueces con una mente muy especial en California. Para ayudar a eToy y a la digna causa de la libre expresión y el arte en general, se incentivaron proyectos en contra de los malvados eToys Inc. Se sacó entonces un comunicado de prensa en el que los titulares decían: «Nuevo juego en Internet diseñado para destruir eToys.com», lo bastante sensacionalista, en efecto, como para ayudar a los periodistas a construir sus artículos y pareciendo incluso «objetivos»...

Funcionó bien y bastante rápidamente, no para destruir a eToys (ninguno de nosotros estaba tan ido) sino para llamar la atención sobre el caso. Cientos de agencias de noticias, incluyendo a la CNN, la revista TIME, Associated Press, etc., cubrieron la historia, por lo general desde el punto de vista que les ofrecíamos en nuestra nota de prensa, y casi siempre mostrando simpatía por nuestra causa.

do a conseguir la aprobación y el respaldo de la opinión pública es una propuesta destinada al fracaso. La década de los sesenta terminó ya, y no hay una sola agencia corporativa o gubernamental que no esté en condiciones de librar la batalla de los medios. Se trata sencillamente de una cuestión práctica de inversión, de capital. Los medios de masas tienden a ponerse del lado de lo establecido, las ondas radiofónicas y la prensa pertenecen a entidades corporativas y las estructuras capitalistas disponen de gran cantidad de fondos destinados a las relaciones públicas. Por eso, no hay manera de que los grupos de activistas puedan superarles en ese terreno. Fragmentos aislados de información no pueden subvertir el proceso de creación de políticas ni alterar la opinión pública cuando todos los demás medios de masas están transmitiendo el mensaje contrario. Toda opinión subversiva se pierde en el bombardeo de los medios, si es que la oposición no la tergiversa para sacarle provecho. En otro tiempo, la combinación de desobediencia civil con manipulación de medios conseguía desestabilizar y dar la vuelta a los regímenes semióticos autoritarios. Un ejemplo excelente es el caso del Movimiento de los Derechos Civiles. Los participantes en el movimiento se dieron cuenta de que la Guerra Civil seguía librándose a nivel ideológico, de manera que podía ponerse a una región social, política y geográfica en contra de la otra. En las regiones del norte y el oeste de los EEUU no sólo se había producido un desarrollo industrial, sino también un desarrollo en los métodos de control de la población y en particular de las minorías. La Guerra Civil había acabado con la retrógrada economía política del sur, pero no había logrado alterar su estructura ideológica (un elemento mucho más difícil de modificar) y, por lo tanto, no había alterado sus mecanismos simbólicos de control. Lo único que necesitaba hacer el movimiento de los derechos civiles era hacer evidente este fracaso, y las plenamente modernizadas regiones del norte se encargarían de obligar al sur a adoptar una postura ideológica más compatible con las necesidades socioeconómicas del capitalismo avanzado. Las imágenes que surgían en los actos de desobediencia civil lograron suscitar

Curiosamente, por aquel entonces las acciones de eToys empezaron a bajar y a bajar en la Bolsa: de los 67 dólares por acción de antes de la «campaña» a los 20 $ cuando el caso estaba en toda la prensa, hasta llegar a los 5 $ en que de momento se ha quedado.

Costó un mes de protesta pública, llevada a cabo desde cientos de nodos diferentes, convencer a eToys de que no se comportara como lo había hecho. El 29 de diciembre, justo 30 días después de la primera orden del juez cerrando la pagina de los artistas, eToys anunció que retiraba la demanda contra www.etoy.com.

Cuando estabamos todos ya a punto de celebrarlo, la gente de eToy, los artistas, nos llamaron diciendo que en realidad se trataba de una trampa, que eToys no iban a retirar la demanda «realmente» y que había que seguir peleando.

la indignación del norte ante la ideología retrógrada del sur y que se declarase de nuevo el estado de guerra entre las regiones. Estudiantes voluntarios, asistentes sociales, y eventualmente el cuerpo de la policía federal y el ejército (movilizados por el gabinete ejecutivo) se aliaron y lucharon en favor del movimiento.

A pesar de todo, los dirigentes del Movimiento de los Derechos Civiles no pecaban de ingenuos. Sabían que las únicas leyes racistas que se eliminarían serían las que no estaban vigentes en el norte, que no se iba a acabar con el racismo. Éste simplemente se transformaría en una manifestación más sutil de la endocolonización que contrastaría con el racismo de la época, que se manifestaba de forma explícita en una serie de leyes segregacionistas. De hecho, la convicción compartida por todos los afroamericanos de que existía un barrera sólida más allá de la cual la política no podía avanzar fue clave en la rápida decadencia del movimiento y en la rápida ascensión del movimiento del Poder Negro (*Black Power*). Por desgracia, este último movimiento no sacó más partido de su campaña mediática que el primero, quizás por carecer de la infraestructura para cubrir sus propias necesidades materiales. En el caso del movimiento de los derechos civiles, la desobediencia civil como método de manipulación de los medios obtuvo resultados porque la dinámica histórica del capitalismo actuó de plataforma para su éxito. La historia era todavía heterogénea y la manifestación normativa de la ideología capitalista era aún un espacio irregular, tanto a nivel nacional como internacional. Pero, ¿qué podemos hacer ahora que hemos llegado a un punto en que las ideologías visibles y diferenciadas de Occidente han dejado de existir, y en que la historia no es más que una ficción uniforme que repite una y otra vez las victorias capitalistas? ¿De dónde surgirá la indignación del público? ¿Qué ejército, qué gobierno, qué corporación, qué poder apoyará a los desposeídos cuando las explotadoras relaciones endocoloniales son precisamente lo que permite a estas agencias florecer? Por ello, el CAE defiende el enfrentamiento directo utilizando un impulso económico obtenido gracias al bloqueo de información privatizada (filón de oro del capitalismo tardío).

El cabreo fue enorme, por supuesto, e inmediatamente nos pusimos todos de nuevo en marcha. Mandamos otra nota de prensa que fue reproducida, entre otros, tal cual por Bloomberg, el principal diario financiero...

La lucha siguió por un periodo adicional de 18 días, en mitad del cual, eToy finalmente presentó su propio vehículo de protesta: www.toywar.com, en el que llevaban trabajando desde noviembre, cuando se les amenazó por primera vez. Toywar.com consistía en una serie de imágenes de pequeños guerreros de juguete que los visitantes de la página podían adoptar como avatares en su lucha contra los malos de eToys.

Tras adoptar uno de estos guerreros, el visitante debía esperar a recibir instrucciones del Estado Mayor de Toywar, que especificarían misiones y objetivos.

Hacerse con los medios no ayuda a socavar el régimen semiótico autoritario, ya que ninguna base de poder se beneficia de escuchar un mensaje alternativo. Sin embargo, hacerse con los beneficios bloqueando la información constituye un mensaje claro para las instituciones capitalistas, a las que les puede resultar más barato cambiar de política que defender militarmente un régimen semiótico en apuros. Lograr este objetivo es posible en el ámbito virtual y sólo se precisa la más modesta de las inversiones (si lo comparamos con organizar un ejército). Sin embargo, para que esta resistencia perdure son necesarias actividades clandestinas.

Actualmente, la única, tenue excepción en que la DCE puede utilizarse para manipular los medios es en casos en que la historia y la ideología no han sido homogeneizadas. Por lo general, en estas situaciones el movimiento de resistencia está en conflicto con un poder dominante que el pancapitalismo sigue considerando como algo ajeno a sí mismo. Por ejemplo, el movimiento democrático chino empleó la desobediencia civil y la manipulación de los medios con relativo éxito. Se despertó la indignación. Sin embargo, las rígidas barreras nacionales impidieron que ésta tuviera resultados más provechosos para el movimiento que la concesión de asilo en los países occidentales a quienes habían tenido que huir de las autoridades chinas, o que una tímida presión diplomática contra China. Incluso en la más favorable de las situaciones (como ocurrió con el movimiento en favor de los derechos civiles), a pesar de que el orden ideológico del pancapitalismo se sintió ofendido, el orden económico occidental consideró que tenía más parecidos que diferencias con China y, por tanto, poco hizo —el indignado— Occidente para apoyar al movimiento democrático o para dañar materialmente la infraestructura china.

Muchos de nosotros nos registramos como guerreros, a ver qué tal funcionaba la cosa, pero nunca llegamos a recibir ordenes, sólo algunos interesantes y curiosos comunicados sobre lo achuchada que estaba la cosa y tal. De lo que podíamos deducir que Toyway no iba mas allá de un bonito proyecto de arte «sobre» protesta, resistencia y cosas así. Gente del mismo Toywar nos lo confirmó así recientemente.

Tal y como los días pasaban, tras el anuncio de eToys y el silencio que le siguió, todos nos íbamos mosqueando más y más, y ahi andábamos pinchando a la gente de eToy para que finalmente se decidieran a hacer algo de lo que todos les pedíamos y ellos se resistían a hacer, siguiendo consejo de sus abogados.

Desobediencia civil electrónica y simulación[2]

Muy pronto en la historia del desarrollo de los medios electrónicos, Orson Welles demostró (quizás por accidente) los efectos materiales de la simulación. La simulación de un boletín de noticias en que se anunciaba que unos alienígenas habían invadido la Tierra provocó un leve pánico en las personas que quedaron atrapadas en la sala de los espejos que se formó con la implosión de la ficción y no ficción provocada por el anuncio. Sólo había cierto grado de credibilidad en lo que a la verdad de la historia se refiere. Simultáneamente, toda la información era verdad y toda la información era mentira en aquel momento histórico en que hizo irrupción lo hiperreal. Hemos visto cómo se reproduce esta narrativa en la década de los noventa en el marco de la cultura de resistencia electrónica, pero con algunas peculiares diferencias.

En un apéndice a *ECD and Other Unpopular Ideas*, escrito en 1995, el CAE observó que existía una creciente paranoia entre las agencias de seguridad de los Estados Unidos que deseaban controlar la resistencia electrónica. Resulta curioso que estas agencias se metieran miedo a sí mismas con sus concepciones de lo que es la criminalidad electrónica. Es como si Welles se hubiese asustado con su propio anuncio. En ese momento cómico, el CAE propuso con cierta ironía que la DCE había sido un éxito sin esforzarse demasiado, y que sólo la advertencia de que iba a producirse algún tipo de resistencia electrónica provocaba el pánico en las agencias de seguridad, hasta tal punto que su objetivo principal quedaría atrapado en la hiperrealidad de las ficciones criminales y de la catástrofe virtual. Éste es un comentario que el CAE desearía no haber hecho nunca, ya que algunos activistas han empezado a tomárselo en serio y están intentando actuar de acuerdo con él, principalmente utilizando la red para producir amenazas de activismo hiperreales, con el fin de azuzar el fuego de la paranoia de los estados-corporación. Una vez

2. El CAE quisiera agradecer a Heath Bunting su valiosa contribución al desarrollo del modelo de CAE para la subversión simulacionista.

Queríamos, por ejemplo, que publicaran toda la documentación judicial del caso, para que la docena de abogados que se habían ofrecido voluntariamente a iniciar acciones legales contra eToys pudiera estudiarla y empezar a trabajar.

Finalmente fuimos tan insistentes que nuestro contacto en eToy nos confesó la verdad: el 29 de diciembre eToys, la empresa malvada, estaba más que dispuesta a retirar la demanda judicial, ofreciendo además unos términos excelentes (pagaban ellos todos los gastos jurídicos, etc.). Pero fue eToy, el grupo de artistas, quien decidió retrasar el acuerdo, de modo que tuvieran unos días más de «conflicto» para poner Toywar.com en «acción». Claro, llevaban tiempo trabajando sobre los guerreros de juguete y aún no estaba acabada la obra, ¿cómo iban a aceptar la rendición del enemigo antes de haber acabado ellos siquiera de presentar su temible ejército? Si la batalla acababa enton-

más, se trata de una batalla mediática destinada a ser perdida. El pánico y la paranoia del estado se transformarán a través de los medios de masas en paranoia pública, y ésta, por su parte, no hará sino reforzar el poder estatal. En los Estados Unidos, el público con derecho de voto apoya de forma invariable penas más duras para «criminales», más cárceles, más policía; y es esta paranoia hiperreal la que consigue los votos que los políticos paladines de la ley y el orden necesitan para convertir estas corrientes de opinión en legislación o en directrices del gobierno. ¿Cuántas veces hemos sido testigos de ello? Del maccartismo, del temor de Reagan por el Imperio del Mal, de la guerra contra las drogas: en todos estos casos el resultado ha sido la cesión de más fondos al ejército, a las agencias de seguridad y las instituciones disciplinarias (con la plena connivencia de un público de votantes atemorizado y paranoico). Así se aprieta más el cinturón endocolonial. Teniendo en cuenta que los Estados Unidos se están ocupando de la rápida creación y expansión de agencias de seguridad destinadas a controlar la criminalidad electrónica (y dado que estas agencias no hacen distinciones entre acciones motivadas por convicciones políticas y las motivadas por el lucro), parece un error facilitar a los vectores de poder medios de conseguir el apoyo del público para este desarrollo militar, así como una base para aumentar la legislación nacional e internacional en lo que al control político de los medios electrónicos se refiere.

Es difícil decir si se podrían emplear las tácticas de simulación de modo más persuasivo. Ya que tanto la CIA como el FBI han estado empleando estas tácticas durante décadas, no es difícil encontrar ejemplos que se podrían invertir. Uno de los casos clásicos es el derrocamiento del gobierno de Arbenz en Guatemala con el fin de apoyar a la United Fruit, proteger los intereses petrolíferos y minar una democracia con tendencias tan izquierdistas que legitimó el Partido Comunista aun estando dentro del campo de influencia de los Estados Unidos. Desde luego, la CIA construyó una buena infraestructura operacional utilizando el sabotaje económico para provocar inestabilidad, pero el acto final fue el de la subversión electrónica. La CIA

ces, eToy quedaría con el poco heroico papel de la víctima amenazada en cuya ayuda habían acudido multitud de activistas que habían conseguido acoquinar al enemigo, etc. Esto desde luego no cuadraba con la cuidada imagen de ciberterroristas que eToy se había esforzado en cultivar. Éste era un grupo que, al fin y al cabo, habían hecho carrera con un «secuestro digital» y que desde entonces no había dejado de alimentar, incluso de atiborrar, esa imagen de clandestinos y fuera-de-la-ley.

Pese a que de alguna forma nos habíamos visto abocados a sacar nuevos comunicados de prensa, a seguir peleando y a incitar a nuestros compañeros a seguir haciéndolo también, y todo ello sin ninguna razón real, decidimos no molestarnos: después de todo esta lucha adicional había generado más repercusión en prensa, incluso un mayor fortalecimiento de la comunidad de activistas, etc. Estábamos contentos con los resultados.

simuló transmisiones radiofónicas de movimientos de tropas antigubernamentales en torno a la capital. Al interceptar estos mensajes, el gobierno guatemalteco no dudó de que un ejército rebelde se había reunido y estaba preparándose para el ataque. Nada más lejos de la realidad: el pueblo apoyaba masivamente al gobierno y sólo existía una pequeña facción rebelde. Por desgracia, algunas autoridades del gobierno se dejaron llevar por el temor y cundió el caos en su seno. El FBI utilizó un método de subversión similar al ataque contra los Panteras Negras en el que utilizaron comunicaciones hiperreales. Igual que la intervención de la CIA en Guatemala, la infoguerra del FBI contó con una fuerte infraestructura. La organización estaba infiltrada en el Partido de los Panteras Negras (Black Panther Party, BPP) y había conseguido llegar cerca de su dirección. Así conocía la naturaleza (y los protagonistas) de las luchas internas del partido. También había conseguido el apoyo de las fuerzas locales de seguridad con el fin de hostigar a las secciones en todo el país. La tesorería del partido estaba siempre vacía por las constantes detenciones practicadas por miembros de la policía que intencionadamente abusaban de su poder, con el fin de drenar las arcas del partido al forzar a los miembros a pagar fianzas para los detenidos. En estas condiciones, la paranoia estaba a la orden del día entre los Panteras Negras y, cuando se produjo la ruptura entre la sección de San Francisco y la de Nueva York, el FBI vio la oportunidad perfecta para provocar la implosión del partido. Como resultado de una sencilla campaña de envío de cartas que avivó las llamas de la desconfianza entre los cabecillas del este y los del oeste, el partido se desmoronó, víctima de las luchas internas. (La campaña del FBI consistió en crear y enviar documentos que parecían venir de una facción de oposición dentro del partido y en que se criticaba a líderes específicos y sus políticas de partido.)

Se podría invertir el método y volverlo contra las agencias de la autoridad. Las luchas internas que ya tienen lugar dentro del gobierno, y entre éste y las instituciones corporativas, hacen de ellos sus propias víctimas. El ejército y la infraestructura económica que fueron necesarias para las operaciones en los ejemplos citados no

Pero cuando se empezó a contar la historia en unos términos que atribuían la victoria sobre eToys al funcionamiento de la terrible maquina de guerra de Toywar, nos pareció que el trabajo de los activistas autónomos que habían reaccionado a tiempo y, de hecho, salvado a eToy, estaba siendo ignorado de muy mala manera.

Moraleja: una cosa es una cosa y otra cosa es otra cosa, o bien una cosa son las redes de gente dispuesta a cooperar y liarla y otra cosa, como diría el Iñaki, son los teatrillos cutres de toda la vida.

son precisos para las operaciones de DCE, ya que la guerra interna ya está en marcha (dado que la tendencia natural del capital hacia la depredación, el miedo y la paranoia forman parte de la experiencia cotidiana de los que entran dentro de las coordenadas del poder, y por lo tanto no es necesario gasto alguno para provocarlo, como fue necesario en el caso del Partido de los Panteras Negras). Sin duda, cartas o mensajes por correo electrónico cautamente redactados y enviados podrían tener un efecto implosivo (aunque dudo que provocasen un colapso total); sin embargo, hemos de asimilar y aplicar las lecciones aprendidas de estos casos clásicos de tácticas de simulación. Lo primero y más evidente es que esta forma de resistencia debería hacerse de forma encubierta. Además, es necesaria información interna fidedigna. Éste es el área más problemática dentro de este tipo de maniobra táctica, aunque no es imposible encontrar una solución. Para lograr una utilización eficaz de las tácticas de simulación, deben desarrollarse métodos y medios de investigación, obtención de información y reclutamiento de informadores. (El CAE está dispuesto a apostar que el próximo escrito revolucionario sobre resistencia tratará de este problema, el de la generación de inteligencia amateur). Hasta que esto ocurra, la acción subjetiva-subversiva será poco eficaz. De momento, quienes no cuenten con una estrategia encubierta plenamente desarrollada sólo pueden actuar tácticamente contra los principios estratégicos de una institución, no contra situaciones y relaciones específicas. Evidentemente, una respuesta táctica a una iniciativa estratégica no tiene sentido. Resulta muy probable que una acción de este tipo no tenga los resultados deseados y sólo alerte a la agencia víctima de la acción para prepararse contra posibles presiones externas.

Debemos también recordar que la infoguerra simulacionista es sólo una táctica destructiva: es una forma de causar una implosión institucional, y tiene poco valor productivo en cuanto a la reconstrucción de políticas. Volviendo al ejemplo del racismo, agencias que han institucionalizado políticas racistas (y en esto se incluyen casi todas las instituciones del régimen pancapitalista) no cambiarán por una infoguerra de desgaste institucional. El régimen semiótico de políticas racistas

continuará intocable dentro de otras instituciones interrelacionadas debido a los beneficios comunes que consiguen manteniendo estas políticas. El CAE insiste en que no se conseguirán instituciones que desafíen el *status quo* y que sean productivas a través de gestos nihilistas, sino mediante la introducción de cambios en el régimen semiótico sobre una base institucional, a la par que se mantiene intacta la infraestructura material para la reinscripción.

El problema de la contención

Controlar las materialmente destructivas tendencias de la hiperrealidad tiene otras consecuencias problemáticas cuando se aplican estos códigos de destrucción al espectáculo. Muy llamativo resulta el problema de la contención. Si una agencia autoritaria cree ser víctima de un ataque o estar amenazada (catástrofe virtual aplazada) y por ello pasa a ser el centro de atención de la opinión pública, atacará de manera totalmente impredecible. Puede actuar de una manera que le resulte perjudicial a sí misma, pero también puede actuar de modo perjudicial para miembros desprevenidos de la esfera pública. Al introducir al público en la ecuación, las agencias amenazadas deben enfrentarse a una consecuencia de gran importancia: para mantenerse al ritmo de la infoesfera deben actuar con celeridad. Vacilar no es una opción, aunque sea para analizar racionalmente el problema y reflexionar. En el actual mercado de relaciones públicas, el éxito y el fracaso han sufrido una implosión, y toda acción, cuando se representa bien, se sitúa en la esfera de la victoria y el éxito hiperreal. La única distinción útil que se puede hacer es entre acción y pasividad. La pasividad es el signo de la debilidad y la ineptitud. Atrapada en este vector de alta velocidad, una agencia amenazada emprenderá una acción explosiva (no implosiva). Se escogerán los chivos expiatorios y seguidamente se emprenderá una acción contra estos individuos o grupos poblacionales. (El macrocosmos perfecto de esta secuencia de acontecimientos está representado en la política exterior de los EEUU y las acciones que se realizan en su nombre.) En otras palabras, una vez la amenaza provoca la secuencia de destrucción (ya sea la amenaza virtual o real), la fuerza de resistencia no podría contener ni redirigir las fuerzas, a menudo fuera de control, que se liberarían. Esta incapacidad para contener la explosión hace de este modelo (sólo en sus efectos) algo próximo al terrorismo. No es que los activistas estén dando pie a una práctica terrorista (nadie muere en la hiperrealidad), pero el efecto de estas acciones puede tener las mismas consecuencias que el terrorismo, en cuanto que el estado y los vectores del poder corporativo contraatacarán con armas cuyos efectos serán materialmente destructivos e incluso mortales.

Lo extraño es que una acción de estas características no estaría motivada por una preocupación por la infraestructura, sino por el régimen semiótico y la imagen pública de la entidad en la hiperrealidad. Sin embargo, cuando se saca al público de la ecuación, la secuencia cambia radicalmente. La agencia bajo presión no tendría que actuar con tanta precipitación. Tendría tiempo de investigar y

de lanzar un ataque más preciso, porque las muestras de debilidad (la imagen pública de pasividad) no tendrían el efecto perjudicial que tiene su representación pública intencionada. En ésta, la peor situación imaginable para los activistas, la respuesta sería mucho más precisa, y por tanto las consecuencias las pagarían aquellos que se arriesgaron a emprender la acción. Si la agencia no se da cuenta de esta amenaza de subversión y tuviera lugar la implosión, el público no tendría noticia ni sentiría las consecuencias directas (aunque sí cabría esperar consecuencias indirectas, como un aumento del paro). En cualquier caso, la metralla de una explosión violenta no alcanzaría el paisaje de la resistencia. En otras palabras, la contención se actualizaría. También resulta interesante que la agencia bajo presión financiará actividades de contención. Ninguna agencia quiere hacer públicos sus problemas financieros, una brecha en su sistema de seguridad, etc. Por lo tanto, construirá sus propios diques. Sin embargo, si el público entra en la ecuación, desaparecen todas las probabilidades de contención y las consecuencias son menos que aceptables. Por esta razón el CAE sigue creyendo que todos los modelos útiles de DCE (o a todos los efectos, casi cualquier acción política que no sea de concienciación o pedagógica[3]), dentro de las condiciones políticas actuales comparten su naturaleza encubierta y la aversión hacia los medios de masas como escenario de la acción.

Escribir el discurso sobre DCE

Dado el deseo de mantener a los medios de masas ajenos a la DCE, el CAE consideró oportuno terminar con algunas sugerencias sobre cómo hablar semipúblicamente sobre lo que debe debatirse entre compañeros dignos de confianza. Este problema no es nada nuevo, por lo que, afortunadamente, existen antecedentes (el más notable, el de la Escuela de Frankfurt). Su estrategia consistía en redactar en el estilo más denso y arcano que se pueda imaginar, de tal modo que sólo los iniciados podían descifrarlo. De este modo, el discurso permanecía fuera de la esfera pública, siendo imposible su asimilación por el mercado. Afortunadamente no es necesario llegar a esos extremos. La redacción puede ser clara y accesible, pero debe ponerse a salvo de la mirada de los medios. Esto es sencillo. Lo único que hace falta es hacer de él una mala imitación. Por eso el CAE habla en términos de modelos generales y casos hipotéticos (sin hablar nunca de acciones concretas). No sólo no queremos hacer públicos datos específicos, por razones evidentes, sino que, para la mayor parte del público de los medios populares, las generalidades y los modelos no son de mucho interés. Los modelos son lentos y librescos, y en la veloz vorágine de imágenes del espectáculo popular resultan sencillamente aburridos.

3. Una situación o acción pedagógica da a los participantes la oportunidad de huir de algún tipo de autoridad que se daba por supuesto. En ese momento de liberación pueden pensar en alternativas con respecto al tema específico o general que se trata. Este tipo de labor entra dentro de la acción cultural politizada. Pero esta acción es sólo pedagógica, no política. Prepara las conciencias de los individuos para nuevas posibilidades y, en el mejor de los casos, les induce a la acción política. La actividad inspirada por situaciones pedagógicas se considera acción política. Cuando habla de acción política, el CAE se refiere a la redistribución o reconfiguración temporal o permanente de las relaciones de poder (material o semiótico). También queremos comentar que la distinción entre estas categorías no debe considerarse integral sino como una representación de la tendencia general en la tipología de la acción activista.

El CAE también sugiere estudiar acciones estratégicas históricas análogas, en particular las que han sido provocadas por vectores de poder autoritario. A ninguno de los medios populares le interesa especialmente hablar más de ellos, de los tiempos de antaño, ni les interesan las atrocidades del pasado (excepto las perpetradas por los nazis). El análisis de estos temas deja a los medios sin nada interesante para el público. Esta estrategia se refiere a temas de constelaciones, desviaciones, apropiación, etc. Utiliza lo que ya está disponible, no des nada a los buitres mediáticos, y lo único que les quedará para la apropiación será el canibalismo (de ahí la proliferación de lo retro). A estas alturas ya casi no se puede evitar el que los medios se apoderen de la DCE. Ya se ha vendido a cambio de 15 minutos de fama y está potenciando una nueva ola de auge cibernético, pero los activistas electrónicos pueden suspender este acontecimiento mediático dejando de suministrar material. Podemos estar agradecidos por que la DCE y otras formas de resistencia electrónica que se han desmaterializado dentro del mundillo hiperreal del hacktivismo sean cibermodas que desaparecerán rápidamente en el tecnohorizonte y dejarán a los comprometidos que sigan con su trabajo como de costumbre.

LUFTHANSA: EL ACTIVISMO *ON-LINE* BAJO PRESIÓN *

«Los ordenadores de los activistas alemanes fueron requisados por la policía política: la nueva legislación iguala el «hacking» con el terrorismo.»
Armin Medosch

A primeras horas de la mañana, en Frankfurt la policía política uso la fuerza para acceder a las salas de la oficina de la iniciativa Libertad! y requisó todos sus ordenadores, discos duros, Cd's y documentos.

La policía también acudió al piso de uno de los responsables de los dominios libertad.de y sooderso.de y requisó el equipo que allí se encontraba. Antecedentes: Libertad había participado en una manifestación *on-line* contra la compañía aérea alemana Lufthansa. Una amplia coalición de asociaciones está trabajando en una campaña bajo el nombre «deportation alliance», donde se combinan métodos políticos de protesta *on-line* y *off-line* porque Lufthansa permite a la policía usar sus vuelos para deportaciones forzosas de solicitantes de asilo. Dos personas han muerto en dichos vuelos debido a los métodos de inmovilización empleados. Deportation Alliance denuncia que Lufthansa está beneficiándose de la muerte y el sufrimiento de la gente. Lufthansa dice que se ve obligada a hacerlo porque la ley le obliga a poner sus aviones a disposición del estado.

El 20 de junio se produjo una escalada en la lucha con la realización de una manifestación *on-line* contra Lufthansa. Más de 150 organizaciones participaron en la preparación de la manifestación *on-line*, 30 servidores publicaron material, un «manual del usuario» y un software especialmente diseñado. Sin embargo, las organizaciones hicieron hincapié en que su software era muy distinto de herramientas como floodnet o stacheldraht, que pueden ser utilizadas para los llamados «ataques de denegación de servicio distribuido (ddos)». Los ataques ddos pueden tumbar los servidores más sofisticados, como se demostró con los ataques realizados en el año 2000 contra yahoo y ebay y otras empresas de comercio electrónico que, a día de hoy, todavía no se sabe quién los realizó.

La manifestación *on-line* de Deportation Alliance era de un talante distinto. Siguieron el principio de «una persona, una voz», que se asemeja más a una sentada pacífica o a la acción de un piquete que a un ataque ddos. La única razón que hacía necesario el software era que la mayoría de las páginas del servidor de Lufthansa son formularios y páginas crea-

* Texto original en http://www.e-c-b.net/ecb/news/articles/1003337964, 7.10.2001

das para los vuelos, en función de los datos introducidos por el usuario. El software ayuda a rellenar automáticamente los formularios y por tanto ralentiza el proceso de reserva.

La manifestación *on-line* contra Lufthansa nunca intentó colapsar totalmente el servidor y, además, tampoco lo consiguió. Tuvo un carácter eminentemente simbólico, era una manera de llamar la atención sobre las prácticas problemáticas de la aerolínea. Además, se había solicitado previamente un permiso para la manifestación en la oficina policial correspondiente de la ciudad de Colonia como cualquier otra manifestación política legal. Esto fue realizado a sugerencia de los abogados de Deportation Alliance, pero tampoco se esperaba que fuese tomada en serio. Inmediatamente sacó a la luz las implicaciones políticas y legales que conllevaba una manifestación *on-line*. En primer lugar abre el debate sobre el tema de Internet como «espacio público». Y si es un espacio público entonces debe existir el derecho a que la gente se reúna libremente y haga una manifestación. Los organizadores de la manifestación *on-line* aducen que esto era exactamente lo que estaban haciendo. El Ministerio de Justicia alemán opina otra cosa. Un portavoz argumentó que el derecho de manifestarse sólo es válido en el mundo real.

Los abogados de Lufthansa debieron estar de acuerdo porque pusieron una demanda diciendo que se produjeron 1,2 millones de hits en lufthansa.com, en pocas horas, provocadas por más de 13.000 direcciones ip, que causaron un daño económico sin especificar; que la acción tenía la intención de ser «coercitiva» y que el llamamiento a la participación era una «incitación a causar daños». Sin embargo, no fueron demasiado diligentes a la hora de hacer sus deberes, y no consiguieron descubrir a los promotores de la iniciativa de manifestación *on-line*. Libertad, la organización cuyo equipo fue requisado, no fue ni mucho menos el centro de la acción. Fue uno de los muchos sitios web que publicaron el llamamiento a la participación, al albergar una réplica con las páginas de la manifestación *on-line* y ofrecer el software de 100 k para su descarga.

El caso está todavía muy fresco para llegar a ninguna conclusión, pero un portavoz de los organizadores de la manifestación *on-line* declaró a ecb-news que estaban considerando una autoinculpación masiva; eso quiere decir que todas las organizaciones involucradas en la acción contactarían con la policía y se acusarían a sí mismas de haber hecho lo mismo que Libertad y, por tanto, la policía tendría que imputarlas también a ellas. También muchos personas destacadas de los ámbitos políticos y culturales han dado su apoyo a la acción de junio y quizá se les

pueda convencer para que se autoinculpen. No se sabe si la acción va a seguir ese curso, pero una cosa está clara: Lufthansa ha demostrado tener muy poco juicio al denunciar a un pequeño grupo antirracista, pues esto seguro que les da mala publicidad, algo mucho peor para ellos que el «daño económico» de la manifestación *on-line*.

El problema, sin embargo, estriba en una serie de cuestiones que no han sido aclaradas sobre la naturaleza del ciberespacio. ¿Hay un espacio público en el ciberespacio? Los políticos y los grandes medios de comunicación en los últimos años han hecho todo lo posible para demonizar Internet como un terreno propicio para extremistas, pedófilos y otros peligrosos criminales.

Esta continua propaganda ha llevado a aprobar una legislación muy cuestionable. El Reino Unido aprobó una nueva «Ley contra el terrorismo 2000» que, entre otras cosas, dice que el hacking puede ser terrorismo, entendiendo por hacking el acto de provocar daños en sistemas informáticos; según esta ley, se puede considerar «actividad terrorista» el acto de amenazar con dañar sistemas informáticos o incitar a otros a hacerlo «por razones políticas o ideológicas».

Ahora nuestra benefactora y quierosersuperpoderosa Unión Europea está en periodo de consultas para la adopción de una nueva legislación antiterrorista, de la cual existe una versión en borrador que sigue al pie de la letra el ejemplo británico. ¡Hacktivistas, tened cuidado a partir de ahora! Dentro de poco seréis encerrados en la Torre de Londres, decapitados —si tenéis suerte— o descuartizados por los eurodiputados conservadores y del Nuevo Laborismo sedientos de sangre.

El Electronic Disturbance Theater y la desobediencia civil electrónica

Stefan Wray*

El «Electronic Disturbance Theater»

El Electronic Disturbance Theater (EDT) o Teatro de la Perturbación Electrónica es un pequeño grupo de ciberactivistas y artistas comprometidos en el desarrollo de una teoría y práctica de la desobediencia civil electrónica (DCE). Hasta ahora el grupo se ha centrado en sus acciones electrónicas contra los gobiernos mexicano y estadounidense para llamar la atención sobre la guerra existente contra los zapatistas y otros grupos en México. Pero las tácticas del DCE pueden ser empleadas por un amplio número de movimientos políticos y artísticos.

El Electronic Disturbance Theater, trabajando en las intersecciones de políticas radicales, arte performativo y recombinante, y el diseño de software, ha producido un dispositivo de DCE llamado FloodNet, un software usado en Internet dirigido a sobrecargar, inundar y bloquear el sitio web de un adversario. A pesar de que en el presente está haciendo de catalizador para hacer avanzar el uso de tácticas de DCE, el Electronic Disturbance Theater confía en pasar a un segundo plano y convertirse en uno de los numerosos pequeños grupos autónomos que hacen crecer y evolucionar las formas y medios de una resistencia computerizada.

Desobediencia civil electrónica

Siguiendo la tradición de la acción directa no violenta y la desobediencia civil, las propuestas de desobediencia civil electrónica toman prestadas las tácticas de ocupación y bloqueo de estos movimientos sociales previos, y las aplican ahora a Internet. Una táctica típica de desobediencia civil es

* Artículo del 17 de junio de 1998, presentado en la Socialist Scholars Conference, 20-22 de marzo de 1998, en Nueva York

que un grupo de gente bloquee físicamente —con sus cuerpos— la entrada de un edificio u oficina de un adversario o que ocupen físicamente la oficina para hacer una sentada.

La desobediencia civil electrónica, como forma de realizar una acción directa descentralizada y masiva, usa los bloqueos virtuales y las sentadas virtuales. Al contrario que ocurría con la tradicional acción directa, el activista de DCE puede participar en un bloqueo o una sentada virtual desde su casa, trabajo, universidad o cualquier otro sitio que tenga acceso a la red. Es más, el activista de DCE puede actuar contra un adversario a cientos o miles de kilómetros de distancia. El Electronic Disturbance Theater, a través principalmente de su dispositivo de FloodNet, está potenciando maneras de conjuntar de forma global, masiva, colectiva y simultánea la desobediencia civil electrónica y la acción directa.

Zapatismo digital

Los zapatistas en Chiapas, México, entraron en la escena global justo después del 1 de enero de 1994, cuando sus comunicados, firmados por el Subcomandante Marcos fueron difundidos por todo el mundo a través de la red. Rápidamente, a través de servidores, listas, grupos de noticias y Cc (con copia) —algunos ya existentes y otros de nueva creación— : las listas, noticias, informes, análisis, convocatorias de manifestaciones, llamamientos a encuentros intercontinentales se difundieron por América, Europa, Asia, África y Australia.

Empezamos a oír que los zapatistas usaban los términos intercontinental, redes de luchas y redes de resistencia. Este nuevo medio, Internet, se convirtió en un medio vital para la trasmisión de información desde dentro de la zona en conflicto de Chiapas a otros puntos de resistencia en México, y a otros puntos más allá de las fronteras físicas de México. Hasta hace poco, el principal uso que había hecho de Internet el movimientos pro-zapatista había sido el de herramienta de comunicación.

Sin embargo, en tiempos recientes, especialmente desde la masacre de Acteal en Chiapas, a finales de 1997, Internet se ha empezado a ver no sólo como un canal de comunicación sino como un espacio para la acción directa y un espacio para la desobediencia civil electrónica. El EDT, gracias a la promoción de sus tácticas de DCE mano a mano con el movimiento pro-zapatista, está forzando la situación y se ha propuesto desafiar la visión que sostiene que Internet debería ser sólo un espacio de comunicación; Internet también ha de ser un espacio para la acción directa.

Flood Net

En enero de 1998, un grupo de Italia, la Coalición Digital Anónima, hizo circular la propuesta a través de las redes zapatistas de una sentada virtual en cinco sitios web de las instituciones financieras de Ciudad de México. El método que propusieron fue que mucha gente pulsara simultáneamente —es

decir, manualmente—la tecla de recarga de las páginas de lo sitios web seleccionados, de manera que, en teoría —si participaba suficiente gente en la acción— , estos sitios web quedarían bloqueados de forma efectiva.

Basándose en esta teoría de acción electrónica colectiva y simultánea, pero descentralizada, contra un sitio web escogido, el grupo que acabaría deviniendo el Electronic Disturbance Theater automatizó el proceso de pulsación manual repetida de la tecla de recarga. El 10 de abril, la FloodNet Tactical Version 1.0 fue presentada durante el ensayo general de una acción de desobediencia civil electrónica contra el sitio web del presidente mexicano Zedillo. En tanto que aplicación de Java, con función de actualización, la primera prueba de FloodNet enviaba una orden de recarga cada siete segundos a la página de Zedillo. Informes de los participantes y nuestras observaciones confirmaron que lo más de 8.000 participantes en esta primera acción con Flood Net bloquearon intermitentemente el acceso a la página de Zedillo, durante ese día.

El siguiente sitio elegido para una acción de desobediencia civil electrónica fue la página de la Casa Blanca de Clinton, el 10 de mayo. Se puso en marcha un dispositivo Flood Net similar. En lugar de recargar las peticiones cada siete segundos, el intervalo se redujo a tres segundos. Pero debido a que se usaron 5 *mirrors* (paginas replicadas), algunos de los cuales no tenían contadores, no se sabe con exactitud el número de participantes. Debido a la falta de informes sobre el bloqueo de la página de la Casa Blanca —y partiendo de la suposición de que la pagina de la Casa Blanca está ubicada en un ordenador mucho más potente que aquel en el que estaba alojada la de Zedillo— no se sabe bien lo que pasó, pero todo parece indicar que la página de Clinton no se pudo bloquear de forma efectiva el 10 de mayo.

El gobierno mexicano devuelve el golpe

Para protestar contra el aumento de las expulsiones de observadores internacionales de los derechos humanos, y para demostrar la capacidad de la gente que físicamente están fuera de las fronteras geográficas de México de actuar contra una agencia del gobierno mexicano, el Electronic Disturbance Theater escogió la Secretaría de Gobernación como blanco para su acción del 10 de junio. Este departamento gubernamental supervisa el servicio de inmigración mexicano y es el responsable directo de la expulsión de observadores internacionales. Gobernación también tiene bajo su control las fuerzas de seguridad pública federales que han estado actuando junto con los militares contra las comunidades zapatistas en Chiapas. El 10 de junio, el EDT usó Flood Net contra el sitio web de Gobernación, tal y como había hecho anteriormente el 10 de abril y el 10 de mayo. El gobierno mexicano devolvió el golpe. El gobierno mexicano o los programadores contratados por el gobierno habían desarrollado un mecanismo de respuesta a FloodNet.

El Electronic Disturbance Theater cree que pasó lo siguiente. Un java script fue introducido en el sitio web de Secretaria de Gobernación con la finalidad

de activarse cuando se ejecutara un FloodNet contra éste. Al activarse, el sitio de Gobernación abriría una ventana tras otra en el navegador del usuario de FloodNet. Si el usuario de FloodNet permanecía conectado suficiente tiempo, ya fuera con Netscape o Explorer, se le colgaría el ordenador. Por eso, los diseñadores de software del EDT están trabajando para corregir el problema de modo que este tipo de contramedidas resulten inofensivas en futuras acciones.

Futuros destinos

En su corta historia, el Electronic Disturbance Theater ha demostrado su capacidad para realizar acciones contra infraestructuras de oponentes políticos en Internet. Mientras tanto ha mostrado que sus acciones son de tal escala que obligan a una reacción e intervención por parte del estado, al menos por parte del gobierno mexicano.

El Electronic Disturbance Theater continuará creciendo y desarrollando tácticas como FloodNet. Eventualmente, los dispositivos tácticos como FloodNet pueden ser sólo una herramienta potencial detrás de una matriz de máquinas electrónicas y dispositivos de software a los que los ciberactivistas y los artistas tendrán acceso y de los que sabrán valerse. Esperamos que pronto el Electronic Disturbance Theater sea sólo un pequeño grupo entre una multitud de pequeños grupos, nodos y células que contribuyen a que la resistencia global electrónica pueda tener lugar.

Nosotros seguimos comprometidos a nivel internacional. En septiembre de 1998, el festival de Ars Electrónica de Linz, Austria, festival anual donde se celebra la unión de arte y tecnología, se centró en la Infowar y aceptó nuestra propuesta SWARN. Jugar con la idea de en un enjambre, como una matriz de dispositivos parecidos a FloodNet, emergiendo, actuando y dispersándose simultáneamente contra una matriz de objetivos políticos ciberespaciales. Si los pulsos electrónicos generados por nuestras acciones con FloodNet son representados por un montón de pequeñas secuencias, los pulsos electrónicos generados por un enjambre de acciones convergentes de DCE pueden convertirse en un torrente enfurecido. Te invitamos a participar, a ayudarnos a promover y crear nuevas formas de desobediencia civil electrónica.

«ES MEJOR QUE TUMBEN UN SERVIDOR A QUE TE DEN UN BALAZO»

Entrevista a Ricardo Domínguez, hacktivista mexicano

Mercè Molist*

«Lo que cuenta, en última instancia, es el uso que hacemos de una teoría... Debemos tomar las prácticas existentes como punto de partida para buscar los errores fundamentales.»

Felix Guattari,
Por qué Marx y Freud ya no molestan a nadie

RICARDO DOMÍNGUEZ

43 años. Nueva York. Padres mexicanos. Nació en Las Vegas.
Era un actor que odiaba el teatro.
The Electronic Disturbance Theatre (EDT).
Le han llamado «uno de los primeros ciberterroristas del planeta».
Ataque simultáneo al Pentágono, Zedillo y Bolsa de Frankfurt. El Pentágono respondió con Hostile Java Applet.
En los 80: Critical Art Ensemble.
Dos libros: *Electronic Civil Disobedience* y *The Electronic Disturbance. Íbamos a romper todos los sistemas*.
En el 94: zapatistas.
DoS - Virtual Sit-in.

Que las ideas caigan en la calle

Como Gibson, en el *Neuromancer*, ni hackers ni cyborgs pueden entrar en el capitalismo virtual, romper el hielo. Las panteras modernas crean miles de realidades y así los hackers pueden entrar. Decidimos ser las panteras para ayudar a los hackers, mover los espejos del capitalismo virtual.

Creamos ACT UP, acciones en la calle por el SIDA, y empezamos a usar la tecnología: fax y teléfono.

THE YES MEN

Ramonet, uno de los fontaneros de Rtmark, trabajaba en una macroempresa de videojuegos: eran un montón de diseñadores y programadores currando venga horas para hacer versión tras versión del mismo juego de San Rambo Matamoros: ahora los mata con balas explosivas, ahora con arpones balleneros, ahora con pinchos morunos: un encanto de trabajo. Cuando Ramonet se fue cansando de tanto tiro y tanta testosterona explosiva, decidió hacerle una pequeña pasada a su compañía: introduciría una ligera variación en los comandos de forma que en determinado momento del juego el Rambo dejaría el subfusil y, buscando al enemigo mas cercano, le daría un gran abrazo teletubbi y un morreo con lengua y torsión de cuello. En otras ocasiones aparecería un cerdito que, sin que el

En el 86. Tienda que no quería vender condones, llamadas cada cinco minutos pidiendo comprar condones. Al final los vendieron.

En el 89 llegamos a la conclusión de que el capital ya se ha hecho electrónico totalmente y escribimos los libros donde se dice: «El capitalismo ya dejó el mundo. El activismo callejero es incorrecto, debe hacerse en las calles electrónicas. Los hackers no nos van a ayudar porque para ellos lo único que existe es la política del código. Los políticos tampoco ayudarán, ni izquierda ni derecha».

En el 91 conoce la BBS The Thing y hasta el 94 estudia cómo funcionan los ordenadores.

1-1-94: zapatistas.

Según la Rand Corporation, los tres pies de la guerra cibernética son: lo físico, lo sintáctico y lo semántico. Los zapatistas no tenían electricidad (físico) ni código (sintáctico), sólo tenían la palabra (semántico).

En diez días había zapatistas por todo el mundo, gracias a los ordenadores. Todo pasó muy rápido. En el 97 sube otra vez la lucha zapatista. Queríamos hacer algo electrónico y el grupo Los Anónimos de Italia entraron en contacto y nos mostraron la Netstrike que ellos ya hacían. Creamos FloodNet, un script que envía peticiones a la página que se quiere.

La primera acción reunió a 18.000 personas en cuatro horas.

Inicio del hacktivismo

«Se necesita unir el cuerpo real y el electrónico —los hackers lo dividen—, decir al gobierno quiénes somos, dónde vivimos.»

Durante Ars Electronica, en 1998, hicimos un ataque contra tres sitios: Zedillo, el Pentágono y la Bolsa de Frankfurt. Nos llamaron por teléfono amenazándonos desde el gobierno mexicano, decían. Heart, un grupo hacker holandés, nos acusó de estar destruyendo la red. Éstos son los digitalmente correctos, los que

jugador pudiera evitarlo, se dedicaría a lamerle el culete al Rambo, que obviamente perdería toda su concentración en el matarile. Claro que Ramonet preparó estas variaciones para introducirlas subrepticiamente en la versión ya revisada y lista para ser copiada millones de veces y la metió, vaya si la metió, justo a tiempo de que se distribuyera con el estreno del juego.

Por supuesto que pillaron al Ramonet y lo echaron a patadas de la empresa que tuvo que dar bochornosas y enrevesadas explicaciones del tema.

Desde entonces ha llovido mucho y el modelo de sabotaje corporativo de Rtmark y los Yes Men ha ido utilizando más y más los recursos de la red para liarla a su estilo. Pronto se dieron cuenta de que la gente, usando su intuición, tecleaba los nombres de los dominios a los que querían llegar directamente en la barra de navegación: así cuando el George W. Bush, éste de ahora, se presentó a

creen que la banda ancha es más importante que los derechos humanos. Nos dijeron que el poder tumbará a todo el activismo en línea y a nosotros también. Les respondimos que nuestro sistema es táctico, nuestro hacktivismo es táctico. Para romper sistemas sólo con el HTML necesitas a miles y miles de personas. No es como un DoS (una denegación de servicio, como la que sucede cuando se activa un programa de ataque contra una página y logras hacer caer un servidor), que lo hacen dos personas. Entonces, Wired nos llamó diciendo que el Pentágono estaba atacando nuestro FloodNet, con un arma informática. El Pentágono quebró la ley porque no puede usar sus armas contra civiles

En el 99 damos nuestro código al mundo con el Disturbance Developers Kit. Sale gente en todo el mundo que lo usa para sus acciones (ehippies, contra WTO en Seattle, 500.000 personas).

Hemos salido más de una vez en portada del *New York Times*.

La NSA nos invitó a hablar con ellos. Les hicimos una performance e intentamos convencerles de que no hacemos guerra cibernética ni cibercrimen y que los zapatistas no somos terroristas. Nos dijeron que somos el comienzo del Perl Harbour electrónico y que era inmoral.

Lo que hacemos es simulación.

La guerra de los juguetes: la empresa etoys.com denunció al grupo de netart etoy.com. Hicimos un script que iba a comprar juguetes y, cuando llegaba el momento de pagar, anulaba la compra y volvía al principio. Su servicio iba cada vez más lento hasta que sus acciones se fueron por el suelo. Por primera vez, hicimos la guerra contra un cuerpo virtual (etoys no tenía tiendas).

Acción contra Starbucks: mientras pintabas un dibujo en el ordenador, el programa atacaba a su servidor; cuanto más pintas, más fuerte es la acción. Lo tumbamos. La gente nos envió después los dibujos que habían hecho.

Pensamos también que podría hacerse con la danza: alguien bailando mientras está atacando un servidor.

presidente y su nombre empezó a sonar, se dieron cuenta de que el dominio georgewbush.com estaba libre como los pajarillos y, por supuesto, lo trincaron: empezaron a meter burradas y a hacer una página delirante, pero pronto se dieron cuenta de que tenían un muy serio competidor en el Bush mismo, cuya página resultaba siempre más bizarra que la de los chicos de Rtmark.

De modo que se decidieron por un recurso muy «táctico»[7] y se dedicaron a copiar tal cual la web oficial del Bush, incluyendo sus airados avisos sobre la web falsa (y llamando falsa a la otra, por supuesto) y también ayudando al Sr. Bush a explicar mejor algunas de sus ideas. El resultado era francamente interesante como experimento de política ficción y consiguió hacer a Bush salirse de sus bastante limitadas, por lo demás, casillas haciéndole declarar todo tipo de lindezas.

Nos hemos movido de la política de la respuesta (capitalismo, socialismo, anarquismo...) a la política de la cuestión, que es más dura porque no sabemos la respuesta pero debemos tener una política de la cuestión, de cada una y de cada comunidad. Es una cuestión también poética, la más fuerte.

El hacktivismo es 98% documentación y comunicación y 2% acción sin violencia. No atacamos a gente ni a cosas físicas, sólo cosas inmateriales. No pretendemos que nada vaya a caer. Para que funcione lo nuestro, debe ser toda una comunidad, miles de personas.

hackers – crackers – hacktivistas

No vamos contra la ley.

Hay un espacio para las acciones masivas, para la comunidad no técnica, que sólo tenga que hacer clic para quejarse.

Estamos trabajando desde el siglo XXVII. Trabajar no sólo ante la crisis (problema de los hacktivistas) sino con diez años de antelación.

Zapatista Tribal PortScan: busca puertos y a los que están abiertos les manda un poema zapatista

El cracktivismo son los redireccionamientos, robar los números de tarjetas de crédito del servidor de Davos... puede pasar, pero siempre que se diga por qué se ha hecho.

ENTREVISTA

¿Vive en Nueva York?

Brooklyn.

¿Profesor de performances?

Nada más este semestre, por invitación. Soy vendedor de libros o de pizzas o de vídeos... No tengo empleo constante

¿Su ocupación es el hacktivismo?

Si me pagaran... De vez en cuando me invitan a espacios así pero nunca me ha llegado dinero directamente de eso. Ahora estoy dando clases de performance electró-

El tema tuvo su gracia sobre todo porque replanteó un interesante campo de intervención derivado de la suplantación y tergiversación sistemática de páginas web, provocando efectos constantemente fuera de la red y volviendo de nuevo a ella, en la medida en que incluso cuando ya se había desvelado la falsificación la gente seguía visitando ambas para compararlas y desternillarse a costa del copiado.

Dicho y hecho los Yes Men desarrollaron el ReamWeaver, un programilla que te permite no sólo copiar cualquier web que te guste especialmente, sino, sobre todo, mantener tu copia actualizada en relación al original, a la vez que mediante el recurso de darle algunas pistas para que cambiando las palabras clave pueda seguir la guasa sin excesivo trabajo.

nica, tratar de definir la matriz performativa, qué ha pasado, cómo se ha avanzado, cómo se puede definir. Todos los alumnos son profesores ya reconocidos en el mundo como padres y madres de la performance, que han creado este estudio.

EDT (Electronic Disturbance Theater)

Soy uno de los fundadores. Somos cuatro. Carmin Karasic, una mamá de Boston, experta en computadoras que estudió en MIT y ahora es profesora de arte, experta en encontrar problemas en sistemas; Brett Stalbum, que vive en California, profesor de arte y nuevos medios, parte de un grupo de net-art C5; y Stefan Wray, activista, escritor, que vive en Texas.

¿Son ustedes terroristas?

Se ha tratado de etiquetarnos así, pero esas marcas vienen con una filosofía de la ley. En ningún punto hemos trabajado en términos terroristas, de matar a alguien, destruir un edificio.

¿Terroristas light?

Ni eso. La desobediencia civil comienza en 1848 cuando Henry David Thoreau hizo una protesta contra la guerra de EEUU a México. Thoreau hizo su protesta sin violencia. Escribió un libro: La desobediencia civil, que leyó Gandhi, Luther King,...

ACT UP...

...estamos en la misma historia. Nuestra lucha se basa en la no violencia, en tratar de usar los cuerpos físicos que se ponen a parar el movimiento del capital, decir con los cuerpos: ya basta. Nos vamos a sentar aquí sin movernos hasta que venga la policía o los medios, porque estamos protestando.

Una sentada es parte de la historia de la DC y de la DC electrónica, lo que hacemos nosotros, que ahora se llama hacktivismo. El nuestro es el hacktivismo no digitalmente correcto, porque usamos el código más básico que existe en el mundo: HTML. Cualquier hacker te dirá que hay códigos más importantes, más altos y eficientes. Nuestro trabajo no es tecnológicamente eficiente, sino que se trata de ser simbólicamente eficaz.

Ahí una de las suplantaciones más sonadas de los Yes Men. Alguien en algún momento fue y compró el dominio gatt.org. El GATT, como todos sabéis, es el nombre del gran Acuerdo General sobre Aranceles Aduaneros y Comercio que hace tiempo impulsa la OMC (Organización Mundial del Comercio). Los Yes Men subieron una web reamweaverizada de la original, cambiando algunas palabras tontas: «desarrollo sostenible» por empobrecimiento hasta las trancas, «ajustes estructurales» por ajustes de cuentas, y un «futuro prospero» por os vais a cagar chatos. El caso es que la cosa funcionaba y cantidad de gente entraba en www.gatt.org, se daba un garbeo y salía convencida de encontrarse en la página de la mismísima OMC. Los Yes Men lejos de desanimarse, pusieron bien a huevo que la gente pudiera contactar directamente con el director general de su OMC, Mike Moore, y claro la gente le escribía recibiendo amables respuestas personalizadas. Viéndole tan accesible, pron-

Nuestro sistema es que miles y miles de personas vengan, cada máquina representa un cuerpo. Si fuésemos terroristas, usaríamos el sistema que hizo el hacker alemán Mixter el año 2000, Tribal FloodNet, donde no más necesitas una o dos personas que pueden tumbar a Microsoft, Yahoo... Con estos sistemas pueden hacerlo, y creo que este tipo de hacking se puede ver, es eficaz, hace un trabajo bien hecho y rápido. Pero ese tipo de acción entiendo que es ilegal, parte del cibercrimen.

¿Hay una ética hacktivista?

Sí. Debe representar a una comunidad. El terrorismo siempre se hace escondido, no se dan nombres, pocas personas, usan una máscara, no dicen: soy un terrorista y vivo en la calle 8 de Brooklyn, apartamento 4 y mi teléfono es éste. Nosotros somos transparentes porque esto es parte de la historia de la DC. Los medios, la policía, deben saber exactamente quién es la persona que está haciendo esta acción. Hacemos transparentes nuestros cuerpos electrónicos y nuestros cuerpos reales. Esta tradición no es parte de la comunidad hacker. Ellos siempre han sido anónimos, secretos, código alto... Los hackers son como espías del gobierno, escondidos, no salen y dicen «Hola, soy espía». Nosotros no nos escondemos.

Si no son hackers, ¿por qué se llaman hacktivistas y no artivistas?

Los medios, específicamente el New York Times, nos llamó hacktivistas. Al comienzo no me gustaba mucho este nombre porque lo ponía en el círculo del hacker, pero es un signo que tiene un valor que atrae a los medios, y decidí usarlo tácticamente. Nuestro hacktivismo es digitalmente incorrecto, mientras que hay otro digitalmente correcto, como el hacktivismo de Cult of the Dead Cow.

¿El correcto es el constructivo?

Depende de si eres de la China comunista. Pero ellos trabajan en código muy alto, hay muy poca gente que pueda trabajar en estos sistemas, no se si tú o tu mamá pueden ayudarles. No tengo nada contra este hacktivismo, pero es un sistema cerrado, en el que no puede participar todo el mundo. Si quiero cambiar el código, ver cómo trabaja, necesito un alto nivel. El sistema que nosotros usamos es más bajo que script-kiddies, somos lo

to hubo asociaciones de abogados y economistas que decidieron invitarle a dar conferencias en sus convenciones y reuniones. Claro que Mike Moore mismo no podía ir, pero estaría encantado de enviar a Andreas Bilchbauer, una de sus más queridas manos derechas.

Así se inició una serie de visitas del Dr. Bichlbauer como alto representante de la OMC, en cuyas conferencias se dedicaría a exponer los principios profundos de su organización, anunciando campañas contra la siesta, presentando inventos como una especie de polla gigante con pantalla táctil incorporada que permitiría vigilar a los empleados constantemente y enviarles pequeñas descargas eléctricas cuando se les viera perder tiempo, o anunciando finalmente la disolución de la OMC tras reconocer que casi ninguno de sus objetivos se había cumplido y que, menos mal, porque alguno que se había medio logrado no había hecho más que empeorar las cosas.

peor, somos HTML. Dejamos que la comunidad, cualquier persona, una abuelita, ciega, que no puede caminar, pueda hacer clic.

Ustedes crearon una herramienta, el Zapatista FloodNet.

Si, es meramente «refresh». Es código HTML. Muy simple. Así, activistas callejeros que no tienen tiempo de aprender todo el sistema de lenguajes de programación, es un modo de que estos grupos comiencen a usarlo.

Cuando en 1999 dimos el código, comunidades indígenas en Australia lo usaron, activistas gay, los hippies electrónicos en Inglaterra... todos empezaron con nuestras ideas y la Guerra de la Web y todo eso. No tengo nada contra la tecnología eficiente, pero queremos dar a todos el poder de hacer este tipo de acciones sin problemas.

El hacktivismo ha tenido más apoyo de la comunidad de net-art, concretamente arte político, que de la comunidad técnica. Veo el hacktivismo como arte político, como los DoS de hacer dibujo y estar atacando, etc. Y dentro del arte, su discurso de Internet como megaescenario y la simulación me hacen pensar en el postmodernismo. ¿Es el hacktivismo arte político postmoderno?

El hacktivismo creció del zapatismo y el net-art. Lo que lo hace diferente del postmodernismo es que allí la simulación era sobre más simulación, el infinito. Lo que enseñan los zapatistas es que la simulación no es una cosa postmoderna sino más de realismo mágico, en que la simulación se usa para enfocarse sobre la realidad específica: cómo se vive, cómo se existe...

Actuando en el simulacro, ¿actúas en la realidad?

Sí, porque el sistema no es apuntar el simulacro para hacer más simulaciones en términos de Las Vegas. En términos zapatistas esto quiere decir que como nuestras acciones son simulación se reflejan en el mundo real, específicamente lo que está pasando en Chiapas. Cuando usamos la simulación negamos el cinismo y pesimismo postmodernista.

¿El simulacro sería la Netstrike?

Sí.

Las primeras charlas de Andreas fueron planeadas y desarrolladas por los Yes Men tal cual, ya hacia la tercera el grupo había comprendido la necesidad de contar con aliados en cada terreno y se empezó a contar con los grupos antiglobalización locales para liarla juntos.

Con ello se cumplía un paso más en lo que nos parecería un esquema ideal de trabajo de ciberguerrilla: se trabaja desde la red, se consiguen efectos en el exterior y, además, estos efectos se articulan políticamente con organizaciones y grupos autónomos capaces de amplificar la cosa y mantenerla rodando. No es poca cosa.

De hecho, apenas estuvo la OMC disuelta, Ramonet y Paco recibieron un encargo de una organización ecologista para liar a la Dow Chemical. ¿Recordáis? Fue la responsable de un megaaccidente en Bhopal, en la India, que impunemente ocasionó la muerte de miles y miles de personas y unos

¿Le puedo presentar como padre del hacktivismo y hijo del ciberpunk?

Sí. El ciberpunk comenzó con Gibson, que escribió Neuromancer en una máquina de escribir; esto es algo muy importante: el ciberpunk no viene de la máquina o del código, sino del sistema metafórico que es el poder de lo estético, un modo de pensar que a veces debe pelear contra modos de pensar científicos o políticos, que ya tienen sus espacios donde su epistemología está legítimamente presentada en espacios de poder y económicos muy grandes.

El espacio estético no tiene un campo tan grande y poderoso, pero sí puede pensar más rápido, de otro modo, que a lo mejor no necesita el esfuerzo científico y económico ni respaldo de la política o lo militar. Lo estético puede cruzar las barreras de la realidad más simplemente, más rápidamente y al mismo tiempo con más emoción. Por eso es muy importante el sistema de net-art, porque eso nos da la habilidad de pensar en el museo, la galería, con la comunidad artística, un espacio de pensamiento que para mí es también legítimo y algo que los zapatistas nos han dado: un modo de pensar, una política estética. Y no son los primeros. En los comienzos de la histeria sobre la SIDA teníamos en los ochenta a gente haciendo diseño de camisetas, de pósters. Ahora muchos de estos sistemas se usan en la música y otros. Esto era algo muy importante: la estética del movimiento, cómo se ve, cómo se refleja.

Usted dice: no somos terroristas, no somos violentos, pero en cambio hablan de la netwar. ¿Ustedes están haciendo la guerra, política, la revolución o qué? ¿Existe realmente esta netwar? ¿Quién la está ganando?

La Netwar o guerra de información comenzó con un think tank, la Rand Corporation, de los militares, en los cincuenta. Ellos, en el 91 dijeron que esta guerra cibernética iba a comenzar y se iba a ganar por los estados del norte, que tenían los instrumentos físicos y el poder sintáctico, las gentes que podían controlar el software, el código, para esta guerra informática. Si uno sigue las ideas de ciberguerra de la Rand, se puede decir que los EEUU han ganado la guerra informática, tienen todo el poder y el sistema electrónico.

destrozos que ni te cuento. Bueno, con ayuda de información procedente de la organización ecologista, de su Departamento de Prensa y con la mala baba de los Yes Men se compraron algunos dominios, como Dowethics.com y Bhopal.com, donde se fueron exponiendo algunas cosillas.
Dowethics.com se presentaba como una página de la Dow Chemical dedicada a la clarificación de la conducta ética de la empresa, aclarando que dicha ética sólo se le podía exigir a la empresa frente a sus accionistas, haciéndoles ganar dinero. Dowethics manifestaba así que no sentía ningún remordimiento por las víctimas causadas en Bhopal, dado que lo ocurrido había sido un efecto colateral de la gran misión ética de Dow respecto a sus accionistas: seguir haciéndoles ganar pasta.

Si bien con los sabotajes a la página de Bush y de la OMC se había montado un pollo considerable, en ninguna de estas ocasiones se llegó al extremo al que llevó el ataque a Dow, lo que quizá

Pero hay un elemento: lo semántico, que es parte del uso del lenguaje, del poema, que puede crear otro modo, no de guerra sino de paz o disturbio informático. Ellos no lo comprenden directamente ni es un espacio importante para ellos, porque no se trata de un poder basado en la situación económica o militar sino de un espacio difícil de ensamblar, como el Libro de los espejos que escribió Don Durito, la tecnología maya o las historias del viejo Antonio. Estas historias no son código secreto, son parte de un sistema que ha crecido por miles de años de modo que el corazón de la comunidad puede cantar y darse un valor fuera de la violencia militar y económica.

Uno puede decir directamente que la guerra informática ya está ganada por el poder, por el imperio y los terroristas, pero los zapatistas dicen que esa guerra entre el imperio y los terroristas es la tercera guerra mundial, mientras que los zapatistas ya han peleado la cuarta guerra mundial y la han ganado. O sea, que nos están esperando en el siglo XXVII.

Y al mismo tiempo, en el 2000, comunidades hackers como 2600 o Defcon han invitado al EDT, y la guerra que empezó entre nosotros de palabras, en el 98, ha cambiado mucho.

Ahora muchas comunidades nos han abierto la puerta para empezar a hablar sobre desobediencia civil electrónica y sobre que los hackers no deben sólo pelear por los derechos de la información, sino también por estos derechos en la calle.

Cuando estuvimos en la conferencia de 2600, esa comunidad marchó con nosotros en Filadelfia contra los republicanos, y la policía vino y agarró a los hackers. Se han comenzado a abrir las puertas. Lo importante del hacktivismo es que abrimos la puerta a los activistas callejeros para que empicen a usar sistemas técnicos, y a los hackers la posibilidad de trabajar y pensar en una vida fuera del código. A los militares, les damos un espacio que no pueden comprender. Y a la comunidad estética le abrimos un espacio poético social. Agit-pop.

¿Ha habido entonces un acercamiento? ¿En Europa también?

Eso está siendo más duro. Los hackers aún no quieren hablar mucho, por eso estuve contento que en mi plática en el CCCB hubo hackers de Barcelona que quisieron

revele quién manda en América. La multinacional exigió a Verio.com, proveedor de dominios y de acceso a Internet, no sólo que cerrara las páginas atacantes sino que cerrara el servidor mismo, thing.net, en el que estas páginas estaban alojadas y en el que, por cierto, había otros varios miles de páginas. Así sucedió y thing.net estuvo cerrado un buen tiempo a causa del ataque. Con ello se cerraba el bucle y el ataque que, salido de la red, había provocado abundantes efectos fuera y se había articulado políticamente con agentes externos, era repelido en la red misma, en el servidor y debía ser retomado, como así se hizo, multiplicando los servidores que albergaban copias de las páginas perseguidas... y extendiendo así, como decía el Padlecito, el modelo de la ciberlucha esta hasta los más insospechados rincones.

hablar conmigo. Sí hubo ocasión en el año 2000, cuando un grupo me invitó a ir a Alemania a hacer acciones contra Lufthansa y el uso del gobierno alemán de mover inmigrantes amarrados en los aviones, hubo muertos por eso. Lo importante fue que se unió a nosotros un grupo de chicos que eran parte del Chaos Computer Club alemán, que nunca quería sentarse en una mesa conmigo. Así que sí he visto espacios donde comienzan a hablar, sobre todo las comunidades más jóvenes que los hackers que están ahorita, que empiezan a ver que hay una sociedad política fuera de las computadores que necesita su valor y respaldo. Empiezan a abrirse las puertas un poco.

La idea de la Netstrike nació en Italia, como los hackmeetings. ¿Qué tiene Italia?

Lo interesante es que respondieron muy rápido a los zapatistas y allí creció muy rápido en el 94. Se me hace que ese tipo de zapatismo digital fue muy importante en Italia para abrir un espacio social, político y estético.

La comunidad italiana entendió muy rápido de qué hablaban los zapatistas y la red intergaláctica. Hay una situación histórica en Italia con ciertos modos de pensar, desde 1900, la izquierda y también los futuristas.

Estas políticas de comunidad y diferente modo de economía han hecho que Italia se moviera muy rápidamente, el primer netstrike contra las armas nucleares, a favor de los zapatistas. Italia ha sido el centro de una convergencia de elementos muy importantes.

¿Sigue habiendo relación con Italia?

Constantemente. Trabajo como director del Thing Tank y tenemos una thing en Italia y conozco a Jaromil, Candida Televisión, he estado en Italia muchas veces.

La familia...

Sí, muy íntimo. Y muchos de ellos vienen a casa en Brooklyn y están conmigo.

Usted dice que el objetivo es parar el capitalismo virtual con un gran simulacro. ¿Puede explicarlo?

El gran simulacro es lo que dice Don Durito, una huelga a través de los arcos de la realidad. En el segundo encuentro intergaláctico Don Durito dijo que tenÍamos que

Para más información: The Yes Men (2004) *The True Story of the End of the World Trade Organization*, disinformation, Nueva York.

Nota

1. Lo táctico es la opción de aquellos que, careciendo de un terreno propio donde acumular recursos, se la juegan siempre en terreno enemigo, teniendo que improvisar y trabajar con los elementos mismos que definen el poder del enemigo: cuanto más poderoso sea éste, razón de más para optar por un trabajo táctico. ¿Sugerente? Buscad cosas de Michel de Certeau, hay una edición en castellano de textos suyos y jugosos comentarios escritos por una panda de amiguetes cuyo libro deberíais comprar, o mangar en el AFANAC: *Modos de hacer (Arte político, Esfera Pública y Acción Directa)*, publicado por la Universidad de Salamanca en enero de 2001.

hacer esta huelga, que se va a hacer de un simulacro basado en la realidad de cada uno. El capitalismo virtual no tiene pensamiento, emoción, sobre la carne física. Es completamente inmaterial. Enron, WorldCom... Sí que hay hombres que cogen todo el dinero, pero éste trabaja tan instantáneamente que es planetario, flota fuera de nosotros. El simulacro que hablamos es el del sueño, el que sale de cada uno, de mi sangre, de mi piel, mis ojos, no del código, por eso es poético, que viene de la sociedad, la comunidad. Cuando nuestro simulacro se hace masivo, más material que inmaterial, pone un choque contra el sistema virtual. Puedes verlo en la guerra de los juguetes: el espíritu poético, de la huelga que cruza las realidades, puede parar la flecha económica de hiperrapidez. Es el simulacro de tú y yo, más material que el espíritu. No tengo espíritu, soy espíritu. No tengo un simulacro, soy simulacro. El capitalismo virtual es también una simulación, la más rápida, se come todo, pero en un espacio muy abstracto.

Sobre el zapatismo: ¿cómo unos campesinos se convierten en protagonistas de Internet? ¿Dices que tomaron una central eléctrica y vieron la luz, pero cómo lo explico?

Ellos bajaron con una visión antigua, la tradición marxista-leninista, la tragedia. Pero cuando bajaron, por accidente, completamente sin plan, en un minuto cruzaron la red electrónica, pero en lugar de decir qué diablos es esto, no es parte de nuestro movimiento, vieron que el movimiento era eso, romper el sistema electrónico y no con armas ni bombas ni guerra sino con la palabra. Y lo entendieron en unos 5 o 10 días. Puedes ir a las compañías más grandes del mundo y decirles: ¿qué rápido puedes cambiar tú? Ellos entendieron todo en unos días, que ya no eran revolucionarios tradicionales, que la red era semántica..

Pero, ¿cómo vieron esta red?, ¿cómo tuvieron acceso? ¿Pasaron por delante de un cibercafé?

No, no, no. Lo que pasó fue muy fácil: el subcomandante escribió en un papel, con lápiz, la primera declaración de Lacondona; alguien dijo: ¿puedo hacer una copia? Fue a la iglesia donde estaba el obispo y él tenía teléfono, computadora...

VOTOS AL MEJOR POSTOR

En una democracia como la norteamericana (la nuestra no, por dios), donde las grandes corporaciones y lobbies tienen tanto poder y ascendencia sobre los políticos, es de todos sabido (www.opensecrets.org) la facilidad con que las grandes (y malas) compañías compran a los políticos, vía donaciones para sus gastos de campaña, con la fundada esperanza de que luego, cuando alcancen el poder, les devuelvan los favores, como ahora mismo está haciendo Bush con el botín de Irak.

Claro que esto tiene el ligero inconveniente de que en ese proceso de yotecomproytumedevuelveselfavor, unos y otros suelen olvidarse de los ciudadanos, en quienes, al fin y al cabo, reside la soberanía. Eso está muy mal. También podría suceder que el político saliera populista y, una vez en

Allí escribieron esa nota y lo hablaron a La Jornada, que lo mandó a la red. Eso pasó en unos 45 minutos. En ese momento vieron los zapatistas el proceso.

O sea, los campesinos supieron cambiar. Y ahora, tienen electricidad, tienen ADSL, ¿tienen portátiles?

No

¿Quieren que se los mandemos?

Se está haciendo, despacito. Pero hay una diferencia: el Ejército Zapatista de Liberación Nacional no necesita nada, no necesitan ayuda, ni dinero ni armas ni nada electrónico. Las comunidades autónomas, como Aguascalientes, sí necesitan ayuda: comida, medicinas, electricidad, computadoras, escuelas... Estas comunidades no tienen nada, mientras que el 42% de la electricidad de México viene de Chiapas, pero menos del 1% de esta electricidad va a Chiapas. Los indígenas no tienen nada. Pero los zapatistas tienen allí computadoras, hacen películas que se enseñan en el MOMA, el CCCB... Chiapas Media Project, Chiapas Indymedia... son gente indígena, humildes, pobres, pero no tontos. Aprenden muy rápido. Así que el esfuerzo de las comunidades zapatistas es ayudar a esas comunidades autónomas. Pero el ejército EZLN no necesita nada.

Pero un grupo guerrillero se mueve continuamente e Internet tiene cosas, como los servidores, que no pueden moverse así como así.

Esos computadores son de las comunidades, de las escuelas, de la gente que está trabajando las tierras, de las «abejas», las mujeres que tejen... Allí están los servidores, los sistemas, que usan para vender café, telas... Es cuestión de crear una economía autónoma, fuera de la economía que les quiere imponer el neoliberalismo, como trabajar para MacDonalds, etc. Y cada vez que viene el ejército no ataca al Ejército Zapatista sino a estas comunidades que están tratando de hacer un desarrollo económico sostenible decidido por esas comunidades. Están haciendo más dinero vendiendo su café directamente a diversos sitios que las comunidades que trabajan para el gobierno. Así que las computadoras existen allí, pero son de las comunidades.

el poder, se olvidara de sus financiadores y no les guarda la debida gratitud. Muy mal también y muy poco racional. Si bien está claro que las corporaciones tienen todo el derecho del mundo a invertir su dinero de modo que preparen el terreno para sus negocios, semejante inversión debería poder hacerse con garantías y, por supuesto, no debería lesionar la relevancia que a los ciudadanos otorga el ser depositarios de la soberanía nacional esa.

¿Qué hacer? A eso ha dado respuesta James Baumgartner, uno de los diseñadores de Vote-auction.com (subasta de votos.com) en cuya web, como en cualquier otra página de subastas, se admiten ofertas y demandas que deben pujar.

¿Qué se consigue con ello? El votante recibe dinero por su voto y vota al candidato que su comprador le indica. Con ello la corporación se asegura de la efectividad de su inversión y, aunque el sis-

Y, desde el 94, ¿qué se ha aprendido del uso político de la red?

Lo básico es que la red para la comunidad en resistencia es tres cosas: comunicación, el correo electrónico, que es la base de todo, un 95%, eso es lo que entendieron los zapatistas inmediatamente y no tantas lecturas de Marx, etc. Número 2: documentación, retratos, qué pasó, cuándo pasó, a quién mataron, cómo está la investigación; he trabajado con las mamás en Juárez de hijas desaparecidas, hemos hecho acciones y uno de sus problemas es que no tienen modo de documentar lo que está pasando, así que les estamos mandando cámaras digitales, computadoras... porque es importante documentarlo todo. Ahora, nosotros hemos dado otra posibilidad que a lo mejor en el 5% se necesita, no siempre es lo mejor, una solución, que es la DCE, que las mamás en Juárez lo pueden hacer. Así, cuando ellas crean que en una situación se necesita, pueden llamar para una acción. Pero es una táctica, no una estrategia. Una táctica que un grupo debe decidir si es buena o mala para su situación pero que debe tener la habilidad de hacerlo.

¿Pero hacer caer un servidor realmente sirve para algo? ¿Crees que nos están escuchando cuando enviamos miles de cartas de protesta o hacemos una netstrike?, ¿realmente sirve de algo?

No hace mucho hicimos una acción contra la Corte de México y se cayó por 22 horas. A ellos no les sirve para nada, pero para nosotros es lo mismo que hacer una marcha en la calle. Es visible porque toda esta gente, 48.000 personas, se unieron a hacer esta acción, desde Corea del Sur, Perú... No importa que se caiga o no se caiga, lo que importa es que alguien en Tahiri está leyendo una nota de qué está pasando con los zapatistas y puede enviar su respaldo. Es comunicarnos entre nosotros.

Porque... no nos escuchan, ¿verdad?

Cuando salimos en los medios dominantes es un modo de hacer que por un momento expliquen lo que pasa, ya es un pedacito y a lo mejor alguien leyendo es la primera vez que ve la palabra zapatista. Pero es 98% información para una comunidad que quiere hacer algo: una mujer ciega que no puede ir a las acciones a Génova o

tema siga igual de corrupto, el ciudadano se convierte en beneficiario directo de esa corrupción, y eso siempre consuela.

Ya que las corporaciones van a gastarse dinero comprando la soberanía nacional, por lo menos que se ahorren los intermediarios y la compren directamente de sus dueños: los honrados ciudadanos.

¿Una broma? Pues no les pareció así a los jueces de Nueva York, Michigan, Illinois y California, que se pusieron de acuerdo para forzar el cierre de la página y amenazar a cualquier usuario que se sintiera inclinado a vender su voto con tres años de prisión. La página fue cerrada en EEUU y vuelta a abrir en Austria, unas semanas más tarde. De voteauction.com había pasado a vote-auction.com que también fue cerrada. Desde entonces han existido vote-auction.net y voteauction.biz. Todas han sido clausuradas.

Quizá habría que probar con tecnología p2p... y a ver qué pasa.

Seattle, o un papá con niños, o alguien que no puede caminar, pero está con nosotros. La DCE le da una habilidad de mandar una carta de protesta sintiendo que también puede hacer desfile en estas comunidades. Así que la información es para nosotros.

¿Las netstrikes que han hecho siempre han sido zapatistas?

En el 98, sí. En el 99 ayudamos a otros grupos a aprender cómo hacerlo, apoyando sus acciones contra la OMC, el G-8... Pero el 95% de las acciones que hemos hecho han sido zapatistas.

Hablemos de los hackers otra vez. Usted ha dicho que «ellos creen que la banda ancha es más importante que los derechos humanos». Yo pienso que la banda ancha es como la tierra que pisamos, ¿es entonces más importante defender la tierra que los hombres o al revés... ¿cómo?

Ésta ha sido la gran diferencia entre hackers y hacktivistas. Creo que promover la información debe ser libre y todo esto es correcto y muy bien. Pero debe haber momentos en que la gente pueda marchar en el superhighway. Hay tiempos en que la gente siente que quiere hacer desfile, sentarse... si no, no te van a ver. Así que tácticamente hay espacios donde se necesita marchar en los sistemas digitales. No digo que tenga que ser por siempre ni que quiera que todo el sistema se caiga. Sólo decimos que tácticamente a veces es bueno que hagamos esto, por unas horas.

¿Pero esto no legitima también al grupo de extrema derecha que ataca un sitio de izquierdas?

Sí. La idea de desobediencia civil es políticamente neutral.

Pero si el sitio que se ataca está en un servidor con otros sitios, reciben también los otros sitios y servicios, sin culpa...

Pero también eso pasa cuando se hacen acciones en la calle. Puede haber una ambulancia mientras se hace una marcha y no puede pasar o deberá dar un rodeo. Aunque tu estás intentando defender en abstracto a esta mujer, en real necesita tu ayuda, pero no puedes hacer nada. Pero mira, el servidor de Thing tiene diferentes sitios y nos han atacado y han querido cerrarnos, pero cuando pasa esto, limpiamos y empezamos otra vez.

Para mí es mejor que tumben un servidor a que te den un balazo. Estaría bien si las guerras se hiciesen así; en vez de atacar a Irak, un videojuego.

¿Qué opina sobre el webdefacement?

Es cracktivismo. Y creo que hay ocasiones donde ha trabajado muy bien. En septiembre 11 del 2000 estuve en Melbourne y alguien secuestró el dominio de la OMC. En el 98, un hacker tumbó sitios de bombas nucleares. Eso se me hace bien.

¿O sea, está de acuerdo con el cracktivismo?

Sí, pero no con el que pasa algo y no sabes por qué. Debe haber una razón. Si se hace con estilo y con una política clara de las razones que se hace, como los que en Davos entraron en el servidor y tomaron la información de Clinton, Bill Gates y todos, y no lo usan contra ellos sino que lo ponen en un CD y se lo mandan al periódico.

¿Tienen contacto con otras naciones oprimidas, como Palestina o Chechenia?

No directamente. Siempre he tenido notas de hacktivistas rusos de los dos lados y les ayudo a los dos, es mejor que hagan sentadas virtuales el uno contra el otro que que se maten. También ha habido ocasiones en que comunidades israelitas y palestinas me hablan al mismo tiempo. Así que los pongo en contacto y creo que así, por unos minutos, hay un espacio en que ambos están hablando y a lo mejor se conocen un poquito más.

¿Y tirar satélites, en vez de tirar servidores?

Eso es algo más alejado del HTML :) En la guerra informática de los EEUU y los terroristas a lo mejor es algo que hacen ellos.

¿No están cansados ya de la Netstrike? ¿No hay nuevas ideas?

Sí, pero como dicen los zapatistas una idea, aunque tenga ya tres años, debe durar mucho tiempo para crecer, reformarse... Pero mira: un proyecto que pasó por accidente, en el 99 mucha gente nos decía del futuro del hacktivismo y acabamos diciéndoles: los zapatistas tienen satélites, tienen cámaras de vigilancia que están usando contra los paramilitares y los militares mexicanos. Y esas imágenes van directas a las comunidades de derechos humanos, ONGs, comunidades zapatistas... Así que llamamos a estas las hermanitas, que están viendo, dando el ojo al hermano grande, y cualquier cosa que el gobierno mexicano hace, no importa dónde están en la jungla, nosotros estamos viéndolos. Y comenzó en Time Magazine: los zapatistas tienen satélites. Un mes después, en un periódico de militares mexicanos decían lo mismo. Bien, pues finalmente ése es un proyecto en el que estamos trabajando y diversos grupos han querido ayudar a él.

¿Pero no era una broma?

Empezó semánticamente, pero sabemos que el gobierno comenzó a creerlo y ahora hay fundaciones que han venido a preguntarnos si nos pueden ayudar a hacerlo y lo estamos pensando. Esta idea de espiar a los espías viene de los Black Panther, que usaban cámaras para seguir a los policías en las comunidades negras y tomarlos cuando vendían droga o pegaban a alguien.

Ustedes dicen que los hackers no los van a ayudar y, a la vez, que ustedes vienen a ayudar a los hackers a romper el capitalismo virtual. ¿Cómo se entiende?

Eso lo decíamos en el 89, cuando escribimos The Electronic Disturbance, que ni hackers ni políticos nos ayudarían. Pero, al mismo tiempo, queríamos ser las Panteras Modernas, que crearían unas realidades que iban a empezar a cambiar las ideas de estos grupos. Esto está sucediendo, estamos tratando que comiencen a ver que sí se pueden usar esas cosas.

Esto es táctico: cuando estoy con los militares me preguntan qué estoy haciendo y les digo que teatro. Cuando estoy con los hackers, les digo que estoy haciendo zapatismo. Cuando estoy con los activistas callejeros y dicen qué es esto, hacking. Cada posición tiene su simulación que hace que este grupo responda de forma diferente a lo que creían que estaba pasando. Así, las panteras modernas hacen una huelga a través de los arcos de la realidad, haciendo miles de realidades, porque cada grupo necesita una diferente realidad para entrar a la realidad. El mero centro de la comunidad zapatista se llama La Realidad.

En este entramado, ¿los políticos son los enemigos?

Lo pueden ser si siempre tratan de resolver la situación de la comunidad en términos del siglo XX, porque lo que pasó con los siglos XIX y XX era la política de la respuesta, totalmente hecha en la cabeza. Los comunistas podían ir a Das Kapital, los capitalistas a Smith... y todo estaba hecho. Bush y Bin Laden son dos tipos de cilógicos fundamentales porque ellos creen que hay un apocalipsis que va a venir. Creen en ideas viejas. Hay un montón de abstractos que han creado el mundo y lo único que nosotros vemos es que han matado. El zapatismo es un tipo de política que no tiene respuesta sino cuestión.

¿Y cuál es la cuestión de usted?

Para mi siempre ha sido: ¿tiene la comunidad de cuatro millones de indígenas en México derechos? Salinas en el 85 para firmar con Wall Street tuvo que dar los derechos de las tierras de estos grupos. Y Salinas quitó el artículo 27, que viene de la Revolución Mexicana donde pelearon Zapata, Pancho Villa..., que decía que las tierras eran de las comunidades indígenas, que tenían derecho a votar, a la educación, etc.

Es como hacíamos en ACT UP. Nosotros no hacíamos la revolución porque ya sabes que ahora la revolución es de IBM. Así que poníamos una cuestión: ¿hay algún modo de curar el SIDA? Y ésta es la primera vez que una comunidad viviendo con una enfermedad dice: nosotros también sabemos y queremos estar en las mesas de discusión e investigación.

El zapatismo viene de esta misma comunidad de la cuestión. Ahora los zapatistas autónomos se preguntan: ¿cómo hacemos una economía global pero que se respete la economía local?

¿Podemos decir que existe ya la red de resistencia intergaláctica, formada por pequeñas células como EDT?

Sí, bajo muchos diferentes nombres: hackmeetings, meetings de medios tácticos, Indymedia, opensource... Hay un montón de comunidades que trabajan en diferentes proyectos pero siempre con una política de la cuestión.

¿Y todas van contra el capitalismo virtual?

Sí.

¿Van a crecer más?

Siempre podemos querer más.

¿Pero qué dice la mágica palabra?

Que ya ganamos. Uno de los libros de Don Durito explica que el subcomandante Marcos estaba muy triste una noche porque le llegó la noticia de que lo habían matado, porque siempre lo anda matando el gobierno. Y Don Durito dice: «Oye, nariz grande, ¿qué diablos estás haciendo, por qué estas llorando? Porque me han matado. ¿Y qué diablos importa que te maten o no? Ya la guerra está ganada. ¿Cómo puedes decir eso? ¿Estamos aquí en una jungla y el poder y...? Mira, yo he estudiado el neoliberalismo y estas notas yo las escribí en el siglo XXVII. Y ya sé que para ustedes los pobres del mundo todo se va a pasar muy duro, van a perder batallas y van a perder vidas, pero la guerra ya se ganó. Así que no estés tan triste.»

Y, por último, ¿qué pinta en todo esto su interés por la nanotecnología?

Es la gran posición de la siguiente política de la cuestión, de resistencia, porque en 1986 un científico escribió The engines of creation y dijo: ahora tenemos la posibilidad de mover los átomos, no de choque pero industrialmente. H_2O es agua, así que vamos a hacer unos martillos del tamaño de átomos para unirlos. Tú dices: yo quiero agua. Y te la hace. O una manzana: y te hace una. O el pelo más rojo esta mañana. Eso es lo maravilloso de la nanotecnología. Todo el capitalismo virtual se basa en tener un límite del material, por eso las peleas por el agua, porque hay un límite. Con nanotecnología no hay límite del material, es infinito. Por tanto, es una ciencia que está contra el mercado, el mercado del límite. El lado malo: quién tiene el control, qué compañías harán estos sistemas... Otra vez el poder que sólo dará agua infinita al presidente Bush pero no a la gente humilde. Ése es un problema. Por tanto es necesario que las comunidades de resistencia comiencen a estudiar cómo trabajan estos sistemas para dárselos no a Bush ni a Bin Laden, sino a las comunidades que de verdad lo necesitan.

Estas máquinas las están haciendo, no es ciencia ficción. Son empresas muy fuertes y creo que para mí es muy importante, también para los activistas, tratar de hacer resistencia sobre el capitalismo virtual, pero también intentar pensar... Otro nivel es la genética. La nanotecnología apenas comienza y siempre digo que las comunidades de resistencia siempre llegamos diez años tarde y es mejor comenzar a investigar estos temas antes, cuando es una tecnología que está empezando. Y un modo de hacerlo es como los hackers, entrar en los sistemas, como un trabajador, como hice para entrar en los ordenadores. Yo no tenía y para conocerlo entré en una compañía a hacer diseño. Conocer qué es esto y cómo trabaja. El next performance que me gustaría sería trabajar en una de esas compañías de nanotecnología, para ver lo que están haciendo de verdad, qué es el martillito, qué es lo que están usando, cómo se ve la máquina...

Enlaces relacionados:

2600, the Hacker quartely: www.2600.com
Critical Art Ensemble: www.critical-art.net.
Cult of the Dead Cow: www.cultdeadcow.com.
DefCoN: www.defcon.org.
Electro Hippies: www.fraw.org.uk/ehippies/index.shtml.
ETOY: www.etoy.com.
EZLN: www.ezln.org.
Hackmeeting: www.hackmeeting.org.
IndyMedia: www.indymedia.org.
Open Source: www.opensource.org.

AGUJEROS NEGROS EN LA RED

Marga Padilla*

Para no quedar aislados en un gueto o reducidos a mera opinión pública, los movimientos sociales luchan por visibilizar los conflictos. «Debemos hacernos visibles», parece ser la consigna. Sin embargo, esta lucha por la visibilidad está asumiendo su propia condición paradójica pues, una vez abandonada la polaridad luz/oscuridad, cada vez está más claro que para dejarse ver hay que ocultarse.

Como podemos leer en la «Primera proclama incendiaria...» del colectivo «Los invisibles» de Madrid, repartida en una manifestación en defensa del centro social okupado El Laboratorio: «Cubrimos nuestros cuerpos con monos blancos para salir de la invisibilidad, partiendo de una metáfora contradictoria: queremos ser tod@s invisibles para hacernos ver. [...] Cubrimos nuestros cuerpos con monos blancos porque creemos que en este momento se hace necesario recuperar la palabra y el espacio que la represión y la criminalización nos arrebatan...». Recuperar la palabra y el espacio... Pero, ¿cómo es ese espacio en el que debemos movernos entre metáforas contradictorias? ¿Qué es lo que se muestra y qué lo que se oculta? ¿Quién nos va a iluminar y qué imagen será reflejada?

REDES SOCIALES - SOCIEDAD EN RED

Hasta hace bien poco, la organización en redes estaba asociada a prácticas críticas, antiautoritarias, disidentes o antagonistas, una vez que la organización en torno a coordinadoras y otras estructuras aún más pesadas empezó a mostrarse como excesivamente rígida.

La participación en redes, al ser optativa, provisional, no vinculante y no totalizante, parecía ser la forma adecuada para la cooperación sin mando.

Pero la revolución de las tecnologías del procesamiento de la información y de la comunicación han expandido las posibilidades de construir redes, cada vez más extensas, cada vez más globales, cada vez más integradas, cada vez más difusas... y cada vez más ambivalentes.

De todas ellas, sin duda la más fascinante es Internet, una red de redes con nombre propio que ofrece enormes posibilidades de experimentación y mucha ambigüedad pues, junto al protagonismo que sentimos al saber que estamos construyendo algo que sin nuestra presencia sería de otra manera (sensación difícil de experimentar en otros ámbitos más materiales), crece también la sospecha de que esa red, como todas las demás, pueda servir para cazar(nos), y que la presa sea el propio vivir.

De esta sospecha surge la cautela con la que toda posible presa se mueve en pos del mejor camuflaje. Pero el camuflaje no es suficiente cuando lo que se quiere es «salir de la invisibilidad».

Visibilizar la privacidad para preservar la vida

Cuando la realidad es sufrida como una relación de fuerzas muy desfavorable, la red se percibe principalmente como un mecanismo de intensificación y adaptación de las relaciones de poder y, por tanto, como una amenaza para el yo.

Entonces, esos yoes que ven la red como un instrumento del poder para colonizar un espacio interior que llega hasta la alcoba sienten miedo: miedo a ser vistos (controlados) y también a dejar de ser vistos (excluidos). Sabedores de que para ser alguien no queda otro remedio que conectarse en red, defenderán la conectividad, sí, pero con un punto ciego que preserve la privacidad, y exigirán a cambio al Estado algo que éste, siendo un Estado de derecho, no podría negar: el derecho a vivir una vida privada, aunque conectada, es decir, conectividad a cambio de privacidad. Pero esta privacidad habrá que conquistarla.

Mientras la privacidad se defiende como un derecho universal y, por tanto, formal, desde el espacio disgregado de la ciudadanía, la defensa de este derecho se puede mantener de forma consistente. Sin embargo, cuando esos yoes privados se combinan entre sí en un espacio más agregado, una nueva relación de fuerzas deberá ser trazada al decidir cuánta parte hay de público y cuánta de privado en cada información, en cada vida y, sobre todo, al decidir quién decide esto.

Los nombres de los médicos que practican abortos o que se niegan a hacerlo, los nombres de los policías o funcionarios de prisiones denunciados por torturas... ¿Vida pública o vida privada? ¿Quién lo decide?

O un caso aún más problemático, puesto que el colectivo debe decidir sobre sí mismo: alguien cercano al proyecto sinDominio hizo pública información que pertenecía al espacio privado de la asamblea telemática de este proyecto con el objetivo de desprestigiarlo —lo que se conoce como «el asunto de las suplantacio-

nes»— y parte de la asamblea consideró que para defenderse de esta agresión había que dar «más visibilidad», es decir, hacer la asamblea totalmente pública. La solución técnica para conseguir esta visibilidad hubiera sido publicar en la web los contenidos completos de la lista de correo en la que la asamblea de sinDominio se organiza.

Cuando la vida se vive como vida privada, ello da lugar a un espacio disgregado de derechos formales en el que las formas de vida intentan preservarse pasando desapercibidas. Pero cuando ese espacio disgregado remite y ocurre una mayor agregación, la privacidad ya no parece la mejor manera de dejarse ver, pues exponerse empieza a ser más necesario que preservarse.

Visibilizar el proyecto para soportar la vida

Cuando la realidad muestra toda su carga de violencia y de muerte, y cuando sabemos que esa realidad se resiste a ser cambiada y que, por tanto, no hay alternativa, la red puede ser vivida como un espacio comunicativo adecuado para una comunidad de proyectos.

En la medida en que en la red, en tanto que espacio virtual, el conocimiento vale más que el dinero, y en la medida en que el conocimiento puede ser accedido por todos y cualquiera, se vislumbra una posibilidad no utópica para abandonar esta nave que se hunde y embarcarse en una bella aventura. Esa posibilidad consiste en virtualizar la vida y en dejar que el mundo material se reduzca a mero residuo.

Pero esa realidad que se resiste a ser cambiada, al ver que el conocimiento puede mirar hacia otro lado y seguir sus propios derroteros, hará todo lo posible por recuperar las energías de esos grupos de amigos que han iniciado un proyecto propio, y desplegará una gran capacidad de seducción tecnológica para reconducir y reconducir sigilosamente hacia el mercado aquellos conocimientos que creían ser libres.

Esto no se hará con imposiciones autoritarias ni normativas (o sí), sino más bien a base de una continua creación de interfaces que faciliten más el acceso a los servicios portadores de valor económico.

Las comunidades, ante estos intentos de mercantilizar la red, harán más activos y más fuertes sus proyectos en busca de más y más amigos, bajo la consigna de «seamos nosotros quienes construyamos la red». Al fin y al cabo, construir la red es cuestión de cooperación y de conocimiento, y eso está inscrito en nuestros cuerpos, de manera que no se nos puede arrebatar, excepto con la muerte. ¡Creemos más y mejores interfaces! ¡Tomemos la iniciativa! ¡Intensifiquemos nuestra presencia!

Y, sin embargo, a pesar de la belleza de esta propuesta, y del bienestar que se siente al vivir en comunidad (virtual), ninguna comunidad lo es lo bastante como para acallar la soledad que desde dentro no para de rugir, y ningún proyecto lo es lo bastante como para conjurar definitivamente el asco, la rabia, el malestar y las ganas de sabotear esta realidad de la que somos parte. Visibilizar la transgresión para intensificar la vida.

Cuando la realidad es vivida como una condena a no experimentar nunca la libertad, atrapados en una sociedad de control en la que cualquier posibilidad de permanentizar la liberación es impensable, buscamos espacios y tiempos que pasen inadvertidos para protagonizar una destrucción creativa que intensifique la vida.

Persiguiendo eliminar las mediaciones y experimentar desde la inmediatez, la propuesta ya no será construir la red, sino parasitarla a la manera de virus.

Esa vida que quiere gastarse en vivir se pondrá a favor del caos e intentará sacar ventaja de las perturbaciones y de las caídas, construyendo la red secreta, la antirred de la guerrilla que golpea y corre. Practicará la piratería del software, el cracking, el phone-phreaking, las intrusiones, la difusión de rumores falsos, la piratería de datos, las transmisiones no autorizadas, el libre flujo de la información, las transferencias de dinero ajeno, el contrabando, las conexiones clandestinas, el chateo...

Sabiendo que la mayor fuerza reside en la invisibilidad, construirá una minisociedad underground al margen de la ley, una subred de transgresiones que mostrará la arbitrariedad de los límites, y que la red oficial nunca conseguirá clausurar.

Estas transgresiones serán perseguidas con saña por el sistema policial y judicial, y castigadas con penas de cárcel y con la salvaje y arbitraria prohibición de utilizar las tecnologías comunicativas (teléfono, ordenador, cajero automático, etcétera).

Tal represión en algunos casos dará lugar a campañas de solidaridad, de resistencia, de desobediencia, y por la libertad y, por supuesto, a intensos momentos de amistad. Pero el ataque de los aparatos represivos sobre una subred muy fragmentada y, en cierto modo, ingenua, difícilmente puede ser respondido desde la propia subred, pues el underground no es espacio para comunidades fuertes y, a falta de mejores defensas, de nuevo habrá que defender los derechos formales: derecho a la presunción de inocencia, defensa, asociación, privacidad, conectividad y libre información.

La red jerárquica

Estas tres maneras de vivir en la red y de las que toda vida, en mayor o menor medida, participa, parecen estar enlazadas a modo de círculo: vida privada, vida proyecto, vida intensa, y de nuevo vida privada... para eludir el miedo, el malestar, la opresión y de nuevo el miedo, en un círculo que no parece tener salida.

Aparentemente, la red contradecía los valores imperantes en la empresa: el mando, la jerarquía y la disciplina. Sin embargo, cada vez más el capitalismo va adoptando la forma de red, en busca de mayor flexibilidad y movilidad para el capital y también en pro de una captura productiva de la creatividad social, de modo que podemos afirmar que el capitalismo global es una sociedad en red, y que la red es la forma de organización hegemónica no sólo para los movimientos

sociales, sino para el propio ciclo productivo de mercancías, pero también de lenguajes, símbolos, relaciones... es decir, de realidad.

La red, entonces, ya no puede ser vista de forma ingenua como un espacio horizontal ajeno al mando, pues es, ante todo, una forma de dominio que, lejos de establecer una igualdad radical, impone una política de la relación, una jerarquía de nudos privilegiados, un control por visibilización, una captura por autorresponsabilización y una gestión de la ambivalencia por transitividad entre los nudos.

Obligar a la vida a convertirse en proyecto, imponer la movilización total, producir y producir no importa qué: ése parece ser el mandato de la red, pues la interconexión entre todos los nodos, por más largo que sea el camino que esta interconexión deba recorrer, asegura que una diferencia radical no pueda producirse mientras la red siga siendo eso, una red.

Cuando el mando ya no persigue tanto la consecución de objetivos concretos como una obligación de actividad continua a fin de crear realidad, cuando en esta movilización cada uno debe motivar(se) a sí mismo, cuando toda la actividad relacional se traduce en proyectos... es entonces cuando la crítica sólo puede ser interrupción de la movilización, interrupción de la comunicación, interrupción del sentido, interrupción del orden de la red, sabotaje a la transitividad.

De ahí la metáfora del agujero negro, del cual, por más que se ilumine, nunca se podrá ver nada más que el propio agujero. Quienes hacen de un agujero un sitio para la vida no aspiran a ser comprendidos, valorados ni admirados. Están ahí y no necesitan más. No proyectan, no reflejan, quizás ni siguiera comunican. Simplemente, sabotean una estructura relacional inscrita en la realidad, sabotean la realidad misma aun pagando el elevado precio de sabotear(se) a sí mismos y, por tanto, de hacer(se) daño, pues en el agujero negro ninguna utopía está garantizada.

grupo autónomo a.f.r.i.k.a.
Luther Blisset/Sonja Brünzels

Manual de guerrilla de la comunicación

cómo acabar con el mal

El surgimiento de nuevos movimientos sociales en la última década se ha visto acompañado de nuevas formas de ocupación del espacio público y de entender la (contra)información. Sin embargo, muchas de estas formas no son nuevas, sino que tienen precedentes históricos en las vanguardias artísticas y políticas surrealistas y dadaístas, y han tenido continuidad en corrientes de pensamiento activista que van desde el situacionismo, el movimiento yippie, los provos holandeses y el neoismo hasta las formas actuales de plagiarismo, afirmación subversiva, tergiversación, distanciamiento y deterioro de imagen. En el manual se hace un exhaustivo repaso histórico y conceptual de los grupos, ideas y formas de actuación que podemos, asociar con la práctica de la guerrilla de la comunicación.

Han dicho de el:

«Un nuevo intento de hacer pasar por antagonismo político lo que no es más que exhibicionismo esnob de la vanguardia artística que se apunta a la moda postsitu.»
Jo. Pe., *Molotov*

«Lo que nos faltaba, los listillos de turno que pretenden cambiar el mundo con cuatro chistes intelectuales y una ilusa estetización de la política.»
El Chino, *La Lletra A*

«Éste es un ejemplo claro de lo que pueden dar de sí cuatro okupas que se meten a escribir sobre estética.»
María Zambrano, *Salamandra*

ISBN 84-88455-84-4
VIRUS editorial, Barcelona. 240 págs., 13.20 €
(2ª edición)

Stewart Home

EL ASALTO A LA CULTURA

Corrientes utópicas desde el Letrismo a Class War

De la tensión entre política y arte nacieron durante el siglo XX las vanguardias que cuestionaron tanto la POLÍTICA como el ARTE. Se trató de grupos y corrientes de pensamiento a veces muy minoritarios y de vida efímera que, aun así, tuvieron una gran trascendencia entre los adversarios de la cultura dominante. Envueltos en intensas y violentas disputas acerca de su actividad práctica y teórica, que contribuyeron a enriquecer las reflexiones acerca del modelo de sociedad que trasciende al arte dominante y las maneras de enfrentarse a uno y otro, muchos de estos movimientos sucumbieron a sus propias contradicciones internas.
Stewart Home se adentra en las entrañas de un mundo muy complejo y poco conociso, e intenta establecer las líneas de continuidad que unen a movimientos aparentemente tan distantes en el tiempo como el Dadaísmo, el Situacionismo y el Punk.

«El libro de Home es el primero, que yo sepa, en hacer un seguimiento de esta "tradición" tan particular y en tratarla con seriedad. Es un sano correctivo de la perpectiva sobreestetizada del arte de vanguardia del siglo XX actualmente prevaleciente.»
City Limits

«Al reflejar los aspectos más difíciles de categorizar del arte, que se lanza a sí mismo a políticas visionarias, el libro seguro que despertará el interés de científicos, políticos, artistas de performance y activistas.»
Art and Text

ISBN 84-96044-04-1
VIRUS editorial, Barcelona. 240 págs., 12 €
(2ª edición)