

12 lecturas sobre Hacktivismo

by EWhAck

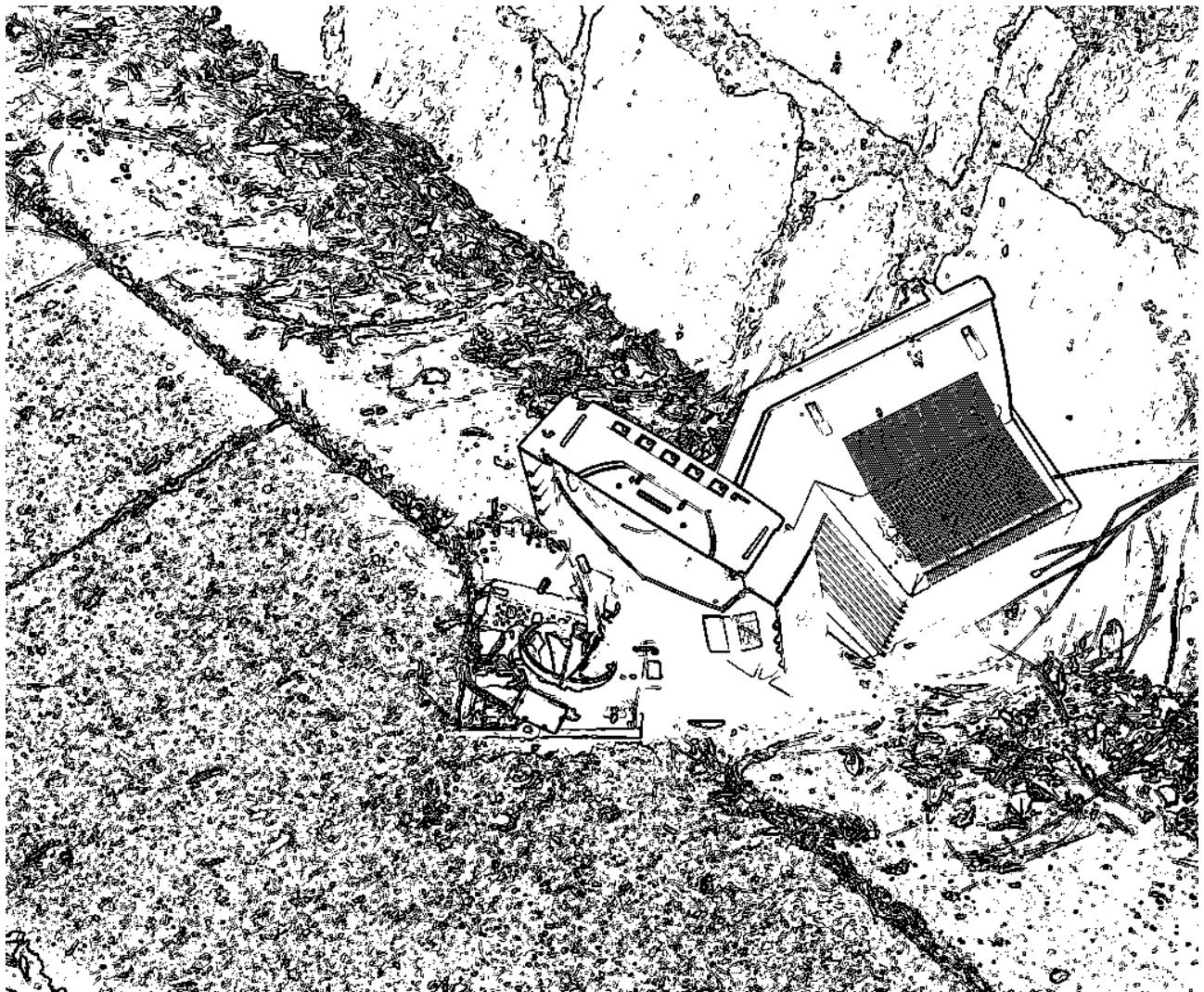
evhack.info@gmail.com

con la colaboración de:

patxangas@sindominio.net

txopi@sindominio.net

xavi@sindominio.net



Fotografia original Copyleft de Rich Anderson CreativeCommons by-sa [flickr.com]

10 Lecturas sobre HACKTIVISMO es una recopilación de artículos originalmente publicados en la revista *@rroba* (desde Noviembre del 2005 hasta Agosto del 2006). Se reproducen aquí sin permiso de la revista. Porque no hace falta pedirlo. Desde el principio la revista *@rroba* aceptó, amablemente, que el conocimiento y la información recopilados por la autora no serían propiedad de nadie, que el hacktivismo, así como sus historias y experiencias serán siempre libres. Todos los textos aquí recogidos son Copyleft: se permite su copia, modificación y distribución por cualquier medio siempre y cuando se haga bajo los mismos términos, es decir, grantizando la libertad de copia, modificación y distribución.

01. **HACKTIVISMO: Desde Mururoa hasta Chiapas, pasando por Tejas**
02. **HACKTIVISMO EXTENDIDO: Robótica contestataria y hacking jurídico**
03. **CYPHERPUNK: Criptografía rebelde**
04. **HACKMEETING 2005: Tres días de libertad en construcción permanente...**
05. **HACKLABS: Un cuerpo social para el hacktivismo**
06. **METABOLIK BIOHACKLAB: Metabolizando autonomía digital**
07. **CIELITO LINDO: Un hacklab enredando en Lavapiés**
08. **VOCES ABIERTAS: Streaming the radio desde la retaguardia hacktivista**
09. **HACK.IT: Socializar saberes sin fundar poderes**
10. **INDYMEDIA.ORG: La mayor red mediactivista contra la hegemonía informativa**
11. **TAZ 2.0: Servidores autónomos e infraestructura global de los pueblos (PARTE I)**
12. **TAZ 2.0: Servidores autónomos e infraestructura global de los pueblos (PARTE II)**

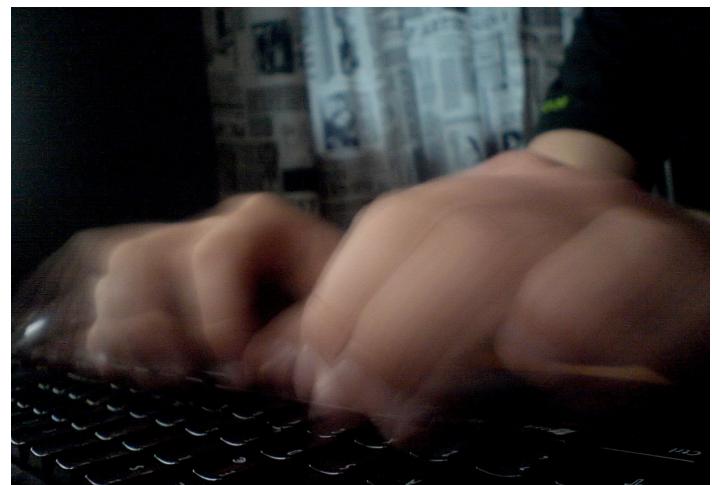
HACTIVISMO I:

Desde Mururoa hasta Chiapas, Pasando por Tejas

EVhAck

(evhack.info@gmail.com)

Lejos del estereotipo de personas introvertidas, aisladas y exclusivamente obsesionadas con la programación y la seguridad informática, muchos hackers toman conciencia de las dimensiones políticas del código que escriben y se lanzan para amplificar sus efectos políticos. Surge así el hacktivismo, ese híbrido entre hacking y activismo, un polémico espacio de intervención política y tácticas de subversión digital cuyos orígenes recientes se remontan al netstrike, el ciberzapatismo y la reacción de algunos miembros de Cult of the Death Cow a los defacement y ataques DoS contra la infraestructura comunicativa de países en vías de desarrollo.



[cc] by 2.0 Pal Berge: flickr.com]

través de medios electrónicos". Así nació el site hacktivismo.com y el proyecto Camera/Shy, una herramienta de esteganografía al alcance de cualquiera. Más tarde surgiría el sistema Six/Four: un proxy contra la censura que permite establecer comunicaciones seguras y anónimas entre dos máquinas vía protocolo ssl. El objetivo de estas dos herramientas es ofrecer oportunidades para la libertad de expresión en países con regímenes totalitarios. Sin embargo esta definición y práctica del hacktivismo surgió después de una larga discusión que enfrentó a diversos hackers políticos entorno a las diferentes formas de entender las alianzas entre el hacking y la política. Para entenderlas tenemos que remontarnos a las montañas de Chiapas...

■ ¿QUÉ SIGNIFICA HACKTIVISMO?

De un modo u otro el hacking y la informática siempre han estado unidos a ciertas actitudes políticas, difícilmente clasificables, eso sí, desde la vieja dicotomía de la derecha y la izquierda. Por lo tanto el hacktivismo (sin el *tag* bien definido, pero con esa mezcla entre aspiraciones político-sociales y habilidades técnicas) se remonta hasta los orígenes de la red, los yippies[1], la Free Software Foundation [2] o los primeros cypherpunks (entre ellos Philip Zimmermann [3], creador de GPG). Los ideales de acceso universal a las computadoras, libre flujo de información y derecho a la privacidad son una constante de la cultura hacker del "do it yourself" o el "information wants to be free". Pero el término hacktivismo no surgirá hasta mucho más tarde.

Oxblood Rufin, miembro veterano del Cult of the Death Cow [4] o cDc (mítico colectivo de hackers asentado en Tejas) y fundador de hacktivismo.com, nos recordaba hace poco [5] cómo su compañero Omega usó por primera vez la palabra hacktivismo en 1996 para referirse al "hacking con objetivos políticos". Pronto la definición tomó un cariz más concreto y el propio Oxblood asumió la tarea de "usar la tecnología para mejorar los derechos humanos a

"Los ideales de acceso universal a las computadoras, el libre flujo de la información y el derecho a la privacidad son una constante de la cultura hacker"

■ MÁS ALLÁ DEL HIGH-TECH: HACKTIVISMO LOWTECH DESDE LAS MONTAÑAS DE CHIAPAS

Los informes de la Rand Corporation dividen la infoguerra en tres capas: la capa física (definida por la infraestructura de hardware y redes), la capa lógica o sintáctica (definida por los programas, protocolos y sistemas que corren sobre la capa física) y la capa semántica (de contenido). Antes de que cDc acuñara el término hacktivismo, los Zapatistas [6], conscientes de su incapacidad de ganar batalla alguna en las capas físicas y lógicas, decidieron optar por la capa semántica (amplificando su mensaje a través de la red) como espacio de intervención política y hacking tecnopoético: la capa de la legitimidad y la dignidad histórica, la capa de la verdad en la que el gobierno mexicano apenas podía compilar ya más engaños entorno a la situación de abandono de los pueblos indígenas. Así fue como los Zapatistas decidieron atacar con bombas semánticas

[7] el ciberespacio. Era el año 1994 y los comunicados de los indios de la Selva Lacandona atravesaban el planeta viajando de correo en correo, a través del enrutamiento de las redes sociales de personas que, cautivadas por el diseño poético de los cuentos mayas guerrilleros, reenviaban los comunicados a familiares y

amigos. El resultado fue un firewall contra una posible invasión militar del gobierno mexicano a la zona de Chiapas, un firewall construido por miles de miradas de ojos internacionales que esperaban el siguiente comunicado zapatista.

Pronto surgiría el ciberzapatismo [8]: una forma de “disturbio electrónico” en la red. El Critical Art Ensemble (CAE o Conjunto de Arte Crítico [9]) llevaba algunos años experimentando en las interfaces entre la literatura ciberpunk, los nuevos medios electrónicos y la política antagonista. En 1998 Ricardo Dominguez y otros miembros del CAE decidieron crear una herramienta de activismo low-tech. El *Zapatistas Flood Net* era un pequeño programa en javascript que repetía 3 veces por segundo la petición de página al servidor objetivo de la protesta. Para el participante en este acto de “desobediencia civil electrónica” [10] bastaba con dejar abierta la ventana de su navegador y sentarse a ver. 80.000 personas participaron en esta manifestación virtual y el servidor que alojaba la página web del entonces presidente de México cayó. Acciones parecidas se coordinaron también gracias a los electrohippies [11].

La propuesta original de apoyar a los zapatistas con acciones de desobediencia civil electrónica vino de un grupo de hacktivistas italianos (el Anonymous Digital Coalition) que años antes, en 1994, estrenaron el modelo de acción política Netstrike [12] (manifestación virtual) consiguiendo tumbar varios servidores web franceses en protesta por las pruebas nucleares en Mururoa. Las reacciones gubernamentales tardaron cierto tiempo pero llegaron con virulencia. El pentágono acusó al CAE de ciberterrorismo [13] y desarrolló un programa que tumbaba el sistema operativo de los ciberzapatistas mientras que el gobierno italiano secuestró el servidor que alojaba netstrike.it en el 2001 [14] y detuvo a 42 hacktivistas en el 2002 por su vinculación con el netstrike e indymedia.org.

LA DISCORDIA: HACKTIVISMO E INFOGUERRA

Si bien el netstrike o la desobediencia civil electrónica presentan cierta legitimación, gracias a la masificación de cibernautas que hacen peticiones a servidores (en analogía con las manifestaciones urbanas que paralizan el tráfico), pronto diversos grupos de “hackers” empezaron a hacer ataques de denegación de servicios o intrusiones destructivas (como defacements) en nombre del hacktivismo. Así por ejemplo Legions of the Underground [15] declararon la infoguerra a Iraq y China por no respetar los derechos humanos.

Rápidamente el cDc (así como muchos otros colectivos de hackers, entre ellos L0pht, Phrack, el CCC alemán o Hispahack) hicieron un llamamiento [16] en contra de la destrucción de las infraestructuras telemáticas como forma de acción política. Y aquí volvemos al principio de este artículo, la reacción a estas formas destructivas de hacktivismo puso de manifiesto la necesidad de definir y practicar otras formas de hacktivismo más constructivas y centradas en ofrecer herramientas a ciudadanos de regímenes totalitarios; en lugar de destruir la infraestructura de red con la que los ciudadanos de esos mismos regímenes pudieran luchar por su derecho a la libre expresión.♦

EVhAck (evhack.info@gmail.com)

REFERENCIAS

- [1] <http://en.wikipedia.org/wiki/Yippie>
- [2] <http://fsf.org>
- [3] <http://www.philzimmermann.com>
- [4] <http://www.cultdeadcow.com>
- [5] http://www.cultdeadcow.com/cDc_files/cDc-0384.html
- [6] <http://www.ezln.org.mx/>
- [7] http://palabra.ezln.org.mx/comunicados/1994/1994_04_10_e.htm
- [8] <http://www.eco.utexas.edu/Homepages/Faculty/Cleaver/zapsincyber.html>
- [9] <http://www.critical-art.net/>
- [10] <http://www.thing.net/~rdom/ecd/ecd.html>
- [11] <http://www.fraw.org.uk/ehippies/index.shtml>
- [12] <http://www.contrast.org/netstrike/>
- [13] <http://www.thehacktivist.com/archive/news/1998/Hacktivists-NYTimes-1998.pdf>
- [14] <http://www.ecn.org/inr/netstrike/ilmanifesto.html>
- [15] <http://www.legions.org/>
- [16] <http://www.noticias.com/articulo/08-01-1999/redaccion/hackers-contrarios-utilizar-sus-conocimientos-ciberguerras-181i.html>

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría orginal y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.

<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Lunes 4 de Febrero del 2006

URL: <http://barandiaran.net/textos/evhack/cielito/>

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.



La selva Lacandona, territorio zapatista, uno de los lugares que vió nacer el hacktivismo, el mensaje de los indígenas de Chiapas (Méjico) multiplexado por las redes de internet cuando ésta apresas había empezado a llegar a los hogares de los más afortunados. [(cc) by 2.0 Natares: flickr.com]

HACKTIVISMO EXTENDIDO

robótica contestataria y hacking jurídico

by EVhAck

El hacking se entiende generalmente como algo asociado exclusivamente a la informática. Sin embargo, ni el origen de la palabra ni muchos de sus significados presentes limita el hacking al mundo de las redes de ordenadores. Robots subversivos y grafiteros, licencias víricas de software o demandas contra el canon son algunos de los ejemplos con los que la imaginación hacker ha conseguido desplazar los límites de un sistema creando efectos imprevisibles para su diseñador.



GraffitiWriter el robot grafitero desarrollado por el Instituto de Autonomía Aplicada, capaz de escribir frases en el suelo a una velocidad superior a los 20 Km/h, todo un artefacto hacktivista para intervenir en el espacio público. Las instrucciones para su construcción (incluyendo el código de software que controla los sprays que hacen de impresora) se encuentran en la web del Instituto: <http://appliedautonomy.com>.

HACKTIVISMO MÁS ALLÁ DE LAS FRONTERAS DEL TECLADO

Al hablar de hacking o hacktivismo es casi inevitable evitar las imágenes del teclado, el ordenador o Internet. Sin embargo, el término *hack* surgió en el club de maquetas de ferrocarril del MIT [1], para referirse a la pequeña intervención en los circuitos del ferrocarril que permitía ampliar el sistema. Un *hack*, explica la web del club, “alcanza el objetivo deseado sin cambiar el diseño del sistema en el que está imbricado (...) a pesar de estar reñido con el gran sistema, un *hack* es generalmente bastante ingenioso y efectivo”. El *Jargon File* [2] (el diccionario de referencia para orientarse en la jerga hacker), creado y mantenido por Eric Raymond, ofrece una enriquecedora definición de hacker. La sexta acepción del término indica que hacker significa “experto o entusiasta de todo tipo” (pudiendo uno ser hacker de la astronomía, por ejemplo). La séptima acepción es más aclaratoria: “Aquél que disfruta del reto intelectual de superar o sortear creativamente las limitaciones”. Si a esto le añadimos una dimensión colaborativa copyleft y unos objetivos políticos de transformación social en defensa de la libertad y los derechos sociales, podemos empezar a imaginar formas de hacktivismo que superan los estrechos límites del teclado. Allí donde haya sistemas, códigos y limitaciones técnicas hay espacio para el hacking y el hacktivismo. La ingeniería robótica y el sistema jurídico son algunos espacios en los que se han escrito muchas de las páginas más imaginativas de la historia del hacktivismo.

ROBÓTICA CONTESTATARIA

En 1999 surge el *Institute for Applied Autonomy* [3], sus ingenieros

publican en revistas científicas, dan conferencias en universidades, participan en congresos académicos... y construyen robots contestarios. El *Graffitiwriter* fue uno de sus primeros proyectos. Diseñado como artefacto mediador para intervenir en el espacio público, *Graffitiwriter* es un robot autónomo capaz de escribir graffitis en el suelo a considerable velocidad (más de 20 Km/h). Como buenos hacktivistas copyleft en su web incluyen toda la información necesaria para construirlo fácilmente.

«Allí donde haya sistemas, códigos y limitaciones técnicas hay espacio para el hacking y el hacktivismo.»

Pero a pesar de que la propia idea y la construcción del robot ya es interesante de por sí, el *hack* en este caso vino de uno de los estudios sociológicos que se realizó con él. Admitimos pasivamente el bombardeo de la publicidad en el espacio público visual, allí donde miremos hay un cartel luminoso, o un gigantesco cartel rojo incitando a la compra de un producto que nos promete felicidad (cuando no es una de las top models más deseadas del mundo, despertando los instintos más profundos para asociarlos a un objeto de consumo). Y, sin embargo, nos cuesta retomar ese mismo espacio y expresar nuestros deseos e ideas libremente. Si se le pregunta, la mayoría de la gente responderá que no le parecen bien las pintadas, que no estaría dispuesto ha realizar una. Así lo descubrieron los investigadores de Instituto de Autonomía Aplicada... hasta que decidieron probar qué pasaría si esas mismas personas dispusieran de un robot que pintara en la calle lo que ellas decían por un micrófono. Resultados concluyentes: “los estudios muestran que casi en el 100% de los casos cualquier

persona en la calle estará dispuesta a cometer actos vandálicos si se le da la oportunidad de hacerlo a través de la mediación de tecnología tele-robótica". Un buen *hack* para demostrar que lo que la ley considera un "acto de vandalismo" se convierte en un acto de jocosa expresión personal si se usa un robot de por medio: señores jubiladas, niños de 8 años, ejecutivas de oficina... convertidos en grafiteros callejeros. (Y sí, por supuesto, *Graffitiwriter* también se ha utilizado para escribir mensajes de protesta delante de la línea policial en más de una manifestación).

Sin ir tan lejos hay buenos ejemplos locales de robótica contestataria. La Fábrica de Cosas Bonitas [4] ha lanzado un proyecto llamado ANA. Se trata de utilizar la misma plataforma de los robots utilizados por el ejército norteamericano para darles las vuelta y usarlos en la línea de protesta contra la cumbre del G8 en Hamburgo. "La única diferencia para el manifestante" dice su web "es que no lleva su pancarta entre sus manos, sino que la tiene a una distancia de medio kilómetro". Una pequeña gran diferencia si se trata de una carga policial.

■ REPROGRAMAR EL CÓDIGO JURÍDICO

Todas las civilizaciones dependen del registro físico de una serie de reglas de funcionamiento social: se llama código jurídico. Su aplicación al hardware social que somos nosotras genera un orden económico, educativo o cívico y unos procesos determinados. Bien o mal el caso es que las leyes funcionan, operan... como un sistema operativo! Y aquí se abre todo un mundo para la imaginación hacktivista. Sin duda el *hack* jurídico más importante de la historia del hacktivismo se lo debemos a Richard Stallman [5] y Eben Moglen [6] creadores de un pequeño programa que se ejecuta en las rutinas del copyright: la licencia GPL (General Public License [7]), la protectora del software libre: el copyleft. Cuatro libertades (uso, modificación, copia y publicación) y una sola restricción: no permitir ninguna copia o derivado que limite las libertades anteriores. Inserta este pequeño programa en el régimen de propiedad intelectual que atraviesa el desarrollo de software y al de unos años tendrás un toda una serie de programas recombinables, acumulativos: un proceso imparable de colaboración pública (justo lo contrario para lo que el copyright fue



Richard Stallman, fundador del software libre, durante la presentación del primer borrador de la GPLv3: la licencia de software libre más extendida y cuya última versión permitirá mantener el software libre de las amenazas de las patentes, los mecanismos anticopia y la incompatibilidad con otras licencias. Foto tomada de Flickr.com. Copyright de Webmink (bajo licencia CC-by-sa).

programado). Pero las leyes y sus contextos (su hardware) evolucionan, y mucho. Así que llegó el momento de reprogramar la GPL. Evitar la implantación "maliciosa" de los mecanismos anticopia (DRM, TCPA-Palladium), el sabotaje de las patentes de software y la incompatibilidad con otras licencias libres es el objetivo de la nueva versión de la GPL, la versión 3.0 [8]. Y a eso se está dedicando la Free Software Foundation durante este año, en uno de los mayores procesos participativos de hacking jurídico que la historia ha conocido.

Pero no todo son licencias de software en el hacktivismo jurídico. El sitio Derecho de Internet [9] (a cargo del abogado y usuario de GNU/Linux Javier de la Cueva) acaba de publicar la segunda versión de la demanda contra el Canon de la SGAE (ese cobro invasivo de las sociedades de gestión que pretende hacernos pagar hasta un 60% más en la compra de cualquier dispositivo de almacenamiento de datos —aunque lo usemos para copiar software libre o las fotos de nuestras vacaciones). En este caso se trata de crear una serie de instrucciones para que cualquier persona pueda interponer la demanda, sin gastarse un céntimo, sin necesidad de abogados. El pack de la demanda incluye los documentos burocráticos a llenar y las instrucciones básicas de cómo y dónde hay que realizar todo el procedimiento. De momento son ya más de 20 personas las que han "ejecutado" la demanda (sin mediación de Javier de la Cueva) y la experiencia está permitiendo ir puliéndola para que tenga un mayor efecto en la jurisprudencia y acabar invalidando el canon. El último *hack* de Javier de la Cueva merece especial atención: comprar el CD virgen en el que se grabe la vista del juicio, desglosado el canon en la factura de compra del CD quizás la justicia se quite la venda si se entera de que la SGAE cobra por cada una de sus sentencias. ☀

Evhack (evhack.info@gmail.com)

REFERENCIAS

- [1] <http://tmrc.mit.edu/hackers-ref.html>
- [2] <http://www.catb.org/esr/jargon>
- [3] <http://www.appliedautonomy.com>
- [4] <http://www.lafabricadecosasbonitas.com>
- [5] <http://www.stallman.org>
- [6] <http://emoglen.law.columbia.edu/>
- [7] <http://uggs.sindominio.net/licencias/gpls.html>
- [8] <http://gplv3.fsf.org>
- [9] <http://www.derecho-internet.org>

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría original y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Lunes 9 de Enero del 2006

URL: http://barandiaran.net/textos/evhack/hacktivismo_extendido

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

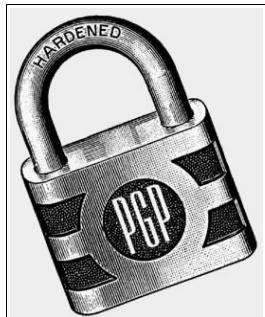
EXTENSION: 1569 palabras, 9964 caracteres

CYPHER PUNK

Criptografía rebelde.

by EVhAck

La historia de la criptografía incluye personajes tan ilustres como el poeta Edgar Allan Poe, el matemático Claude Shannon o el emperador romano Julio Cesar. Pero no será hasta la década de los 70 y el posterior advenimiento de la era Internet que un grupo de personas consiga superar los límites de la inteligencia militar y la curiosidad matemática introduciendo la criptografía en todos los rincones de la vida cotidiana: los *cypherpunks*. Gracias a ellos podemos hoy mantener comunicaciones seguras. La historia de estos pioneros es la historia de la libertad que gozamos hoy en el ciberespacio.



"La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es secretismo. Una cuestión privada es algo que no queremos que todo el mundo sepa, pero una cuestión secreta es algo que no queremos que nadie sepa. La privacidad es la capacidad de revelarse selectivamente al mundo".

ERIC HUGHES. *Un manifiesto CypherPunk*

LA HISTORIA DEL CYPHERPUNK¹ es la historia de la definición de la frontera entre lo privado y lo público, el pilar de la política telemática. En ella han participado científicos, espías, políticos, visionarios, matemáticos, empresarios y, como no, hackers. Durante los 70 y 80 unos tipos con barbas y camisetas revientan el monopolio estatal de la criptografía: creando y distribuyendo herramientas de criptografía de clave asimétrica, una garantía para la privacidad y el comercio en la red.

Estamos en los años 70 y la NSA² (Agencia de Seguridad Nacional) y otras agencias gubernamentales parecidas guardan celosamente todo lo que tiene que ver con la criptografía. Tienen bajo su control a la gran mayoría de científicos y matemáticos que despuntan en estas áreas, impiden la publicación de artículos criptográficos manteniendo a la sociedad civil al margen del poder de proteger sus comunicaciones. Sin embargo, nombres como Whitfield Diffie, Martin Hellman³, Rivest,



Phil Zimmermann, autor de PGP, un programa de cifrado de comunicaciones basado en la criptografía asimétrica y uno de los personajes más importantes de la escena cypherpunk. Esta foto fue realizada justo después de que Phil, en 1996, saliera airosa de uno de los tantos juicios con los que la administración norteamericana le ha presionado durante años.

Shamir y Adlman (RSA)⁴ o Phil Zimmermann⁵ encabezarán la lista los luchadores contra el monopolio gubernamental de las comunicaciones seguras, creando sistemas de cifrado seguro y cambiando de forma irreversible la importancia que tiene hoy en día la criptografía para nuestras vidas en la red (y fuera de ella).

CRÍPTOGRAFÍA DE CLAVE PÚBLICA: EL NACIMIENTO DE UNA AMENAZA PARA EL MONOPOLIO DE LA NSA

David quiere mandar un mensaje a Teresa pero entre ellos no se conocen y encima saben que Pedro quiere escuchar su conversación y quiere hacerse pasar por David. ¿Cómo podría resolver este problema un sistema criptográfico? Éste fue el dilema que, durante muchos años, mantuvo a uno de los pioneros de la criptografía digital, Whitfield Diffie, recorriendo Estados Unidos en su *Dantsu 510*, en busca de una respuesta a lo que pensaba que sería la clave para las comunicaciones electrónicas del futuro. En 1970 conoce a Martin Hellman, contagiándole su entusiasmo por el tema. Ahí estaban, un ex-hacker del MIT con un profesor de Stanford unidos en la búsqueda de una solución que la criptografía de la época no parecía poder resolver.

En noviembre de 1976, Diffie y Hellman publican el artículo "Nuevas direcciones en la criptografía"⁶. Como en tantos otros casos en la historia de la ciencia y la ingeniería la solución resultó ser una idea sencilla pero tremadamente poderosa: dividir la clave en dos. David crea dos claves, una privada y otra pública, y le envía a Teresa su clave pública al tiempo que Teresa hace lo mismo. Si David quiere mandar un mensaje a Teresa debe utilizar su propia clave privada y la clave pública de ella para cifrar el mensaje. Así, Teresa es la única persona que puede descifrar el mensaje ya que ésto sólo puede hacerse combinando las dos claves inversas (la pública de David y privada de Teresa). En este caso aunque Pedro se haga con la clave pública de Teresa y con el mensaje de David, nunca podrá descifralo sin la clave privada de Teresa. Además David puede firmar su mensaje usando su clave privada, de tal modo que Teresa pueda certificar que el mensaje viene de David (y no de malicioso Pedro) combinando el mensaje cifrado de David con la clave pública de éste último.

Así, el artículo de Diffie y Hellman no sólo fue pionero en hacer

¹ <http://www.cypherpunk.org>

² <http://www.nsa.gov>

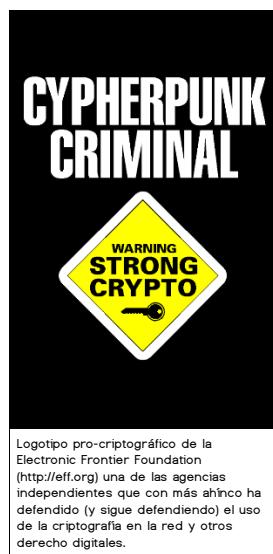
³ <http://es.wikipedia.org/wiki/Diffie-Hellman>

⁴ <http://es.wikipedia.org/wiki/RSA>

⁵ <http://www.philzimmermann.com/ES/background/index.html>

⁶ <http://citeseer.ist.psu.edu/diffie76new.html>

uso de dos claves, sino también en romper con el secretismo de la NSA. La puerta quedaba abierta para la investigación e implementación pública, al margen del control gubernamental. Así, en 1978, se publica el algoritmo RSA, acrónimo formado con las iniciales de sus autores (Rivest, Shamir y Adlman) que aplicaron por primera vez, y de forma eficaz, la idea original de Diffie y Hellman. No contentos con ello, el trío de visionarios funda la empresa RSA Data Security Inc⁷. La NSA empieza a ponerse nerviosa. Durante los años siguientes, el gobierno de Estados Unidos, se adentra en una espiral de litigios y presiones para evitar la proliferación de la criptografía asimétrica. El acoso continuado a los usuarios y científicos, que utilizaban e investigaban públicamente algoritmos de cifrado efectivos, termina uniéndose a éstos y haciéndoles crear una fuerte comunidad de desarrollo y defensa de la privacidad en la red.



CRIPTOANARQUÍA

Phil Zimmermann, activista antinuclear detenido junto a Carl Sagan en una de las múltiples protestas que protagonizaron, se reincorporó al mundo de la criptografía al conocer a Charlie Merritt, a mediados de los 80. Merritt intentaba integrar el algoritmo RSA en un microordenador, el sueño que, sin mucho éxito, había intentado realizar el propio Zimmermann en 1977. El encuentro con el atrevido Merritt lo impulsó a volver a intentarlo. De 1984 a 1991 Zimmermann se dedica exclusivamente al desarrollo del programa informático más famoso y extendido de la criptografía digital: el PGP (Pretty Good Privacy ---privacidad bastante buena). Pero es la manera en que se hizo público el programa PGP⁸ lo que lo convirtió en algo histórico para el activismo telemático.

«Si la privacidad es declarada ilegal, sólo los ilegales disfrutarán de la privacidad»

Por aquél entonces, Joseph Biden, senador de los Estados Unidos publica el borrador 266 de la nueva ley antiterrorista, que venía a exigir a los proveedores de servicios de comunicaciones electrónicas y fabricantes de equipos electrónicos el acceso a los contenidos originales de las transmisiones (voz, datos etc.). Zimmermann se dio cuenta de que, si no lanzaba pronto su programa al mundo, la aplicación de la ley impediría irreversiblemente, su publicación y distribución. Así que decidió, con la ayuda de los ciberactivistas Kelly Goen y Jim Warren difundir, el programa por la, por aquel entonces desconocida pero incipiente, Internet.

El primer fin de semana de junio de 1991 Goen, con un portátil, un módem y un acoplador acústico, marcha de cabina en cabina subiendo el programa a diferentes destinos de la red. Al día siguiente, personas de todo el mundo cifraban sus mensajes con PGP. Zimmerman distribuyó el programa gratuitamente garantizando además su transparencia al hacer el código accesible. Consideró más importante la privacidad que rentabilizar económicamente los 7 años de trabajo. En

la propia documentación se podía leer la siguiente frase: *“Si la privacidad es declarada ilegal, sólo los ilegales disfrutarán de la privacidad”*.

En los primeros años de los 90 Eric Hughes escribiría el manifiesto cypherpunk⁹ recordando el sentir de una comunidad que hizo y sigue haciendo posible disfrutar de un lugar seguro en el ciberespacio. Fueron tiempos donde lo público y lo privado dejaba de estar gestionado por el poder institucionalizado. La virtualidad de los nuevos mundos empezaba a ser real, Internet cada día era más grande y las comunicaciones electrónicas empezaban a ser cotidianas y seguras para aquellos preocupados por su privacidad.

Hoy podemos seguir disfrutando de un lugar seguro en las redes de comunicación pero no podemos descuidar su defensa. Desgraciadamente la empresa que (liderada por Zimmermann) actualiza las versiones de

PGP ha sido comprada por otra que ha decidido cerrar su código (lo que ha provocado abandono del mítico criptoanarquista). Nos queda, sin embargo, la versión libre de PGP: el proyecto GPG¹⁰ (GNU Privacy Guard) un programa extendido y fácilmente integrable en tu gestor de correo favorito. En nuestras manos queda hacer frente al recorte de libertades con el que bajo al excusa antiterrorista se amenaza, una vez más, la herencia de los pioneros cypherpunk. ☀

EvhAck

la mujer que se atrevió a morder la manzana prohibida
del conocimiento, el pecado original del hacker
(evhack.info@gmail.com)



METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría orginal y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Lunes 9 de Marzo del 2006

URL: <http://barandiaran.net/textos/evhack/cypherpunk/>

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSION: 1373 palabras 8498 caracteres

⁷ <http://www.rsasecurity.com/>

⁸ <http://www.ugr.es/~aquiran/cripto/expedien/exped002.htm>

⁹ http://suburbia.sindominio.net/article.php3?id_article=81

¹⁰ <http://gnupg.org>

HACK MEETING 2005

Tres días de libertad en
construcción permanente...

by EVhAck



Durante los días 21, 22 y 23 de Octubre se celebró en el recinto ferial de Es Mercadal (Menorca) la sexta edición del Hackmeeting: un encuentro anual, autogestionado y gratuito, en el que hacking y activismo se fusionan en la frontera entre las redes tecnológicas y sociales. Bajo el lema "libertad en construcción permanente" esta edición, más pequeña de lo habitual dada la dificultad de acceso a la isla, reunió a cerca de 250 personas intercambiando técnicas, conocimientos y proyectos alrededor de temas como la privacidad, el desarrollo de aplicaciones de software libre, los hacklabs, la seguridad de las redes inalámbricas, la historia del ciberpunk o los medios de comunicación alternativos. El lema de la pancarta de presentación del HM, "Que no te engañen... compartir es bueno!", dio el pistoletazo de salida a esta edición marcada por el reciente acoso mediático al libre intercambio de cultura y conocimientos en la red.



Un ordenador en una caja de zapatos. Los hackmeetings nunca de sorprender con todo tipo de artefactos imaginativos y reciclados.

AUTOORGANIZACIÓN EN RED

Como es habitual el HM llevaba ya unos meses auto-organizándose telemáticamente de forma distribuida a través de una lista de correo pública [1] y un wiki [2] alojados en el servidor autónomo sindominio.net. El viernes por la mañana estaba ya todo dispuesto para la inteligencia colectiva de la que surge el hackmeeting, sin necesidad de organizadoras, ni patrocinio, ni asignar número a las participantes.

«Fruto de la red de encuentros y cruce de proyectos que es el HM podemos anunciar el surgimiento del nodo menorquín de la red indymedia o la campaña de acciones contra la criminalización del intercambio de información en la red: compartir es bueno.net»

El infopoint a la entrada recogía la información de bienvenida coordinando las incidencias, el material del HM y la venta de camisetas (con las que sufragar los gastos de este evento gratuito y autogestionado). Posters en las paredes hacían de wikis analógicos en los que completar turnos de barra, cambios de última hora en el programa o anunciar la IP del servidor FTP anónimo. El área LAN y "Cacharreo" servía de conector para una cincuentena de ordenadores y una veintena de cerebros: todo un espacio de intercambio p2p cara a cara, oportunidad para cursos improvisados e instalaciones de Debian GNU/Linux. Tres áreas de conferencias, equipadas con proyector, equipo de sonido y grabación, un comedor y una sala-dormitorio con un centenar de colchones completan esta rápida cartografía del espacio que acogió al HM.

DEL CYBERPUNK A LA WEB 2.0

A nivel de contenido la privacidad marcó sin duda uno de los ejes del HM gracias a los compañeros de BULMA [3] que organizaron charla, taller GPG y *signing party* (fiesta de intercambio y firma de claves públicas de identificación y cifrado). También hubo espacio para la cultura geek y hacktivista: José E. Marchesi (coordinador de GNU España) nos hizo reír y soñar con la historia del editor libre Emacs mientras que Patxangas (sindominio.net y HackResi [4]) diseccionó los arquetipos, distopías y mitos que construyen el imaginario hacktivista contemporáneo a través de una exquisita selección de fragmentos de películas de culto ciberpunk (Días Extraños, Brazil, Blade Runner, Gattaca, Terminator, Ghost in the Shell o Nivel 13).

Avanzando en los temas más técnicos Esteve Fernández deleitó al público con una presentación, realizada en un programa creado por él mismo en AJAX, en la que destripó los secretos de la Web 2.0. a través de Ruby on Rails y toda la serie de aplicaciones y filosofías del diseño web que están transformando nuestro ciberespacio cotidiano. Txipi



Charla de José E. Marchesi (coordinador de GNU-españa) sobre la historia de Emacs, el editor de programación GNU que rivaliza con VI.

(e-ghost [5], metabolik [6] y sindominio) pegó un buen repaso a las vulnerabilidades en las redes inalámbricas a través de WepLab [7], una excelente herramienta de crackeo del cifrado WEP cuya versión gráfica desarrolla él mismo. Siguiendo con proyectos de desarrollo de software libre en nuestras tierras, el nombre en clave *Blogxpupoli* escondía dos charlas acerca de uno de los más arriesgados proyectos hacktivistas de software libre de habla hispana: Blogmail [8], un intento de redefinir los límites del conocimiento aislado en el correo electrónico liberándolo a través de una interfaz web basada en wordpress.

Tampoco faltaron charlas introductorias al software libre, al funcionamiento de básico de redes o rudimentos con GNU/Linux, espacios en los que acercar las nuevas tecnologías a "la gente de la calle". Por su parte la ceremonia tecnopagana del viernes por la noche despertó tanta expectación como sonrisas. Sorprendió, sin duda, el dispositivo de VJ de esta *performance* en clave tecnoreligiosa: la ceremonia se emitía en *streaming* de vídeo, recogido en la conferencia Piksels [9] desde Noruega por desarrolladores de PureData (un lenguaje visual de programación multimedia); éstos fusionaban sus proyecciones en PD para enviarlas de vuelta por *streaming* al hackmeeting en tiempo real y proyectarlas sobre la ceremonia.

FRUTOS DE LA COMPLICIDAD

Fruto de la red de encuentros y cruce de proyectos que es el HM podemos anunciar el surgimiento del nodo menorquín de la red indymedia [10] o la campaña de acciones contra la criminalización del intercambio de información en la red y en favor del acceso universal a la cultura: compartiresbueno.net. Nada de esto hubiera sido posible sin la atmósfera de confianza y trabajo colaborativo que se vivió durante el hackmeeting. "El buen ambiente y la familiaridad de esta edición han sido los grandes protagonistas" comenta Patxangas (uno de los veteranos de estos encuentros) "se nota que después de 6 años de hackmeeting se va afianzando una comunidad cada vez más sólida. Queda ahora por ver si esta red de proyectos y colectivos logra hacer frente a la amenazante sombra que despliegan las industrias culturales y los monopolios del software sobre la libertad que hemos experimentado hasta ahora en el ciberespacio." A este reto tendrán

REFERENCIAS

- [1] <https://listas.sindominio.net/mail-listinfo/hackmeeting>
- [2] <http://sindominio.net/hackmeeting>
- [3] <http://bulma.net/>
- [4] <http://www.hackresi.net>
- [5] <http://www.e-ghost.deusto.es/phpwiki/>
- [6] <http://metabolik.hacklabs.org>
- [7] <http://weplab.sourceforge.net/>
- [8] <http://blogmail.sourceforge.net/>
- [9] <http://www.piksels.no>
- [10] <http://indymedia.org>
- [11] <http://hacklabs.org>
- [12] <http://hackitectura.net/hackmeeting05/>



Una de las mesas de la LAN (Local Area Network): la red de ordenadores que se improvisa cada año en los HackMeeting y donde se puede encontrar más de un centenar de ordenadores: libre intercambio de saberes, información y técnicas. Una red en la que experimentar con las tecnologías libres y la inteligencia colectiva.

que hacer frente los hacklabs [11] una red de laboratorios hacker y hacktivistas estrechamente vinculada al hackmeeting y que surge, precisamente, para dar continuidad durante el año a la experiencia tecnopolítica de este intenso evento.

Si os habéis quedado con las ganas de haber acudido a esta edición estáis de suerte: el centro de medios del HM se encargó de emitir en directo, grabar y comprimir sonido e imagen de casi todas las conferencias (ya accesibles para su descarga vía web [12] y p2p). Eso sí, apuntadlo ahora en vuestras agendas electrónicas: Mataró (Barcelona) albergará la próxima edición de este evento que se confirma como uno de los encuentros más importantes, acogedores y abiertos del hacktivismo europeo.★

Evhack (evhack.info@gmail.com)

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría orginal y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-nc/2.5/es/legalcode.es>

VERSIÓN: versión 8 de Noviembre del 2005

URL: <http://barandiaran.net/textos/evhack/hm2005/>

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSION: 1319 palabras 8409 caracteres

HACKLABS

un cuerpo social para el hacktivismo

by EVhAck

(evhack.info@gmail.com)

Al hablar de hacktivismo y hackmeetings resulta cada vez más difícil pensar estos últimos sin los hacklabs. Los hacklabs [1], laboratorios hacker o hacktivistas, son espacios de autogestión tecnológica, colectivos en los que reciclaje de ordenadores, desarrollo y aprendizaje con software libre y activismo se dan la mano. Estos laboratorios ya superan la cincuentena en toda Europa (Italia, España, Francia, Inglaterra, Amsterdam) pero ... ¿de dónde surgen? ¿qué es exactamente un hacklab? ¿cómo se organizan? ¿para qué?

■ “AL PRINCIPIO FUERON LOS HACKMEETING”

El colectivo y espacio okupado ASCII (Amsterdam Subversive Center for Information Interchange) [2] es quizás unos de los predecesores más claros de los hacklabs; junto al FREAKNET medialab [3] italiano. Okupados a mediados de los 90 estos espacios centraron su trabajo en la intersección entre movimientos sociales y nuevas tecnologías promoviendo el libre acceso a las computadoras y a la incipiente y desconocida Internet. Pero no será hasta finales de los noventa que surjan los hacklabs, propiamente dichos, de la mano de los hackmeeting [4, 5] o, más bien, del deseo de hacer permanecer lo que sucede durante los mismos a escala local: seguir manteniendo una LAN, un espacio en el que reunirse, aprender, intercambiar e investigar. Y es que “al principio fueron los hackmeeting” como afirma Blicero que uno de los fundadores del LOA Hacklab de Milán [6] que surgió precisamente después del segundo hackmeeting italiano (en 1999) [7]. Kernel Panic [8] fue el primero de nuestros hacklabs más cercanos y surgió en Barcelona (después del primer hackmeeting de habla hispana en el 2000 [9]). A estos pioneros laboratorios siguieron Metabolik [10] en Bilbao y Cielito Lindo [11] en Madrid (a finales del 2001). Despues llegaron Downgrade [12] en Zaragoza, el Kaslab de Vallecas, Kakelbont (Vitoria), La Casa Encantada (Compostela), Sevilla, Canarias, y un largo etc. Sin embargo estos espacios no son un fenómeno exclusivamente español, ni mucho menos, Italia agrupa al mayor número de hacklabs que también pueden encontrarse en Londres [13], Francia [14] o Chiapas [15].

■ COMPILANDO EL KERNEL DE UN HACKLAB

Reciclar, investigar/desarrollar, discutir, cacharrear, compartir y aprender o enseñar haciendo (más que impartiendo) ... son algunos de los verbos que componen la actividad cotidiana en estos espacios. Tampoco podemos olvidar la experimentación política y reivindicativa, que es sin duda una de las características de los hacklabs (a diferencia de otros grupos de usuarios de GNU/Linux o espacios como los cibercafé). De ahí el énfasis en el funcionamiento asambleario (las decisiones se toman por acuerdo consensuado), la defensa de los ideales de GNU, la preocupación por hacer llegar los conflictos tecnológicos a la calle, la experimentación con otras formas de hacer justicia comunicativa a través de las nuevas tecnologías y la colaboración con otros



Aula con ordenadores reciclados en el Metabolik BioHacklab en el Gaztetxe de Undondo (Leioa, Bizkaia): Los ordenadores tienen instalado X-evian, una metadistribución de Debian GNU/Linux desarrollada en el propio hacklab.

movimientos sociales (centros sociales okupados, movimientos contra la guerra, contracumbres de resistencia global, etc.).

«Los hacklabs son en sí mismos experimentos, en definición constante. Más que laboratorios puramente tecnológicos nos encontramos ante comunidades sociotécnicas en las que se experimenta con las formas tecnológicas de construir sociedad»

El kernel organizativo de un hacklab, por así decirlo, se compila semanalmente en una reunión en la que se discuten los temas más importantes y los proyectos en curso del grupo; se aprovecha igualmente para realizar tareas rutinarias de mantenimiento de la red local, el servidor y el propio espacio físico. Esta reunión suele ser el momento más apropiado para acercarse a un hacklab por primera vez aunque la toma de contacto suele realizarse a menudo través de las listas de correo. Las listas de correo extienden las reuniones presenciales al ciberespacio donde wikis y blogs complementan las reuniones presenciales para coordinar el trabajo en grupo. Los canales de IRC de los hacklabs suelen activarse a menudo en momentos de emergencia o para sesiones de trabajo digital. En este aspecto la originalidad de los hacklabs reside en su naturaleza híbrida entre espacio físico y virtual, su intersección entre movimientos sociales y ciberespacio, trabajo digital y encuentro presencial.

■ TECNOLOGÍA LIBRE PARA UNA SOCIEDAD LIBRE

La preocupación por hacer llegar el potencial de las TIC a los movimientos sociales y a la sociedad de forma no mercantilista, marcan los objetivos de muchas de las reuniones en los hacklabs y, sobre todo, de los proyectos que surgen de estas. Muchos de estos proyectos están orientados a promover infraestructuras comunicativas libres y autogestionadas. En este sentido destacan las jornadas wireless organizadas por el Kaslab de Vallecas [16] o las de Metabolik en Bilbao [17]; cuando las tecnologías wifi apenas eran un espacio reservado para iniciados. Tampoco olvidemos la creación y el fomento de las redes wireless libres metropolitanas. Fruto de la estrecha relación la tecnología

wifi y los hacklabs son MadridWireless [18] o Mataró Sensefils [19]. Los hacklabs suelen ser nodos activos de estas redes además de mantener un local de libre acceso a Internet montado con ordenadores reciclados; local que sirve las veces de aula informática y espacio de trabajo. Pero lejos de aislarse en su local los miembros de estos laboratorios hacktivistas también participan montando y desmontando la infraestructura tecnológica y mediática de diversos eventos de carácter social antagonista: así el centro de medios contra la guerra en Madrid [20] o el centro de medios del primer congreso de okupación en Bilbao [21].

Otros proyectos de carácter más técnico y de desarrollo de herramientas de software libre son X-evian [22] o sinroot.net [23]. X-evian es un LiveCD basado en Debian GNU/Linux que surgió de las necesidades técnicas durante las protestas frente a las grandes cumbres. La idea era contar con una herramienta que permitiera instalar GNU/Linux en un ordenador reciclado y con todas las herramientas necesarias para la comunicación multimedia. Por otro lado el proyecto sinroot.net surgió para gestionar horizontalmente el servidor del hacklab de Vallecas; otro ejemplo interesante en el que se fusionan aspiraciones de igualdad y reto tecnológico: la supresión del poder del superusuario root en el sistema operativo de un servidor colectivo.



ASCII (Amsterdam Subversive Center for Information Interchange), uno de los primeros espacios okupados dedicado a la libre circulación de la información, el software libre y los movimientos sociales

Salir a la calle a denunciar abusos gubernamentales o corporativos relacionados con las tecnologías y la libertad de acceso a la información es quizás alguna de las acciones que más han visibilizado a los hacklabs últimamente. La idea original surgió de Kernel Panic que denominó a esta práctica *Hacking in the Streets*. Otros ejemplo incluyen acciones directas telemáticas como las de protagonizó Metabolik BioHacklab [24] durante la reunión preparatoria de la primera Cumbre Mundial de la Sociedad de la Información. Más recientemente se ha realizado en varios lugares la Operación Teddy como la que protagonizaron el Kaslab y Cielito Lindo dentro del SIMO (descargándose una canción de Teddy Bautista --presidente de la SGAE) [25]. De hecho esta última acción se enmarca dentro de una campaña de comunicación y acciones directas en favor de la libre circulación de cultura: CompartirEsBueno.Net [26]. Dicha campaña surge de la coordinación de más de una docena de hacklabs preocupados por la necesidad de salir a la calle a defender la libertad de intercambio cultural y a denunciar los abusos propagandísticos que la SGAE y el propio ministerio de cultura e industria han cometido contra los usuarios de redes p2p.

HACKLABS: UN EXPERIMENTO PERMANENTE

Los hacklabs son en sí mismos experimentos, en definición constante. Más que laboratorios puramente tecnológicos nos encontramos ante comunidades sociotécnicas en las que se experimenta con las formas tecnológicas de construir sociedad a través de wikis, redes locales y laboratorios en centros sociales, desarrollo de aplicaciones para la autogestión digital, experimentación con formas híbridas (virtuales y presenciales) de organización.

La falta de institucionalización y el rechazo a la organización jerarquizada mantiene viva la imprevisibilidad, la espontaneidad y el carácter radicalmente abierto y adaptable de los hacklabs. En contrapartida es fácil darse de brúces con espacios poco funcionales, demasiado cambiantes, reuniones poco productivas y mal organizadas y colectivos que dependen exclusivamente del esfuerzo voluntario de una o dos personas. Sin embargo algunos hacklabs siguen en pie después de varios años, sostienen proyectos de considerable envergadura y acumulan ya una experiencia enriquecedora. Si pasas por ellos encontrarás un buen ambiente de trabajo y desarrollo... de no ser así siempre estará en tus manos cambiar las cosas. Como rezan las paredes del hacklab de Vallecas (parafraseando a Eduardo Galeano): "somos lo que hacemos para cambiar lo que somos". Lo mismo sucede en la intersección tecnopolítica que define a los hacklabs ✪

REFERENCIAS

- [1] <http://hacklabs.org>
- [2] <http://scii.nl/>
- [3] <http://freaknet.org>
- [4] <http://hackmeeting.org>
- [5] <http://sindominio.net/hackmeeting>
- [6] <http://www.autistici.org/loa/web/main.html>
- [7] <http://www.ecn.org/hackit99/>
- [8] <http://kernelpanic.hacklabs.org/>
- [9] <http://sindominio.net/~hm/hmcbc00/home.html>
- [10] <http://metabolik.hacklabs.org>
- [11] <http://www.sindominio.net/wh2001/>
- [12] <http://www.sindominio.net/zgz-h1/>
- [13] <http://wiki.hacklab.org.uk/index.php/RampART>
- [14] <http://print.squat.net/>
- [15] http://www.oventhack.net/spanol/index_spa.htm
- [16] <http://kaslab.net/jornadas-wireless2003/>
- [17] http://www.sindominio.net/metabolik/jornadas_wireless_c.html
- [18] <http://madridwireless.net/>
- [19] <http://matarosensefils.net/>
- [20] <http://acp.sindominio.net/article.pl?sid=03/03/23/2043243&mode=nested>
- [21] <http://sindominio.net/~okupaziokongresua/weblog/?p=7>
- [22] <http://x-evian.org>
- [23] <http://sinroot.net>
- [24] <http://www.sindominio.net/metabolik/adt/>
- [25] <http://compartiresbueno.net/index.php/2005/11/19/compartir-es-bueno-llega-al-simo/>
- [26] <http://compartiresbueno.net>

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría orginal y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Lunes 9 de Enero del 2006

URL: <http://barandiaran.net/textos/evhack/hacklabs/>

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSION (PAL/CAR): 82/564 (entrada), 829/1270 (cuerpo), 126/1038 (ref.)

METABOLIK BioHacklab

metabolizando autonomía digital

by EVhAck

En un taller naval abandonado de la periferia bilbaína se encuentra el laboratorio hacktivista Metabolik. Casi cinco años de autogestión de las nuevas tecnologías en defensa de las libertades digitales. Allí se metabolizan proyectos como la distribución de Debian GNU/Linux hacktivista X-evian, la mediateca copyleft Alephandria o la acción directa Operación Teddy en la que, recientemente, integrantes del hacklab bilbaíno se descargaron públicamente una canción de Teddy Bautista frente a la sede de la SGAE.

DE LA INDUSTRIA DEL METAL A LA REBELIÓN DIGITAL

Bilbao quizás sea una de las ciudades que de forma más salvajemente clara ha reflejado la transformación del capitalismo industrial al cognitivo. La fábrica metalúrgica *Euskalduna* ha dado paso a los palacios de congresos y a los centros de ocio comercial, los diques portuarios al museo *Guggenheim*, los astilleros a los centros tecnológicos. Paralelamente, la conquista de derechos sociales mediante las luchas laborales de los 70 y 80 parece haberse disuelto. Lo que valía antes para los músculos no vale ahora para los cerebros. Los contratos fijos de los astilleros dan pie a contratos temporales del sector servicios, las horas extras pagadas se convierten en horas forzadas de programación nocturna, la explotación del medio ambiente es ahora explotación de la cultura, la educación pública genera analfabetismo digital.

También han cambiado las formas de resistencia y solidaridad. Un hangar abandonado cerca de la ría del Nervión, junto a la mítica industria naval vizcaína, acoge ahora un centro social okupado y autogestionado: Undondo Gaztetxea [1]. En la barra un viejo Pentium I hace sonar una selección de Punk-rock. Los jóvenes de la okupa usan el mp3blaster (un programa de música en línea de comandos de UNIX) como si fuera el Winamp. Basta subir unas escaleras para encontrarse una sala con nueve ordenadores en red, una pequeña oficina, una estantería con manuales de informática y una enorme mesa negra octogonal con un *hub* en el centro y fuentes de alimentación en cada esquina. Es el local de Metabolik BioHacklab [2], el primer laboratorio hacktivista en tierras vascongadas y una referencia en el ciberespacio euskaldun e hispanohablante.

ASAMBLEARISMO CYBORG

Hoy es jueves y se reúne la asamblea de Metabolik. Los portaáiles sobre la mesa, algo de merienda y se empiezan a discutir los puntos del orden del día entre la media docena de asistentes a la asamblea de hoy. Los *logs* de la reunión (las actas) se enviarán a la lista de correo



Aula con ordenadores reciclados en el Metabolik BioHacklab en el Gaztetxe de Undondo (Leioa, Bizkaia). Los ordenadores tienen instalado X-evian, una metadistribución de Debian GNU/Linux desarrollada en el propio hacklab.

del hacklab en cuanto termine ésta, conectando así las reuniones presenciales con los espacios virtuales del colectivo. *Asamblearismo cyborg* lo llaman: el uso de herramientas telemáticas para la transparencia y la horizontalidad en la toma de decisiones del grupo, permitiendo así la participación distribuida y virtual del resto de los integrantes, sin jefes, empleados, ni permisos de acceso.

"Somos un colectivo abierto. En las reuniones presenciales nos reunimos unas cinco o seis personas fijas y otras tantas que vienen de vez en cuando. Lo que pasa es que somos muy inestables; lo mismo viene alguien y se encuentra con una reunión de 12 personas que durante todo un mes no conseguimos reunirnos más de 3" comenta Joseba (administrador de sistemas UNIX, integrante de sindominio.net y uno de los fundadores del hacklab). "También hay muchos nómadas e intermitentes" añade Victor "que participan telemáticamente en el colectivo vía blog, correo electrónico o chat". De hecho, el chat, es una de las herramientas preferidas de los metabolikos. En el canal #metabolik de irc.freenode.net podéis encontrarlos casi a cualquier hora del día. "Aquí hay sitio para todos. Yo, por ejemplo, ya que no me veo capaz de echar una mano en temas de mucho nivel técnico, pues me ofrezco para hacer bulto en charlas" suelta Yoelu con humor, al tiempo que provoca una carcajada general entre los presentes.

HACKEANDO LAS CALLES DESDE LA BRECHA DIGITAL

Una pancarta colgada de la pared exclama silenciosamente: *Otra tecnología es posible*. "Es de la primera acción directa telemática que hicimos" explica Txopi (uno de los integrantes más veteranos del grupo) "queríamos denunciar la hipocresía de una administración que dice luchar contra la brecha digital pero va y organiza un congreso para la sociedad civil en el que la entrada costaba 700€" continúa "la conferencia inaugural la daba Hillary Clinton por videoconferencia y los asistentes eran en su mayoría grandes empresas de software monopolista y de tecnología militar". Era febrero del 2003 y los chicos de metabolik salieron a la calle con sus ordenadores, sus antenas wifi, sus pancartas y se plantaron frente al palacio Euskalduna para protestar [3] contra la reunión preparatoria de la Cumbre Mundial de la Sociedad de la información, previa publicación de la "Carta abierta a los señores del aire" [4].

Después de aquella, se han sucedido más acciones, desde el

Hacking the Streets para celebrar el primer aniversario de Indymedia EuskalHerria [5], hasta patetizar las calles en protesta por la inminente directiva europea de patentes, pasando por la reciente y celebrada descarga pública y colectiva de una canción con copyright frente de la sede de la SGAE en Bilbao [6]. "Con esta última acción" comenta Bertuco "hemos puesto en marcha una campaña de comunicación en defensa del derecho de acceso a la cultura; la idea surgió en las jornadas kopyleft.net y detrás del proyecto estamos hacklabs de todo el estado." Estas acciones se han repetido en Madrid, Barcelona, Zaragoza englobadas bajo la campaña CompartirEsBueno.Net [7].

AUTODEFENSA DIGITAL PARA TODA LA FAMILIA

No todo es acción en la calle, ni mucho menos. La mayoría de los proyectos del grupo son de carácter constructivo: dar charlas, talleres, cursos, desarrollar algo de software, reciclar ordenadores... El aula cuenta con 9 terminales de GNU/Linux. "Las terminales arrancan vía red con pxe, tirando del servidor local. De este modo podemos reciclar un ordenador viejo y hacer que tenga la funcionalidad del uno nuevo (el servidor). Es como si muchos usuarios pudieran conectarse a un mismo ordenador pero con teclado y pantalla individual" explica Moe (activista de metabolik y uno de los desarrolladores de X-evian) "eso facilita el mantenimiento de los equipos, la instalación de programas, etc. Basta con cuidar cariñosamente al servidor y las 9 terminales se portan bien". Asoma en las terminales el logotipo de X-evian [8] uno de los proyectos más exitosos del colectivo hacktivista: una distribución autoinstalable de Debian GNU/Linux, todo un sistema operativo libre al alcance de cualquiera. X-evian incluye además una selección de programas, enlaces en el navegador y toda una mediateca copyleft: Alephandria [9].

«Su próximo proyecto es montar una red inhalámbrica local en uno de los barrios más desfavorecidos de Bilbao»

Algunos miércoles, jueves o fines de semana hay cursos de informática o talleres de trabajo colectivo. El año pasado se concentraron todos los cursos durante tres meses intensivos bajo el lema "Autodefensa digital para toda la familia": un paquete conjunto de cursos que comprendían desde la introducción a internet y la iniciación a GNU/Linux hasta el desarrollo de aplicaciones con Python + GTK, pasando por clases de uso de herramientas de cifrado. "Formarnos entre nosotros de forma abierta y participativa y dar cursos a la gente que los necesita es una tarea permanente" dice Fiz "la situación actual de analfabetismo tecnológico es brutal, es difícil encontrar espacios en los que compartir conocimientos y aprender el uso de tecnologías alternativas abiertas".

Metabolik es, sin duda, uno de esos sitios, un espacio de intercambio de experiencias, conocimientos e inquietudes. Un espacio que durante los últimos 5 años ha conseguido generar una red de personas dispuestas a luchar por "una sociedad libre a través de unas tecnologías libres" y a experimentar con los usos sociales de las tecnologías, rompiendo los límites de lo impuesto y explorando siempre



Integrantes del colectivo hacktivista descargándose una canción de internet frente a la sede de la SGAE en Bilbao. Con esta acción se inauguró la campaña de comunicación CompartirEsBueno.Net en favor del derecho de acceso a la cultura. CC-by-sa 2005 Xabier Barandiaran

más allá de lo prediseñado. Su próximo proyecto es montar una red inhalámbrica local en uno de los barrios más desfavorecidos de Bilbao (San Francisco), creando así una infraestructura libre con servicios comunitarios gestionados por sus propios usuarios: una red temporalmente autónoma donde migrantes, hackers, prostitutas y movimientos sociales se encuentren haciendo de la brecha digital un espacio de nuevas oportunidades. Buena suerte. ☺

Evhack (evhack.info@gmail.com)

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre se acredeite la autoría original y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Domingo 16 de Abril del 2006

URL: <http://barandiaran.net/textos/evhack/metabolik/>

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSION: 136 palabras. 8437 caracteres

REFERENCIAS

- [1] <http://sindominio.net/udondogaztetxea>
- [2] <http://metabolik.hacklabs.org>
- [3] http://www.sindominio.net/metabolik/i4all_money4them.html
- [4] <http://www.sindominio.net/metabolik/carta/money4them.txt>
- [5] <http://euskalherria.indymedia.org/>
- [6] <http://sindominio.net/metabolik/weblog/?p=42>
- [7] <http://compartiesbueno.net>
- [8] <http://x-evian.org>
- [9] <http://metabolik.hacklabs.org/alephandria/>



CIELITO LINDO

Un HackLab enredando en Lavapiés



by EVhAck

En pleno centro de Madrid y precisamente en uno de los barrios más ricos en experiencias culturales, étnicas y políticas (Lavapiés) se encuentra el Hacklab WH2001 (también conocido como Cielito Lindo), un espacio de confluencia que saca partido de la riqueza del barrio a través diversos proyectos en los que fusionan lo técnico y lo social: desde las clases de informática para migrantes hasta talleres de telefonía por internet pasando por cursos de programación. El hacklab de Lavapiés es uno de los primeros y más activos de la península, y uno de los hogares más acogedores del hacktivismo español.

LA INTERFERENCIA PRODUCTIVA ENTRE TECNOLOGÍA Y PROYECTOS DE BARRIO

He quedado con Marga y Carolina para ver si entre las tres conseguimos reconstruir algunas de las historias y proyectos que han pasado por el hacklab WH2001 (aka Cielito Lindo) [1], uno de los primeros laboratorios hacktivistas [2] de España. Su nombre WH2001 hace alusión al hacker alemán Wau Holland, fundador del Chaos Computer Club [3], que murió precisamente en el 2001, año de fundación del hacklab. Allí confluyen, desde hace ya 5 años muchos de los experimentos sociotécnicos que atraviesan Madrid, una fuente inagotable de proyectos y un espacio de sinergias políticas y tecnológicas.

Cielito, a secas (así lo llaman sus integrantes), es un lugar pequeño pero acogedor, lleno de sofás, mesas, ordenadores y libros, acompañados de una barra de bar con la que amenizar las reuniones y mantener el alquiler. La Biblio [4], un proyecto de biblioteca popular de barrio, comparte ahora el local con el hacklab, convirtiendo el lugar en un “paraiso” del conocimiento libre. La interacción entre los dos colectivos ha dado lugar a numerosas interferencias productivas: a las clases de español de La Biblio se unen desde hace un par de años las clases de informática para migrantes (todo con software libre). Tampoco faltan cursos de python (uno de los lenguajes de programación de moda) o de Asterisk [5]

(que permite configurar centralitas libres de como telefonía por internet, también conocido voip) así como talleres de edición de video con GNU/Linux (todo un reto para Dejaví, el colectivo de videocreadores que compartió local con los hackers durante un tiempo). Fuera del horario de clases Cielito puede encontrarse abierto como espacio de acceso libre a internet y, por supuesto, para hacer hueco a todos los proyectos que, de un modo u otro, atraviesan el hacklab: Lavapiés wireless [6], la revista digital *suburbia* [7], chicas linux [8], taller de robótica, ...

UN CLUSTER DE INTELIGENCIA COLECTIVA DONDE CADA UNO TRAE LO QUE SABE

Hoy hay reunión del hacklab así que no cesa el goteo de personas que llegan desde diversas zonas de la ciudad. “Aquí cada uno trae lo que sabe y el tiempo del que dispone” explica Carolina “no hace falta ser un experto informático para formar parte del colectivo, lo importante es que la gente se acerque con ganas de compartir y trabajar en equipo”. Muchos son de Lavapiés, otros vienen desde diversas zonas de Madrid, aunque sólo unos pocos de ellos estuvieron en la reunión que se celebró en el 2001 durante el hackmeeting [9] de Leioa (Bilbao), en la que una docena de personas decidió dar comienzo a este proyecto. Eso sí, no fue hasta el multitudinario hackmeeting [10] que tuvo lugar al año siguiente, en el centro social okupado El Labo03 (también de Lavapiés) que el hacklab tomó fuerza. La red Madrid Wireless [11] estaba naciendo por aquél entonces y muchos de sus integrantes (además de otras personas) se unieron al hacklab precisamente a través de la preparación del hackmeeting. “Después entonces” comenta Marga “casi morimos de éxito, llegamos a ser más de 30 personas en las reuniones hasta que surgió el hacklab de Vallecas y después otros y empezamos a distribuir el trabajo y consolidando proyectos de barrio”.

Según seguimos charlando, alguien se levanta y cambia la música haciendo las veces de DJ en el copisterio, un rincón destinado a almacenar información a modo de mediateca digital. Allí pueden encontrarse casi todas las distros de GNU/Linux, así como gigas de música y todo tipo de material copyleft listo para ser copiado libremente. No en vano uno de los objetivos más importantes del hacklab es la lucha por la socialización del conocimiento en esta sociedad de la información en la que, más que nunca, el conocimiento es poder, “un poder injustamente distribuido y custodiado tras los muros de las patentes y el copyright” sentencia Marga. La nueva campaña inter-hacklabs (CompartirEsBueno.Net) [12] ha impulsado toda una serie de acciones en Madrid: primero fué la descarga de la canción “Get on your knees” de Teddy Bautista (presidente de la SGAE) durante el SIMO, luego el top manta copyleft durante el e-Life (un evento con el que el ayuntamiento de Madrid pretendía llenar de empresas



Entrada al HackLab Cielito Lindo. En la foto las mujeres del hacklab y otras geek internacionales que se sumaron a la reunión preparatoria del ETC (Eclectic Tech Carnival).

la brecha digital al tiempo que ponía a la policía a vigilar a los compradores del top manta); y, el pasado 5 de enero, WH2001 y el Kaslab de Vallecas [13] realizaron, en local de éstos últimos, una *sharing-party* (fiesta de intercambio de archivos) en la que, como rezaba el cartel, “lo compartimos todo” [14].

STREAMING DE VOCES MIGRANTES DESDE EL SERVIDOR LOCAL

Lo que caracteriza a Cielito como hacklab es su estrecha interacción con otros movimientos y problemas del barrio. “Uno de los proyectos con los que me siento más satisfecha” afirma Carolina “son las dos experiencias de radio con migrantes en las que software libre, nuevas tecnologías e inclusión social se dan la mano”. La primera se hizo en el contexto de la contracumbre de la sociedad de la información que tuvo lugar en Ginebra. El objetivo de la contracumbre [15] fue visibilizar esa otra sociedad de la información, que a pesar de la falta de apoyo de multinacionales y gobiernos (o precisamente gracias ella) es posible a través de la combinación de tecnologías libres y organización colaborativa. “Así que, gracias a la ayuda de las chicas de Radio PWD [16], que fueron unas pioneras en streaming de audio con GNU/Linux” sigue Marga “decidimos unirnos a la contracumbre con este proyecto”. Más de una veintena de migrantes se interesó por el proyecto y decidieron, por un día, hacer varios programas de radio en los que contar sus experiencias y transmitir su música. Una radio que se emitía por internet para ser posteriormente capturada por hacktivistas desde Ginebra y reemitida vía satélite. En el proyecto también colaboraron los locutorios de Lavapiés, sintonizando la señal para hacerla llegar a los rincones del barrio. La segunda vez que se repitió la radio se realizó previamente un taller de streaming de audio (emisión comprimida en directo por internet) para que gente de La Biblio, junto con los migrantes, pudieran gestionar la radio por sí mismos. Todo esto sucedía en el contexto del día europeo contra las fronteras, un día en el que los migrantes de Lavapiés pudieron hacer llegar sus voces más allá de las fronteras.

Nos movemos a las salas de trabajo y reunión del piso de abajo para buscar un poco de silencio. Aquí se encuentra el servidor local del hacklab (wh2001.sindominio.net) una máquina con diversos servicios (mensajería instantánea, cuentas de correo y listas, servidor web, etc.)



Chicas del hacklab Cielito Lindo en los controles de la radio libre para migrantes que emitía por internet, el servidor está montado sobre GNU/Linux.

«El hacklab Cielito Lindo es un hub, un conector de redes, conocimientos, proyectos y personas»

que usan las integrantes del hacklab y colectivos sociales del barrio. Todo ello rodeado de una red de ordenadores listos para los cursos y para el cibercafé gratuito. Los más viejos usan pxe [17] (un programa que permite convertir los equipos en terminales multiusuario de un servidor central) mientras que las máquinas más nuevas (aunque no por ello consideradas útiles por la mayoría de la gente) forma un *cluster*, optimizando recursos al compartir sus procesadores.

El hacklab Cielito Lindo es un hub, un conector de redes, conocimientos, proyectos y personas. “Para mi cielito siempre ha sido una especie de impulsador de proyectos, el espacio en sí ha hecho posible el surgimiento de muchos colectivos y procesos” dice Marga, “aunque” interrumpe Carolina “siempre queremos más”. Así que ya sabéis: wh2001.sindominio.net, C/ Santa Ana 6, Madrid, Planeta Tierra.

EVhAck (evhack.info@gmail.com)

REFERENCIAS

- [1] <http://wh2001.sindominio.net>
- [2] <http://hacklabs.org>
- [3] <http://www.ccc.de>
- [4] <http://www.sindominio.net/labiblio>
- [5] <http://www.asterisk.org/>
- [6] <http://www.lavapiéswireless.net/>
- [7] <http://sindominio.net/suburbia>
- [8] <http://chicaslinux.net>
- [9] <http://www.sindominio.net/~hm/hmleioa01/>
- [10] <http://www.sindominio.net/~hm/madhack02/madhack.html>
- [11] <http://www.madridwireless.net>
- [12] <http://compartiresbueno.net>
- [13] <http://www.kaslab.net/>
- [14] <http://compartiresbueno.net/index.php/2006/01/02/el-5-lo-compartimos TODO/>
- [15] <http://www.geneva03.org/>
- [16] <http://www.sindominio.net/radiopwd/>
- [17] <http://www.kegel.com/linux/pxe.html> <http://hacklabs.org>

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT 2006 EVhAck: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría orginal y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Lunes 4 de Febrero del 2006

URL: <http://barandiaran.net/textos/evhack/cielito/>

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.



Deal, integrante del hacklab, instalando Asterisk en el servidor para crear una centralita telefónica por internet con software libre.

VOCES ABIERTAS

streaming de radio desde la retaguardia hacktivista

by EVhAck

Las radios piratas y libres han sido, durante años, el buque insignia del mediactivismo de la contrainformación. Hoy, frente a la lucha por okupar las frecuencias analógicas del barrio, la red ofrece la posibilidad de emitir voces disidentes a todo el planeta, en tiempo real, fusionando tecnologías libres con nuevos códigos comunicativos. Entrevistamos a Radio PWD y NerdFiles, dos experiencias cercanas, tan distintas entre sí como radicales en su apuesta compartida: expandir el micrófono al teclado, compartir en vivo la experimentación técnica y dejar hablar a las experiencias de los movimientos sociales y la cultura hacker. Hoy hablan ellas, de sus servidores y sus problemas, de la vida de sus proyectos cyborg, de cómo parar la Gran Máquina y arrancar un Pentium I para empezar a escucharnos.

DE LO ANALÓGICO A LO DIGITAL: DEMOCRATIZAR LA INFRAESTRUCTURA

Durante los años 70 crecen las radios libres por toda Europa, emisiones pirata desde los movimientos sociales de base, autónomos, libertarios, ecologistas, antimilitaristas, feministas.... A pesar del coste y la escasa disponibilidad de la infraestructura necesaria para la emisión, en 1979 se contabilizan en toda Europa más de 2.500 radios de este tipo: todo un experimento de comunicación social al margen de los grandes imperios mediáticos. Su amenazador poder subversivo y la privatización salvaje del espectro radiofónico han dejado pocos supervivientes. Muchas fueron cerradas a golpe de metrayeta (como la famosa Radio Alice [1] en Bologna), otras ahogadas por la proliferación de radios comerciales.

Hoy las tecnologías de streaming (compresión y emisión en directo) de audio por internet permite un nuevo boom de la voz como vehículo de la comunicación liberada. La posibilidad de colgar los programas en la red, el alcance no limitada a un determinado radio de emisión, la multiplicidad de canales participativos (voip, chat, mail, móvil, etc.) o las grabadoras digitales a menos de 100 euros, han transformado completamente el escenario tecno-comunicativo. Surge una nueva generación de radios libres. Hablamos con dos de ellas: la pionera Radio PWD y n3rd fil3s (Nerd Files) un punto de referencia para el activismo geek y la cultura underground hacktivista.



by monkeyc.net Copyleft CC-by-nc-sa tomado de flickrs.com

DOS PROYECTOS SIN COMPLEJOS: RADIO PWD Y NERD FILES

Radio PWD [2] "surgió en una conversación con mi amiga Raquel" comenta Marga, co-fundadora del proyecto, "en la cocina de casa, cuando ella me dijo, en el año 2002, que había oido decir que montar una radio para emitir por Internet era relativamente sencillo. A mí me gustaba trastear y ella antes había participado en una radio libre. Empezamos a emitir desde el Hacklab Cielito Lindo (Madrid), con un Pentium a 110 MHz, con 16 Mb RAM, reciclado, todo con software libre". Ese mismo año Marga y Raquel deciden lo impensable: emitir la totalidad de las conferencias y talleres del Hackmeeting de Madrid por la red, extendiendo cientos de metros de cable por el Centro Social Okupado El Labo03 para hacer llegar el conocimiento hacktivista a todos los rincones del planeta. Desde entonces Radio PWD emite, con una irregularidad sin pausa, un magazine intimamente político que busca "palabras para lanzar contra el mundo hasta dejarle y dejarnos heridas de muerte".



«Cuando una se sitúa al otro lado de la emisión, rebelándose contra la tiranía de las audiencias, la percepción de la comunicación social se transforma completamente»

Josianito y Acacia forman *Nerd Files* [3], mucho más reciente (llevan cerca de un año emitiendo) pero que surge de una encrucijada parecida a la de Radio PWD: "un ensayo para potenciar la difusión de nuevos usos para la tecnología". Ubicado en Barcelona (y en todos los lugares que permite su nomadismo) Nerd Files es un caótico e imprevisible, siempre divertido, programa semanal que se concibe a sí mismo como una mezcla participativa de diferentes capas: "La emisión en directo con entrevistas y colaboradores, las entrevistas grabadas, la gente que se pasa por sorpresa, el chat, los imprevistos técnicos, los links del blog, las llamadas espontáneas vía voip para anunciar eventos, ...".

COMUNICAR DESDE EL SOFTWARE LIBRE: MUCHO MÁS QUE UN INSTRUMENTO.

En el aspecto técnico Marga y Raquel optan por un equipamiento mínimo, la sencillez y la estabilidad para evitar así que "los criterios técnicos compitan con otros" y se desvirtúe la vivencia comunicativa "tenemos un Pentium a 150 MHz, con 32 Mb RAM y emitimos en ogg



El equipo de Radio PWD durante el Hackmeeting 2002 realizado en el Centro Social Okupado Autogestionado El Laboo3. Las chicas de Radio PWD emitieron por vía streaming todas las charlas del Hackmeeting con este equipo reciclado y usando software libre (cuando las tecnologías de streaming aún eran prácticamente desconocidas). [Copyleft 2002 Precari@ barcelonaindymedia.org]

con *icecast2* e *ices* desde wh2001.sindominio.net, aunque luego convertimos a mp3 y colgamos los programas en porticoluna.org, donde hay un servidor de streaming y mucho más ancho de banda.” Nerd Files, por el contrario, pone en el centro de la experiencia de la radio el lado técnico: “Hemos convertido la parte técnica en una parte más del programa. Si algo falla, lo vamos comentando en directo mientras lo arreglamos (*it's not a bug, it's a feature!*) y los oyentes, también atentos a la parte técnica, aportan soluciones vía chat.” Emiten desde el proyecto r23.cc que cuenta con un anillo de servidores de *icecast2* y posteriormente archivan el programa en un *netjuke*. “Para la realización del programa, usamos nuestros portátiles y una pequeña mesa de sonido. Para el encodeo de audio en *ogg*, usamos un patch propio de *PureData* (un lenguaje libre de programación multimedia)”. Además Nerd Files cuenta con un Blog en el que se cuelgan las referencias del programa y usan un canal de chat “donde la participación es muchas veces más interesante que el propio programa.”

El punto de partida de ambos proyectos es el software libre, no como mero instrumento gratuito y eficaz, sino como toda una filosofía del conocimiento y la comunicación. “No me importa si tal o cual herramienta no tiene interface gráfica o carece de alguna funcionalidad (...) porque parte de la creación consiste en apañarte con eso, en partir de lo disponible. Y, desde mi punto de vista” matiza Marga “el software libre, es la tecnología que tengo disponible.”

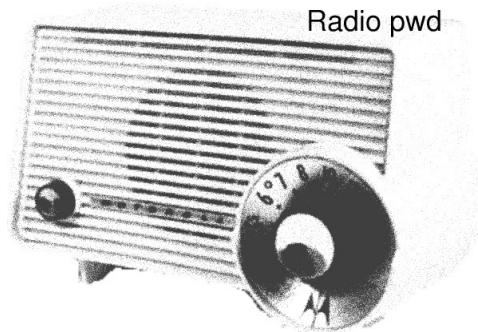
“Para nosotras la filosofía del software libre es muy importante para la realización del programa” comenta Josianito “no sólo en cuanto al software utilizado sino por la idea de que todo el mundo debería hacer su programa, todos debemos colaborar con la documentación de nuestras prácticas, abrir el código de nuestras experiencias para que sirvan de base a los demás”. Y es que la contribución a la comunidad, tanto de Nerd Files como de Radio PWD, reside también en hacer disponibles las fuentes de los programas (de software y de radio), en documentar las prácticas propias y ajenas, hacer del software libre una filosofía práctica de compartir los entresijos técnicos en los que habitamos. Así que ambas radios comparten sus trucos y archivos de configuración en la red y sus integrantes participan igualmente en la asistencia técnica y el intercambio de experiencias con otros movimientos sociales.

“LO MÁS IMPORTANTE ES LO QUE PASA DENTRO”

“¡Las audiencias no importan! ¡Lo importante es convertirse en emisor!!!” exclamaba agitadamente, durante las primeras jornadas copyleft, el filósofo y activista Franco Berardi, fundador de la mítica radio libre Alice y la reciente experiencia de televisiva pirata *TeleStreet*. En Nerd Files tienen bien claro que de lo que se trata es de darle la vuelta al sistema emisión-audiencia: “La idea de fondo que siempre hemos tenido es la de que la gente que nos escucha no sean oyentes, sino parte de los que hacen el programa.” Y es que cuando una se sitúa al otro lado de la emisión, rebelándose contra la tiranía de las audiencias, la percepción de la comunicación social se transforma completamente. “Lo más importante de radiopwd es lo que pasa dentro en Radio PWD” apunta Marga “vivimos en una época en la que las conexiones son infinitas pero el tiempo y el cuerpo son limitados ¡Hay tantas cosas que nunca podré aprender, tanta música que nunca podré escuchar, ¡Qué angustia!”. La solución es tomarse el tiempo de programar la propia emisión, desconectarse para vivir el directo, “es algo fabuloso, una hora entera sin distracciones, sin teléfono móvil.. sólo poniendo la voz, el cuerpo, tal como te salga según estés ese día, atentas al guión”. Además hacer un programa de radio permite ver el mundo de una forma diferente: “convertirse en entrevistador engancha bastante” afirma Josianito “cuando viajas o asistes a encuentros, sirve como excusa perfecta para darle algo de rigor a aquello de ¿me cuentas en qué andas trabajando ahora? Con el tiempo, te conviertes también en recogedor de links o historias, en recolector de experiencias.”

Al final de la noche, cuando termina el programa, queda lo que Marga llama “la idea en funcionamiento”, el mensaje más importante: que es posible recoger un ordenador de la basura y ponerse a hablar con la red, establecer nuevas conexiones con la voz y superar la soledad “en esta sociedad red en la que si pierdes las conexiones has perdido todo.” ☀

Evhack (evhack.info@gmail.com)



REFERENCIAS

- [1] <http://www.radioalice.org/>
- [2] <http://www.sindominio.net/radiopwd/>
- [3] <http://r23.cc/community/?q=taxonomy/term/38>

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría orginal y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.

<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Domingo 10 de Setiembre del 2006

URL: http://barandiaran.net/textos/evhack/voces_abiertas

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSIÓN: 1646 palabras, 10322 caracteres

HACK.IT:

Socializar los saberes sin fundar poderes

Desde las primeras BBS en las que el *cyberpunk* se abría paso en Italia hasta las protestas contra la globalización neoliberal del G8 en Génova, pasando por la creación de Hacklabs, Hackmeetings y servidores autónomos en la red, la historia del hacktivismo Italiano es, sin duda, una de las matrices más importantes del activismo telemático europeo. El reverso del monopolio mediático de Berlusconi es una contracultura experimentalmente política, capaz de reinventarse a sí misma cada vez que la policía llama a la puerta para proclamar que la comunicación liberada ha terminado.

by EVhAck



Socializzare i saperi, senza fondare poteri ("Socializar los saberes, sin fundar poderes"): esta frase, slogan repetido a menudo por los hacktivistas italianos, condensa el hilo de esta historia, la del *movimento hacker* italiano. En primer lugar, por su origen, el lema de Primo Moroni, histórico librero milanés de la izquierda autónoma de los años setenta. En segundo lugar por quién la retoma: los hacktivistas italianos del cambio de milenio que se reconocen en aquella herencia política del 68. Y en tercer lugar por el mismo significado de la frase, que resuena inevitablemente con el intercambio de saberes y técnicas que caracterizan al hacktivismo y el desarrollo de herramientas y servicios de software libre en aras del cambio social.

ISLAS EN LA RED: ECN, CYBERNET Y EL *ITALIAN CRACKDOWN*

El cyberpunk crecía silenciosamente en las viejas BBS del Fidonet Italiano hasta que el verano de 1992 los *Digos* (un cuerpo de policía italiano) visitaron inesperadamente al sysop de Fidonet y los canales cyberpunk desaparecieron. Éste cierre supondría un factor decisivo a la hora de empujar a las contracorrientes cyberpunk a adquirir independencia y crear su propia infraestructura. Así nació *Cybernet* [1] en el año 1993, una red abierta donde todo el mundo podía tanto leer como escribir mensajes.

Rápidamente irían tomando forma en Cybernet los canales Decoder BBS (de Milán), homónimo del fanzine underground del mismo nombre [2] y uno de los exponentes más duraderos de la escena, junto con la revista contracultural *Neural* [3] (ambas activas aún hoy día). Es en estas redes dónde podemos encontrar a conocidos ciberactivistas como Tomasso Tozzi [4] (uno de los responsables del ciberzapatismo y los netstrike) o Ferry Byte que, junto con otros ciberactivistas, monta *Strano-Network*, un espacio dedicado a los derechos digitales, la privacidad, la criptografía y la seguridad. Estos primeros años de *Cybernet* marcaron irreversiblemente la forma de entender las redes: no ya como meras e incipientes herramientas de comunicación sino como



incursiones en las fronteras del comportamiento humano, vislumbrando que cuerpos y máquinas habrían de ir de la mano en la construcción de su propio futuro: el de la sociedad de la información que estaba por llegar.

Previamente al nacimiento de *Cybernet*, ya existía la ECN: *European Counter Network - Isole nella rete* [5] (Contra Red Europea - Islas en la red). Estamos hablando nada menos que del año 1989, cuando los primeros nodos de la ECN comienzan a extenderse con el objetivo de crear una red telemática antagonista europea, una infraestructura digital para los movimientos sociales. Una posibilidad difícil de asimilar para el resto de activistas europeos que no acabaron de entender eso de las redes digitales. Así la ECN apenas superó las fronteras italianas si bien sirvió como matriz para las redes antagonistas que mucho más tarde empezaron a poblar el ciberespacio activista europeo. Estas dos iniciativas pioneras (Cybernet y ECN) marcarían los cimientos de lo que estaba por venir. Pero antes tenemos que hablar de un acontecimiento que conmocionó al, por entonces incipiente, ciberespacio italiano.

«Los primeros años de Cybernet marcaron irreversiblemente la forma de entender las redes vislumbrando que cuerpos y máquinas habrían de ir de la mano en la construcción de su propio futuro: el de la sociedad de la información que estaba por llegar.»

En 1994 sucede lo que sería conocido como el *Italian Crackdown* [6]: una fantasmagórica y enorme operación policial contra las BBS de la red Fidonet con la excusa de combatir la "piratería informática" (como vemos, hay cosas que ya vienen de lejos...). Decenas de registros y servidores secuestrados bajo las acusaciones de "asociación delictiva, contrabando, duplicación de software, violación de sistemas informáticos de terceros". A pesar de que las investigaciones concluyeron rápidamente que la red Fidonet no era utilizada para el intercambio de software "pirata", el efecto fue devastador sobre las redes *amateurs* italianas. Muchos sysop decidieron no volver a ofrecer sus servicios. La red Fidonet quedaba seriamente diezmada. El reverso de la moneda fue que, a raíz del crackdown, los *invisibles digitales* empezaron a trabajar directamente sobre Internet, dejando de lado las BBS. Surge así una nueva era de la cybercultura antagonista Italiana, de la mano de los espacios autogestionados y los encuentros presenciales.

HACKMEETING & HACKLABS, LA EXPERIENCIA ITALIANA

Ya en el periodo comprendido entre el 93 y 94 surge el que es considerado como primer laboratorio hacktivista "verde e proprio" de este planeta: el Freaknet MediaLab/Hacklab [7] en Sicilia. Por primera vez, se cruzaban las BBS, los 286, los centros sociales, la recuperación de "chatarra" electrónica, los cursos de informática y las luchas sociales... incluida la lucha contra la mafia! Poco a poco los hacklabs se extienden como la espuma por todo el territorio italiano [8], ofreciendo cursos de informática gratuitos (particularmente de GNU/Linux), libre conectividad, redes experimentales..., espacios autónomos autogestionados dónde poder experimentar, aprender y compartir conocimientos sobre la tecnología y sus usos sociales. Particularmente rica e interesante fue la historia del LOA [9] milanés, fundado en el año 1998. Un espacio en el que se entrecruzan casi la totalidad de las experiencias que se relatan en este artículo. Un laboratorio efervescente, en el que se

impartían cursos de informática todos los días del año, con un colectivo de más de 20 personas detrás, trabajando y disfrutando día y noche en los proyectos que vendrían poco después. Surge también el primer Hackmeeting [10] celebrado en el *Centro Popolare Autogestito* de Florencia el año 1998 [11]. Desde entonces cada año se irán sucediendo estos encuentros estivales entre los miembros de la comunidad italiana (e internacional) donde se intercambiarán saberes y técnicas de la cultura y la tecnología underground; inspiración de los Hackmeeting españoles y los trans-nacionales.

■ INFRAESTRUCTURA DE RESISTENCIA GLOBAL: LA RED TOMA LAS CALLES, LA POLICÍA TOMA LA RED.

El cambio de milenio trae como primera novedad el nacimiento del proyecto Investici, proyecto bicéfalo que acoge dos proyectos sobre un mismo servidor autónomo (las dos caras de una misma moneda): Autistici.org e Inventati.org [12]. El primero, más ligado a las cuestiones relacionadas con la privacidad, ofrece servicios de *remailer* y *anonymizer* (navegación y envío de correo anónimo), mientras que el segundo se dedica a dar soporte a la comunidad política alternativa y todo tipo de iniciativas hacktivistas: más de quinientas listas de correo, miles de páginas alojadas y seis mil cuentas de correo. Paralelamente nace Indymedia Italia, [13], uno de los más importantes nodos de ésta red de contrainformación surgida en Seattle apenas unos meses atrás. Estos proyectos ofrecieron la infraestructura telemática necesaria para la tremenda explosión de movilizaciones sucedida en territorio italiano entre el año 2000 y la actualidad. Autistici / Inventati y la ECN proporcionando las herramientas técnicas, cuentas y listas de correo, wikis y espacio web; los hacklabs difundiendo el conocimiento necesario para utilizar estas herramientas técnicas; e Indymedia como punto de encuentro, discusión y tablón de convocatorias de movilizaciones. Todo ello culmina en las multitudinarias protestas de julio del 2001 contra la reunión del G8 en Génova.

El régimen de *Il Cavaliere* (el, por entonces, presidente de la república italiana, Silvio Berlusconi), caracterizado por un control monopolístico de la comunicación (dueño de gran parte de la prensa escrita y de casi la totalidad de los canales de televisión) arremete contra la brecha de libertad comunicativa abierta por los hacktivistas. El arranque represivo comienza con lo que ha venido a llamarse la masacre de la Escuela Díaz (el centro de medios alternativos de la contracumbre del G8 en Génova): decenas de policías entran por la noche apaleando, en los sacos de dormir, a los hacktivistas y mediactivistas que allí dormían, destrozando los ordenadores y las cámaras de video y foto que contenían imágenes de los abusos policiales cometidos durante el día (entre ellos el del asesinato del manifestante Carlo Giuliani). Del centenar de detenidos en la Escuela Díaz, más de la mitad son llevados directamente al hospital debido a su grave estado de salud. Se sucede una oleada de protestas digitales, entre ellas un *netstrike* (una manifestación virtual) contra el sitio web del G8 agrupando a centenares de manifestantes virtuales de todo el mundo. La represión, de nuevo, no se hizo esperar: el 10 de agosto de 2001 es secuestrado el servidor www.netstrike.it y son detenidas 20 personas, creándose rápidamente decenas de *mirrors* (duplicados espejo del contenido web) por todo el mundo [14].

Pero esto no es todo, el servidor de Indymedia Italia (alojado en el Reino Unido) es también secuestrado en octubre del mismo año por parte del FBI, con un mandato judicial proveniente de Italia [15]. Más tarde, en junio del 2004, agentes de la policía postal italiana comprometen muy gravemente la

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría original y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Jueves 3 de Agosto del 2006

URL: <http://barandiaran.net/textos/evhack/hackit>

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSIÓN: 1.800 palabras, 11.573 caracteres

seguridad y la privacidad de las seis mil cuentas de correo y de las quinientas listas de Investici, con la excusa de interceptar el correo de una sola cuenta bajo sospecha. Todo esto dio pie a que, tanto la red Indymedia como el proyecto Investici (pero especialmente éste último), se reconstruyeran técnicamente desde cero; basándose en una nueva red de servidores distribuidos que hiciera mucho más difícil cualquier tipo de intervención policial o secuestro de los servidores. Siguiendo el principio de "la información quiere ser libre" y del *full-disclosure* los detalles técnicos de este blindaje antirespresivo están a disposición de todo el mundo [16].

■ REINVENTAR NUEVOS TIEMPOS

Desde finales de los 80 hasta la actualidad, el movimiento telemático y hacktivista italiano ha ido reinventándose continuamente. Sin embargo, hay que reconocer que nos encontramos hoy ante un momento de transición. Por un lado los hacklabs no se han revelado como realidades inmutables y permanentes en el tiempo; muchos han desaparecido, otros (como el LOA) se han reinventado a sí mismos (ReLoad [17]) fusionándose en lo que algunos llaman *reality hacking*: "el afán de experimentación, construcción y deconstrucción autónoma de sistemas, en este caso sociales más que computacionales o tecnológicos". Los HackMeeting Italianos tampoco pasan por su mejor momento. Quizás sea que la televisión alternativa centra ahora algunos de los experimentos sociotécnicos más interesantes (como el TeleStreet y los servidores de video ngvision.org y v2v.org). Investici se reconstruye e Indymedia Italia está absorta en preparar el material multimedia para los juicios que, próximamente, se celebrarán contra los abusos de la policía italiana durante las protestas del G8.



Nadie tiene la más mínima idea del próximo paso de esta riquísima comunidad. De lo que no cabe duda es de que todavía tiene una enorme capacidad de sorprender y de reinventarse a sí misma. El futuro no está escrito, y todavía puede darnos muchas sorpresas, *senza fondare poteri*. ☺

Evhack (evhack.info@gmail.com)

REFERENCIAS

- [1] <http://www.freaknet.org/hacklab/history/8-materiali-girati-in-rete/DECODER>
- [2] <http://www.decoder.it/index.php>
- [3] <http://www.neural.it/>
- [4] <http://www.strano.net/town/artefreeart/tozzi/tozzi.htm>
- [5] <http://www.ecn.org/index.php>
- [6] http://it.wikipedia.org/wiki/Italian_Crackdown
- [7] <http://freaknet.org/hacklab/history/>
- [8] <http://www.ecn.org/altravista/index.php?PID=47>
- [9] <http://www.autistici.org/loa/web/main.html>
- [10] <http://www.hackmeeting.org/>
- [11] <http://www.ecn.org/hackit98/>
- [12] <http://www.autistici.org>
- [13] <http://italy.indymedia.org>
- [14] <http://netstrike.ipv7.net/>
- [15] <http://www.rebellion.org/noticia.php?id=6272>
- [16] <http://dev.autistici.org/orangebook/>
- [17] <http://reload.realityhacking.org/index.php>

INDYMEDIA.ORG

La mayor red mediactivista contra la hegemonía informativa

by EVhAck

Indymedia es la red de Centros de Medios Independientes más grande del mundo. Cuenta con más de 170 nodos informativos en más de 50 países: una red libre y colaborativa de servidores de noticias que se enfrenta al reto técnico de resistir a los intentos de bloqueo y censura que los grandes poderes imponen sobre ella. Todo un proyecto media-hacktivista a escala planetaria en el que software libre, contrainformación y privacidad se unen para dar voz a los movimientos sociales.

"La red altera dramáticamente el equilibrio entre los medios de comunicación alternativos y los de las multinacionales. Basta un poco de programación y un equipamiento barato para poner en marcha una página web automatizada y viva que rivalice con las de las grandes corporaciones.". Así empieza el primer mensaje publicado en Indymedia allá por 1999 [0]. Lo que antes era algo inimaginable para los defensores de un espacio informativo libre se ha convertido en realidad. Las nuevas tecnologías han permitido el surgimiento de innumerables blogs, e-zines, boletines y comunidades alternativas de noticias. Algunas de ellas han buscado ir más allá creando centros de medios autogestionados que se sitúan en las fronteras de las luchas sociales para cortocircuitar a los medios de comunicación de masas. La mayor red de centros de medios que existe hoy en día en el mundo se llama *Independent Media Center*, más conocida como Indymedia [1]. Una red que hace suyo el lema de Jello Biafra "no odies los medios, conviértete en ellos" para abrir una brecha en el cuarto poder.

"No odies los medios, conviértete en ellos"

Indymedia [1] es una extensa red de nodos locales, cada uno de los cuales se define como un Centro de Medios Independientes (CMI). Tal y como su propio nombre sugiere, cada CMI aglutina a activistas independientes y organizaciones alternativas de la zona ofreciendo una cobertura informativa no corporativa, no jerárquica y no comercial.

Esta red de nodos sigue creciendo cada año. Tuvo su punto de partida en un primer centro de medios que se creó en Seattle en el año 1999 durante las protestas que se llevaron a cabo contra la reunión que la Organización Mundial del Comercio celebró en dicha ciudad. Indymedia nació, por tanto, gracias al movimiento de resistencia global (mal llamado antiglobalización, cuando de los que se trata es, en este caso, de globalizar la libertad de expresión de los movimientos sociales). Este vínculo sigue siendo



muy fuerte y se aprecia en la actividad frenética que se desencadena en el conjunto de la red cada vez que se celebra una contracumbre contra el G8 (que reúne a los dirigentes de los países más ricos del planeta), contra el Fondo Monetario Internacional o la Organización Mundial del Comercio así como durante las celebraciones del Foro Social Mundial [2]. Más allá de su representación en el ciberespacio, Indymedia actúa también como espacio físico y tecnológico de confluencia de periodistas y mediactivistas independientes durante las cumbres: salas con ordenadores reciclados y conexión a Internet desde la que crónicas, imágenes, archivos de audio y vídeo son enviados al ciberespacio durante las protestas.

Año tras año, se siguen sumando nuevos nodos a la red que cuenta actualmente con 170 nodos en todo el mundo, la mayoría de ellos ubicados en norteamérica (71) y Europa (46) y en menor medida en América latina (17), Asia (12) y Oceanía (12) y tan sólo cinco en África. Relacionados con el Estado español, se pueden contabilizar nueve nodos. Indymedia Barcelona [3] es el CMI más veterano de todos ya que lleva 6 años y medio activo en Internet.

También existen Indymedia Galiza [4] e Indymedia Madrid [5], aunque este último CMI ahora se encuentra en proceso de reconversión. Más recientemente, se han puesto en marcha otros nodos como Indymedia Alacant [6], Indymedia La Plana [7] e IMC Válencia [8]. Por otra parte, tenemos a Indymedia Euskal Herria [9] que cubre las noticias en el País Vasco Español y Francés. También Indymedia Canarias [10] que se localiza a sí misma en el continente africano. Por último, está Indymedia Estrecho o también llamado Indymedia Madiaq [11] que está centrado en el ámbito geopolítico del Estrecho de Gibraltar, es decir, Andalucía y Magreb.

CUANDO LA COMUNICACIÓN LIBRE MOLESTA AL FBI

Para lograr que todo el mundo pueda publicar directamente su información (noticias, fotos, entrevistas, vídeos) sin miedo a que sea manipulada o censurada, los CMIs siguen el principio de la publicación abierta [12], que no es más que un mecanismo de publicación de forma directa, sin intermediarios y sin retardos. De este modo, se asegura que los propios colectivos y periodistas independientes puedan generar las noticias desde su punto de vista y publicarlas directamente en Internet. Además, los comentarios que cualquiera puede añadir a las noticias, dan el derecho de réplica y permiten que surjan interesantes debates, que a veces son más valorados que la propia noticia original. No se trata de construir noticias pretendidamente objetivas desde la posesión de la verdad absoluta, sino de construir y mantener una serie de herramientas libres para permitir la libre publicación, traducción y comunicación, promoviendo que cada cual se forme su propia opinión. Nada más lejos de los monopolios informativos de



Manifestación en protesta por el secuestro por parte del FBI de los discos duros que alojaban varios servidores de Indymedia. Un total de un millón de noticias fueron así silenciadas sin juicio ni aviso previo.

los medios corporativos.

El incesante murmullo de voces críticas, de noticias incómodas para el poder, de fotos incriminatorias y datos reveladores hacen que los enemigos de Indymedia sean abundantes. De hecho, la vigilancia policial a los contenidos de los CMIs es muy estrecha. Los requerimientos y las amenazas (legales e ilegales) para retirar noticias especialmente reveladoras ocurren con cierta frecuencia y en ocasiones los ataques llegan a más: confiscación nocturna de máquinas por parte del gobierno Italiano, amenazas por parte de la policía para retirar contenidos en Alemania y Euskal Herria, juicio en Reino Unido por no retirar un informe con datos reveladores sobre una empresa armamentística, ... y así un largo etcétera. Quizás el ataque más grave realizado contra Indymedia es el que efectuó el FBI estadounidense en tierras inglesas en octubre de 2004. Agentes del FBI confiscaron, sin previo aviso, los discos duros de un importante servidor que contenía aplicaciones web y *mirrors* (copias de seguridad públicas que actúan como servidores espejo de los originales) de 20 CMIs que quedaron automáticamente fuera de línea. Gracias al trabajo de técnicos de todo el mundo, Indymedia Euskal Herria pudo recuperarse en tan solo 2 horas, pero Indymedia Galiza y otros muchos nodos quedaron mudos durante largo tiempo. El trabajo de reconstrucción y realojamiento fue arduo y ha provocado un replanteamiento de la organización técnica de los sistemas de almacenamiento de datos y distribución de servidores en busca de arquitecturas más difíciles de silenciar.

UNA ARQUITECTURA LIBRE Y DISTRIBUIDA

A pesar de la relativa independencia de cada nodo, a nivel técnico existe una gran comunidad de hackers voluntarios de diversos países que colaboran mutuamente para mantener las diferentes máquinas y ayudarse entre ellos en la administración de sistemas, bases de datos y programación. Tanto los técnicos, como los editores y traductores utilizan listas de correo electrónico [13], servidores de *chat* [14] y *wikis* [15] para elaborar las noticias y tomar decisiones. Cada CMI tiene al menos una lista de correo, aunque existen otras muchas listas y recursos globales para tratar temas transversales como los legales, financieros, técnicos, lingüísticos, multimedia, etc.

En cuanto al software utilizado, la apuesta de Indymedia es la del software libre. No podría ser de otro modo ya que sólo el software modificable de código abierto ofrece garantías de seguridad suficientes para proteger la identidad de las usuarias y asegura la ausencia de puertas traseras. Igualmente el software libre permite la transparencia tecnológica necesaria para gestionar los servidores sin jerarquías, de forma colaborativa y sin dependencias técnicas o económicas. Es por ello que la inmensa mayoría de los CMIs corren sobre plataformas GNU/Linux con Apache, PHP, Perl, Tomcat, MySQL y/o PostgreSQL y ejecutan aplicaciones web con licencias libres. Algunos de estos programas (los que gestionan directamente la publicación de noticias) son conocidos gestores de contenidos como Spip [16] o Drupal [17] con retoques o extensiones para adaptarse a los requerimientos estructurales y funcionales de los nodos de Indymedia. Pero lo más interesante de esta red es que la mayoría funciona con aplicaciones desarrolladas específicamente por y para Indymedia: así los servidores de noticias ActiveSF [18], MIR [19] o dadaIMC [20].

REFERENCIAS

- [0] <http://seattle.indymedia.org/en/1999/11/2.shtml>
- [1] <http://www.indymedia.org>
- [2] <http://www.forumsocialmundial.org.br>
- [3] <http://barcelona.indymedia.org>
- [4] <http://galiza.indymedia.org>
- [5] <http://madrid.indymedia.org>
- [6] <http://alacant.indymedia.org>
- [7] <http://laplana.indymedia.org>
- [8] <http://valencia.indymedia.org>
- [9] <http://euskalherria.indymedia.org>
- [10] <http://canarias.indymedia.org>
- [11] <http://estrecho.indymedia.org>
- [12] <http://lists.indymedia.org>
- [13] <http://chat.indymedia.org>
- [14] <http://docs.indymedia.org>
- [15] <http://spipindy.medianice.org>
- [17] <http://drupal.org/node/56591>
- [18] <http://sfad.indymedia.org/news/2003/07/7.php?l=es>
- [19] <http://mir.indymedia.org>
- [20] <http://www.dadaimc.org>
- [21] <http://www.securityfocus.com/infocus/1673>
- [22] <http://en.wikipedia.org/wiki/Friend-to-friend>

La distribución de los servidores es muy compleja y varía en función de las capacidades de cada CMI. Existen grandes servidores exclusivamente dedicados a alojar varios CMIs en diversos lugares del planeta pero la red se sostiene también sobre servidores que no pertenecen directamente a Indymedia sino que están compartidos con proyectos y colectivos afines. En general, pero sobre todo en el caso de los países menos respetuosos con la libertad de expresión, se procura alojar los servidores de cada nodo en continentes diferentes a los de su localización geográfica para dificultar los arrestos de colaboradores y el secuestro de máquinas. Además, en los últimos años, cada vez más activistas particulares están alojando *mirrors* en sus servidores caseros, a los que se accede gracias a un anillo de DNSs. Esta red de *mirrors* permite un mayor reparto del ancho de banda y una mayor robustez frente a fallos técnicos o intervenciones policiales.

DEFENDER EL MEDIO, DEFENDER EL MENSAJE

Debido al peligro de represalias contra los participantes y recursos tecnológicos de los CMIs, se empieza a extender el uso de tecnologías para evitar o dificultar estos ataques. Ejemplos de esto son los *mirrors* que muchos nodos tienen, las copias de seguridad separadas geográficamente, el uso de sistemas de ficheros cifrados [21] para proteger los datos incluso si se confisan los discos duros, etc. Para proteger a los colaboradores que leen o publican material, la política de Indymedia es no guardar *logs* (registros de acceso) en los servidores web. Además los programas permiten conectarse por HTTPS (una forma cifrada del protocolo de navegación de la red) para que no sea posible saber qué información visualiza o publica cada persona. Lo mismo ocurre con los *wikis* y otros servicios web complementarios. Los servidores de *chat* también pueden ser accedidos mediante cifrado y existe documentación en multitud de idiomas para ayudar a los editores y demás colaboradores a configurar correctamente los programas correspondientes.

«La red altera dramáticamente el equilibrio entre los medios de comunicación alternativos y los de las multinacionales. Basta un poco de programación y un equipamiento barato para poner en marcha una página web automatizada y viva que rivalice con las de las grandes corporaciones»

Pero desde el secuestro de discos duros que realizó el FBI, los técnicos están buscando formas de lograr aún mayores niveles de seguridad. Es por ello que en las listas técnicas se está empezando a estudiar la posibilidad de utilizar redes *friend-to-friend* [22] (análogas a las *peer-to-peer*) que permitan dificultar al máximo la censura de la información publicada en Indymedia.

Ya lo decía el visionario Marshall McLuhan, que “el medio es el mensaje”, y en el caso de Indymedia el mensaje (el medio) es claro: construir y defender una red informativa independiente, participativa y segura; unir en el esfuerzo a hacktivistas y mediactivista de todo el planeta para globalizar la comunicación liberada. ☀

Evhack (evhack.info@gmail.com)

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-NoComercial-CompartirlGual 2.5Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando sea sin ánimo de lucro, se acredite la autoría original y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-nc/2.5/es/legalcode.es>

VERSIÓN: versión 11 del Jueves 4 de Mayo de 2006

URL: <http://barandiaran.net/textos/evhack/indymedia/>

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSIÓN: 2108 palabras, 13629 caracteres.

TAZ 2.0: servidores autónomos e infraestructura global de los pueblos (parte I)

by EVhAck

Del 19 de agosto al 3 de septiembre, cinco ciudades francesas acogieron la conferencia bianual del la AGP [1]. La AGP (Acción Global de los Pueblos) es una plataforma de coordinación de múltiples colectivos de base que se oponen a la globalización destructiva optando por la acción directa y por la construcción de redes de cooperación solidaria. Una de las ciudades francesas de acogida ha sido Dijón, sede de pRINT! [2], el primer hacklab francés alojado en el Centro Social Okupado y Autogestionado (CSOA) *Les Tanneries*. Allí se han reunido, durante una semana, hacktivistas de todo el mundo en el bloque de "Luchas Digitales" de la AGP para debatir protocolos de seguridad y solidaridad frente a la represión digital, intercambiando recursos y experiencias. Una oportunidad inmejorable para echar un vistazo a la tecno-diversidad del ciberespacio alternativo y explorar qué son y cómo funcionan los servidores autónomos.



TAZ, siglas en inglés de Zona Temporalmente Autónoma, un concepto creado por Hakim Bey, uno de los poetas de la red, que en 1991 preconizó el surgimiento de experimentos sociales en la red, precursores de una "revolución" invisible capaz de crear nuevos espacios de libertad y creatividad permanente. Hoy muchos servidores de Internet se consideran TAZ, ofrecen servicios gratuitos y gestionados por sus propios usuarios, libres de la tiranía de las multinacionales. [By Sporkist, bajo licencia CC-by, tomado de Flickr.com]

debería ser la red.

La mayoría de los servicios reales de la red los controlan las grandes multinacionales que explotan a las comunidades virtuales de usuarios como si fueran granjas-fábrica de animales culturales, ordeñando nuestros datos comunicativos para mejorar sus ventas y aumentar sus beneficios¹. Pero aún existen lugares en la red que permanecen libres, donde cada uno aporta lo que económicamente y técnicamente puede, espacios en los que administrar colectivamente las máquinas que sostienen nuestra comunicación y nuestro conocimiento; son los *servidores autónomos* de la red, las comunidades que los crean y los habitan. Surgen del deseo de generar en el ciberespacio las experiencias comunitarias vividas fuera de él, del afán de experimentar libremente con las posibilidades comunicativas de las TIC (Tecnologías de la Información y la Comunicación), de conectar protestas y coordinar ciclos de resistencia dentro y fuera de la red.

ZONAS TEMPORALMENTE AUTÓNOMAS

En 1991 Hakim Bey, autodenominado anarquista ontológico y terrorista poético, publicó TAZ [3] (siglas en inglés de Zona Temporalmente Autónoma), uno de los escritos con mayor influencia en la cibercultura rebelde. En él se vislumbra una forma de producir libertad política por debajo del idealizado momento insurreccional y el sacrificio revolucionario. Se trata de crear espacios gobernados por sus propios principios, evitando la confrontación directa para crear brechas de creatividad y solidaridad imprevisibles, imposibles de cartografiar, siempre dinámicos y capaces de crear a partir del caos comunicativo nuevas realidades sociales.

El por entonces casi desconocido ciberespacio sugería la posibilidad, casi ilimitada, de crear y recombinar estas "islas en la red". Años más tarde, algunos servidores de Internet comenzaron a autodenominarse Zonas Temporalmente Autónomas: experimentos de gestión distribuida y horizontal de recursos técnicos, conocimientos e información. Claro que cuando Hakim Bey escribía TAZ el ciberespacio apenas contaba con las BBS, algunos grupos de *phreaking* y un uso limitado del correo electrónico. No hace falta decir que las cosas han cambiado significativamente. Donde antes campaban tribus nómadas de hackers hambrientos de caza y recolección de conocimiento hoy se alzan edificios corporativos repletos de centros comerciales de Microsoft, multicines del consumo de bits y un cibercontrol gubernamental sin precedentes del espacio público y común que

WE ARE EVERYWHERE

"Estamos en todas partes" es uno de los lemas de la AGP; desde Alemania hasta Méjico pasando por Australia e Italia, Canadá o Francia, la diversidad de servidores autónomos es una de sus riquezas. Entre ellos, riseup.net es uno de los más conocidos, con más de 20.000 cuentas de correo y cerca de un millón de personas suscritas a sus listas de correo; 12 servidores en marcha para mantener comunicados a los pueblos en la aldea global. Afincado en Seattle, Riseup es más que un servidor de cuentas de correo y hosting para webs alternativas: manuales de uso, documentación sobre seguridad y ayudas para el uso de software colaborativo conforman un espacio sociotécnico cuyo "propósito es ayudar en la creación de una sociedad libre". Si, como dice el manifiesto del servidor australiano cat.org.au (que nace de las okupas australianas), "la información es poder", su gestión horizontal sin jerarquías ni censuras es una condición previa para crear esa sociedad libre. Una sociedad donde la tercera revolución industrial (la telemática) exige "poner en el centro del juego a la comunicación" como dicen los compañeros de

¹ Basta echarle un vistazo a los términos del contrato para los servicios MSN spaces "usted autoriza a Microsoft a (1) usar, copiar, distribuir, transmitir, mostrar públicamente, ejecutar públicamente, reproducir, editar, modificar, traducir y cambiar el formato de su Envío, siempre en relación con los Sitios Web de MSN y (2) sublicenciar estos derechos, en la medida de lo permitido por la ley aplicable. Microsoft no le pagará a usted nada por su Envío. Microsoft podrá eliminar su Envío en cualquier momento."

la red italiana ecn.org (European Counter Network), una de las pioneras en Europa. Junto a ella creció también nadir.org en 1995, creada por miembros del Caos Computer Club y parte del movimiento antifascista alemán. Al igual que muchos otros servidores autónomos, los hackers que administran Nadir han desarrollado también herramientas de comunicación horizontal para no-expertos: es el caso de la plataforma de publicación abierta MIR que usan muchos servidores de indymedia.org (la red de contrainformación más grande del planeta, con más de 150 nodos distribuidos por los 5 continentes)².

«*Aún existen lugares en la red que permanecen libres, donde cada uno aporta lo que económicamente y técnicamente puede, espacios en los que administrar colectivamente las máquinas que sostienen nuestra comunicación y nuestro conocimiento»*

Otro de los clásicos pioneros es tao.org (The Anarchist Organization, ahora rebautizado como OAT: Organización para la Autonomía de las Telecomunicaciones) hermanado con interactivist.net, un servidor autónomo situado en el hacklab de la okupa ABC No Rio de Nueva York. Interactivist mantiene un portal de noticias junto con Autonomedia (la editorial neoyorquina que publicó originalmente la obra de Hakim Bey). La página principal de muchos servidores autónomos hace de portal en el que visibilizar las novedades de los colectivos alojados. Es el caso de nodo50.org que aloja hoy recursos digitales para más de mil organizaciones hispanohablantes.

Pero no se trata sólo de “asistir” a los movimientos sociales en sus necesidades digitales, sino de romper las relaciones cliente-servidor que caracterizan el consumo tecnológico, romper la brecha digital que separa a expertos y analfabetos digitales reproduciendo asimetrías de poder en las políticas de la comunicación. Con esta idea surgió sindominio.net, un servidor de habla hispana que “apuesta por la inteligencia colectiva” y por crear un espacio “de recomposición de vínculos sociales a través del aprendizaje recíproco y de la libre circulación del saber”. En SinDominio se inspiró espora.org para recrear un experimento similar en territorio Mexicano. En ambos proyectos se dan cita diversos movimientos sociales para aprender conjuntamente a administrar el servidor, conscientes de que las decisiones técnicas son también y, sobre todo, decisiones políticas. Por eso el software libre, que permite un aprendizaje transparente, un acceso gratuito al software y la posibilidad de modificación y desarrollo sin dependencias, es una apuesta común de todos los servidores autónomos.

Sin embargo, a pesar de las oportunidades que brinda el software libre, no resulta fácil que las usuarias administren colectivamente un servidor sin privilegios y sin centralizar tareas. Para ello boum.org (un servidor autónomo francés que aloja unas 3.500 cuentas de correo) ha creado una herramienta de administración colectiva llamada *metche*. Metche envía un email a la lista de administradoras de la máquina cada vez que se realiza un cambio importante de configuración, instalación, etc., con lo que todas las administradoras pueden aprender de lo que hacen las demás, corregir y coordinar la gestión del servidor. Además, *metche* guarda un historial de cambios para poder deshacer entuertos. La probabilidad de que un cambio inexperto o descuidado comprometa la seguridad y estabilidad del servidor se reduce a través de un protocolo: al principio el cambio funcionará en



Entrada del Centro Social Okupado y Autogestionado Les Tannerries, Dijón, Francia. Sede del primer HackLab Francés, pRINT!, que acogió el bloque de “luchas digitales” de la conferencia bianual AGP. Allí se dieron cita a finales de Agosto hacktivistas de todo el mundo para debatir los problemas y oportunidades que afectan a los servidores autónomos en la red.

modo *unstable* (con la posibilidad de volver a la configuración anterior automáticamente), si el cambio funciona al cabo de un día pasa a estado *testing* y finalmente, pasados 3 días, si ningún administrador se opone, se ejecuta definitivamente el cambio y se convierte en *stable*.

Tampoco es fácil mantener económicamente la infraestructura y la conexión de las máquinas. La mayoría de los servidores autónomos funciona en base a donaciones y/o cuotas voluntarias (que pagan los usuarios dependiendo de sus posibilidades). Unos pocos ofrecen además servicios comerciales con cuyos beneficios cubren los costos del servidor. Finalmente, algunos colectivos de administradores y programadores se han organizado en forma de cooperativas de economía participativa. Es el caso de koumbit.org, situado en Montreal, que además de alojar a activistas es un colectivo de 20 profesionales que viven del software libre y desarrollan, entre otras cosas, un módulo de Drupal para facilitar la toma de decisiones colectivamente: decisions.gnuvernance.org.

¿Pueden los servidores autónomos considerarse tales si dependen en última instancia de que las grandes corporaciones corten sus cables de conexión a Internet? ¿Cómo organizarse para generar servicios seguros que no sean vulnerables a la intervención policial y al espionaje? ¿Cómo afectan las nuevas tecnologías web 2.0 a las formas de socialización digital y comunicación que buscan estas Zonas Temporalmente Autónomas? En la siguiente entrega analizaremos éstas cuestiones para descubrir que la creatividad social autoorganizada nunca dejará de sorprendernos.♦

Evhack (evhack.info@gmail.com)

METAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría orginal y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Martes 5 de Setiembre del 2006

URL: http://barandiaran.net/textos/evhack/servidores_autonomos

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSION: 1808 palabras 12096 caracteres

REFERENCIAS

- [1] <http://pgaconference.org>
- [2] <http://print.squat.net>
- [3] <http://biblioweb.sindominio.net/telematica/taz.html>

² A partir del desarrollo original otros hacktivistas (no directamente vinculados a Nadir) retomaron la labor de mantener y desarrollar MIR.

TAZ 2.0:

servidores autónomos e infraestructura global de los pueblos (parte II)

by EVhAck

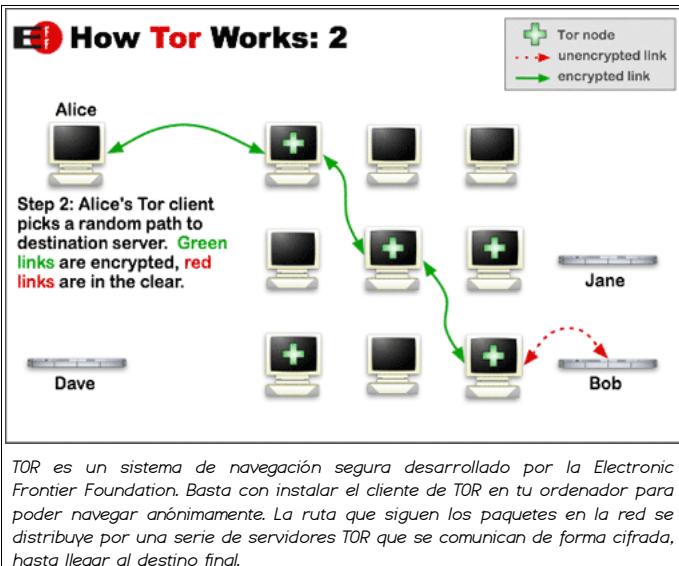
En la primera parte explicamos cómo surgen en la red colectivos y asociaciones que gestionan sus máquinas independientemente de las grandes multinacionales de las telecomunicaciones, ofreciendo servicios de forma gratuita a ONGs y movimientos sociales: Zonas Temporalmente Autónomas de libertad digital. Queda por ver cómo algunas iniciativas van más allá y buscan independizarse de la infraestructura más básica de la red, protegen sus servidores con sofisticados sistemas distribuidos y cifrados o se lanzan a reflexionar y desarrollar software social para la democracia directa en la red.

CORTAR LOS CABLES: HACIA UNA INFRAESTRUCTURA LIBRE

Hace tiempo que el ciberspacio ya no es un lugar necesariamente subversivo, nada tiene que ver la Internet de hoy con las antiguas BBS gestionadas en ordenadores caseros y conectadas por llamadas telefónicas locales. Nadie duda de que es posible (e incluso divertido) montar un servidor casero con una conexión ADSL a 30€ mensuales, tampoco cabe dudar de que no servirá de nada en cuanto un número mayor de 20 usuarios intente conectarse simultáneamente, mamá decida apagar el ordenador o cuando la policía china considere que algo en ese disco duro resulta molesto para el régimen.

«Si los servidores autónomos difunden el uso del cliente TOR y se convierten en servidores de este protocolo, podrá generarse fácilmente toda una red de "servicios autónomos" que preserve el anonimato y la libertad.»

A pesar de la gestión colectiva, la posesión de las máquinas y los diversos protocolos de seguridad que puedan implantarse, la red depende, en última instancia, de las grandes operadoras de telecomunicaciones. Quien tiene el poder de cortar el cable tiene el poder último. Por eso algunos servidores autónomos se han lanzado a la aventura de ir más allá de tener un servidor en un *data center* (hoteles de servidores y acceso a Internet de gran ancho de banda que almacenan máquinas de diversas empresas y asociaciones). El proyecto *communitycolo.net* o *CCCP* (Californian Community Colocation Project) alberga servidores ofreciendo garantías de seguridad y privacidad de forma gratuita, y aloja ya a más de 130 servidores desde 2001. Iniciativas paralelas han surgido en Seattle, Chicago, Toronto,



TOR es un sistema de navegación segura desarrollado por la Electronic Frontier Foundation. Basta con instalar el cliente de TOR en tu ordenador para poder navegar anónimamente. La ruta que siguen los paquetes en la red se distribuye por una serie de servidores TOR que se comunican de forma cifrada, hasta llegar al destino final.

Washington o Nueva York. Gitoyen.net es un proyecto francés más ambicioso aún, que ha conseguido ya generar una infraestructura ciudadana (sin ánimo de lucro) de Internet, convirtiéndose en todo un operador de telecomunicaciones: data centers, POPs, puntos de intercambio de información (como pouix.net) y enlaces de pares entre redes (con otras 124 redes). Gitoyen está compuesto por tres organizaciones sin ánimo de lucro, globenet.net (otro servidor autónomo francés), fdn.fr, y gandi.net (un registrador de dominio a precio de coste) y tres empresas (AlternB, Cursys y Netaktiv).

Otro proyecto que merece una mención especial es free.de. Surge en Düsseldorf (Alemania) en 1991 para coordinar algunas protestas contra la guerra del golfo, ofreciendo direcciones de correo y servidores de noticias. Junto al FREE! Internet café se convierte pronto en toda una referencia de la gestión alternativa de las TIC. Poco a poco termina siendo toda una ISP (proveedor de servicios de Internet) que ofrece conexión vía telefónica y gestiona varias cabinas de servidores desde un espacio autogestionado. En la actualidad Free! es también una red libre local que conecta espacios okupados y otros colectivos activistas. Sin duda las redes wireless permiten pensar en una verdadera alternativa al control corporativo de la infraestructura de Internet; si no hay cable, nadie puede cortarlo, nadie ostenta el poder de controlar la comunicación. De hecho, Gitoyen ya a empezado a usar conexiones *wimax* (última generación wireless de larga distancia) para aumentar su independencia. Mucho más cercano y modesto, pero no por ello menos interesante, es la cooperativa barcelonesa XarxaSenseFils [1], también presente en la reunión de la AGP. Esta iniciativa ha creado ya una red de nodos wifi con acceso a Internet que cubre gran parte de la capital catalana, ofreciendo acceso gratuito a la red (de pago para salida a Internet sólo para usuarios privados).

R* DE RETENCIÓN DE DATOS O ... DE RESISTENCIA?

La seguridad y la privacidad de la información contenida en estos servidores fue uno de los temas centrales de la reunión de la AGP. Muchos han sufrido los secuestros de sus servidores por parte del FBI o de la policía local, otros intrusiones que ponen en peligro la privacidad de sus habitantes. Con el objetivo de resolver algunos de estos problemas surgió el proyecto R* del servidor italiano *autistici.org*. R* de Resistant & Resilient (resistente y fluido), surgió como respuesta a la intrusión de la policía italiana en el servidor durante todo un año

(intrusión que se realizó accediendo al proveedor de acceso y desconectando la máquina). Hasta su implantación, R* se ha mantenido en secreto pero existe ahora una documentación pública disponible de cómo montar este sistema de seguridad. R* consiste en un anillo de servidores conectados a través de una *VPN* (una red privada virtual) donde los datos de las usuarias están cifrados y distribuidos entre todos los servidores cuyos discos duros están particionados y cifrados debidamente. Una base de datos LDAP contiene los datos de los usuarios replicados en cada uno de los servidores, evitando así que el secuestro de uno de ellos haga caer la funcionalidad del anillo. Los hackers de Autistici han tenido que desarrollar también software para administrar todo el sistema que ya está en marcha (con servidores distribuidos por todo el planeta) gestionando sus más de 5.000 cuentas de correo, páginas web, anonimizadores y *remailers*.

Lo que más preocupa en estos momentos es, sin duda, la ley de retención de datos aprobada recientemente en el parlamento europeo. Esta ley exige a todos los ISP y, potencialmente, a los servidores autónomos, mantener guardados los datos de acceso al servidor. Esto implica, para empezar, una importantísima merma de la intimidad y la privacidad de los millones de internautas europeos y también hace peligrar en la práctica la libertad de expresión de otras tantas personas de todo el mundo. Para cada vez más hacktivistas, la solución a corto plazo contra este recorte de libertades, pasa por la red de anonimizadores TOR [2]: un software impulsado por la *Electronic Frontier Foundation* y que permite navegar la red de forma segura. Además los servidores de TOR pueden ofrecer "varias clases de servicios tales como publicación web o un servidor de mensajería instantánea". Si los servidores autónomos difunden el uso del cliente TOR y se convierten en servidores de este protocolo, podrá generarse fácilmente toda una red de "servicios autónomos" que preserve el anonimato y la libertad. En combinación con los *remailers* anónimos de correo electrónico de tercera generación (como Mixminion[3]), la adopción de este tipo de sistemas de cifrado y seguridad permitiría hablar del surgimiento de una nueva era para las "islas en la red".

SERVIDORES AUTÓNOMOS 2.0

Durante el bloque de "luchas digitales" el único tema de discusión no fue la seguridad, la solidaridad entre servidores o los programas de administración colectiva. La moda de la Web 2.0 marcó un punto importante de reflexión. Los hábitos de comunicación están cambiando en la red. Los foros de noticias se están atomizando en blogs individuales y las redes sociales están creciendo gracias a tecnologías específicas como las sindicación de contenidos usando *tags* o anillos de confianza y afinidad. Algunos servidores autónomos han empezado a crear comunidades virtuales gracias a estas tecnologías. Es el caso de SinDominio que ha instalado su propio servidor de blogs [4].



Una torre de servidores montada en un garaje. Muchas de las webs que visitamos en la red no dependen de grandes multinacionales de las telecomunicaciones o grandes instituciones universitarias. Luchar por una infraestructura de telecomunicaciones independiente, gestionada por los propios ciudadanos en una de las labores de muchos hacktivistas. [Foto de Skippy13 con licencia CC-by-sa, tomada de Flickr.com]

REFERENCIAS

- [1] <http://xsf-coop.net>
- [2] <http://tor.eff.org>
- [3] <http://mixminion.net>
- [4] <http://blog.sindominio.net>
- [5] <http://cats.revolt.org>

Empiezan también a discutirse modelos de comunicación colaborativa para una posible Indymedia 2.0, que permita a los lectores filtrar las noticias de acuerdo con su afinidad con otras usuarias o en base a criterios temáticos abiertos y colaborativos. Reprogramar los servidores de noticias de Indymedia en *Ruby on Rails* (una tecnología de diseño web de nueva generación) permitiría además unificar la administración e instalación de nodos de Indymedia y centralizar los esfuerzos de desarrollo.

Pero la discusión y las posibilidades van más allá. CATs [5], un colectivo de desarrolladores de software anarquistas norteamericanos, está desarrollando una plataforma de comunicación, coordinación y toma de decisiones llamada *Crabgrass*. Las usuarias podrán asociarse en colectivos (además de las redes sociales que surgirán del mapeo automático de sus comunicaciones en el servidor). Los foros no sólo implementarán la posibilidad de discutir temas sino de tomar decisiones a través de diversos métodos y técnicas de democracia directa (desde la votación simple al consenso no excluyente). Los envíos de noticias se podrán etiquetar, sindicar y cada usuaria podrá consultar las últimas noticias directamente relacionadas con sus temas de

intereses o con el colectivo al que pertenece. Además dentro de cada colectivo podrán asignarse diversos roles y adaptar igualmente sus espacios personales a las noticias relacionadas con su rol (por ejemplo si cumples la función de tesorero dentro de una ONG recibirás noticias

directamente relacionadas con formas de administración o subvención). Finalmente incluirá módulos de *groupware* (software para coordinar la acción y planificación en grupos) como fechas de reuniones, tareas pendientes, etc. Todo ello con las medidas de seguridad centralizadas en el servidor al que poder acceder vía TOR para garantizar la privacidad.

Más coordinación, más solidaridad, mayor seguridad y privacidad, mayor independencia de las multinacionales y nuevas oportunidades tecnológicas. Son los temas que se trataron en la reunión de hacktivistas de todo el mundo que tuvo lugar en el HackLab pRiNt! de Dijón (Francia) en el que las TAZ (Zonas Temporalmente Autónomas en la red) se dieron cita para redefinir su futuro. Todo ello para coordinar, informar y crear espacios para el cambio social, herramientas y recursos libres y adaptados a las necesidades de la democracia directa. Las TAZ 2.0 están en camino, para quedarse.✿

Evhack (evhack.info@gmail.com)

MAETAINFORMACIÓN DEL DOCUMENTO

COPYLEFT: Creative Commons Atribución-CompartirIgual 2.5: Se permite la copia, distribución, reproducción, préstamos y modificación total o parcial de este texto por cualquier medio, siempre y cuando se acredeite la autoría original y la obra resultante se distribuya bajo los términos de una licencia idéntica a esta.
<http://creativecommons.org/licenses/by-sa/2.5/es/legalcode.es>

VERSIÓN: versión 1.1 del Martes 5 de Setiembre del 2006

URL: http://barandiaran.net/textos/evhack/servidores_autonomos

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSION: 1970 palabras, 12861 caracteres