

V. El compromís polític a la xarxa: de l'activisme artístic al hacktivisme

1. Hackers, crackers, phreakers, lamers, carders

Diuen les cròniques que, en els anys 60, pels passadissos de les universitats americanes s'hi podien trobar dos grups de joves amb cabell llarg i jeans, que fumaven "maria" i volien canviar el món: eren els hippies i els geeks¹. Els hippies ens han deixat cançons, consignes com "fes l'amor i no la guerra" i un misticisme d'arrels orientals, mentre que els geeks varen crear el full de càlcul, el processador de textos i el correu electrònic. Al voltant dels ordinadors i les xarxes analògiques o digitals es varen anar configurant diverses subcultures, com els phreakers², ciberpunks³, crackers⁴, hackers⁵, sneackers⁶, wizards⁷, nerds⁸, bems⁹, geeks¹⁰. L'ambient hippie dels campus universitaris i la revolta estudiantil de 1968 varen tenir la seva influència en els hackers i els geeks que van fer seves les idees de propietat comunal, de llibertat informacional, i de compartir la recerca i els resultats; aquesta cultura del lliure intercanvi d'idees, pròpia també de la recerca científica, s'expressa actualment amb el moviment de l'open source i software lliure (freeware i shareware). Arran l'expansió dels ordinadors a partir dels 70 la paraula geek va quedar restringida als fanàtics dels ordinadors i la de hackers als experts en programació.

"Els *hackers* i la seva cultura són una de les fonts essencials de la invenció i desenvolupament continu d'Internet. Els *hackers* no són el que els mitjans de comunicació o els governs diuen que són. Són, simplement, persones amb coneixements tècnics informàtics la passió de les quals és inventar programes i

¹ The code of the geeks <http://www.mit.edu:8001/afs/sipb.mit.edu/user/rei/Docs/HTML/GeekCode.html>

² Experts en sistemes de telefonia i usos il·legals de la comunicació via telèfon. El seu origen es troba en el moment que algú va "descobrir" que un xiulet que es regalava amb els cereals "Capità Crunch" reproduïa el to exacte dels tons de control dels sistemes telefònics (2600 HZ) i xiulant una seqüència exacta de tons es podien fer diverses accions.

³ Nom que prové de la novel·la *Neuromante* de William Gibson, i que a la comunitat hacker es fa servir per a referir-se als mags de la criptografia.

⁴ Persona que trenca la seguretat en un sistema. El terme va ser creat per la comunitat hacker per a defensar-se contra el mal ús periodístic de la paraula hacker i reflecteix el refús dels vells hackers al vandalisme cracker. Alguns hackers passen per aquesta etapa però la deixen en convertir-se en hackers.

⁵ És un programador expert i entusiasta. En algun moment s'ha arribat a distingir el hacker de barret blanc (administrador de sistemes o expert de seguretat que fa servir els seus coneixements per a evitar activitats il·lícites), el hacker de barret negre (també anomenats crackers, que frueix penetrant en els sistemes de seguretat i crear software perniciosos –"malware") i el hacker de barret gris (no preocupat per l'ètica sinó per fer el seu treball, i si necessita penetrar en un sistema ho fa i frueix posant-se reptes contra els sistemes de seguretat, sense malícia, compartint els coneixements, cosa que permet millorar la seguretat dels sistemes).

⁶ Hacker contractat per a intentar penetrar en un sistema per a provar-ne la seguretat.

⁷ Persona que coneix a fons com funciona una peça complexa d'equip, i pot reparar un sistema ràpidament en casos d'emergència utilitzant instruccions o tècniques totalment incomprensibles per al comú dels mortals. Mentre que el hacker utilitza tècniques avançades, és el wizard qui entén com i per què funcionen.

⁸ Persona que sobresurt en alguna àrea de la tecnologia i que és socialment inepte (són brillants però incapaços de comunicar-se). No confondre amb els hackers, ja que el seu coneixement tècnic no significa necessàriament manca d'habilitats socials. Si un vol saber si és un nerd pot fer un test que trobarà a <http://www.armory.com/tests/nerd.html>

⁹ És el contrari d'un nerd, és a dir, una persona que sobresurt en les relacions humanes i que tècnicament és un inepte. Quan un nerd coopera amb un bem el resultat és excel·lent.

¹⁰ Subgrup dins dels nerds, són els especialistes en equips de computació. El terme sol tenir un sentit pejoratiu.

desenvolupar formes noves de processament d'informació i comunicació electrònica [Levy, 1984; Raymond, 1999]. Per a ells el valor suprem és la innovació tecnològica informàtica. I, per tant, necessiten llibertat també; llibertat d'accés als codis font, llibertat d'accés a la xarxa, llibertat de comunicació amb altres *hackers*, esperit de col·laboració i de generositat (posar a disposició de la comunitat de *hackers* tot el que se sap i, recíprocament, rebre el mateix tractament de qualsevol col·lega). Alguns hackers són polítics i lluiten contra el control dels governs i de les corporacions sobre la xarxa, però la majoria no ho són: el que és important per a ells és la creació tecnològica. Es mobilitzen, fonamentalment, perquè no hi hagi restriccions a aquesta creació. Els *hackers* no són comercials, però no tenen res contra la comercialització dels seus coneixements, sempre que les xarxes de col·laboració de la creació tecnològica continuïn essent obertes, cooperatives i basades en la reciprocitat.”¹¹

Hacker és una expressió idiomàtica anglesa que significa, entre altres, "una persona contractada per a un treball rutinari" però que hi posa el coll en el seu treball. Aplicat a la informàtica es refereix a persones que els apassiona la informàtica, que es dediquen a investigar, aprendre i desenvolupar, amb molts esforços i amb una gran passió, sistemes informàtics i com utilitzar-los de forma innovadora. Tenen la seva pròpia ideologia, el seu principal objectiu no és convertir-se en delinqüents sinó "lluitar contra un sistema injust" . Tenen molta curiositat i proven tots els panys de les portes per esbrinar si estan tancades, no deixen un sistema que estan investigant fins que els problemes que se'ls presenta estiguin resolts. Sí que hi ha hackers que destrueixen fitxers i trenquen els sistemes intencionadament però aquests són un petit percentatge, la majoria d'ells passen inadvertits en els sistemes que opten per hackejar, no deixar rastre és el més important pels hackers. Un hacker és una persona que investiga la tecnologia d'una forma no convencional.

Un hacker és, doncs, algú que frueix amb l'exploració dels detalls dels sistemes programables i amb com aprofitar les seves possibilitats, al contrari de la majoria d'usuaris que en tenen prou a aprendre l'imprescindible; algú que programa de forma entusiasta i, fins i tot, obsessiva, i sap valorar el valor de hackejar; no li espanten els reptes intel·lectuals i els enfronta i supera creativament. El terme hacker connota participació com a membre de la comunitat global de la xarxa, i subscriu la major part dels postulats de l'ètica hacker. Sap que és millor ser descrit com a hacker pels altres, que proclamar-se o definir-se a si mateix com un hacker. Es consideren que formen

¹¹ Manuel Castells, *Hackers, crackers, llibertat i seguretat*. Lliçó inaugural del curs acadèmic 2001-2002 de la UOC <http://www.uoc.edu/web/cat/launiversitat/inaugural01/hackers.html>

part d'una mena d'elit, on el reconeixement dels altres és un dels valors més preuats. Resumint les seves pautes de comportament, podríem dir que els seus actuals 10 manaments són: mai destrueixis res intencionadament en l'ordinador que estàs crackejant, modifica només els arxius que facin falta per evitar la teva detecció i assegurar el teu accés futur al sistema, mai deixis la teva direcció real, el teu nom o telèfon en cap sistema, vigila a qui li passis informació, a ser possible no passis res a ningú que no coneguis la seva veu, número de telèfon i nom real, mai deixis les teves dades reals en un BBS, si no coneixes al sysop, deixa-li un missatge amb una llista de gent que pugui respondre de tu, mai hackegis en ordinadors del govern, el govern pot permetre's gastar-se fons a buscar-te mentre que les universitats i les empreses particulars no, no utilitzis BlueBox almenys que no tinguis un servei local o un 0610 a on connectar-te, si s'abusa del Bluebox pots ser caçat, no deixis en cap BBS molta informació del sistema que estàs crackejant, digues senzillament "estic treballant en un UNIX o en un COSMOS..." però no diguis a qui pertany ni el telèfon, no et preocupis de preguntar, ningú et contestarà, pensa que per respondre't a una pregunta, poden caçar-te a tu, al que et contesta o a ambdós. Pots passejar-te tot el que vulguis pel web, i mil coses més, però fins que no estiguis realment hackejant, no sabràs el què és.

En canvi els crackers (crack= destruir) són aquelles persones que, orgulloses dels seus grans coneixements sobre informàtica i amb el propòsit de lluitar contra el que està prohibit, busquen molestar als altres, destruint sistemes molt complexos mitjançant la transmissió de virus, o es dediquen a trencar les proteccions d'un sistema. No defensen en particular cap tipus de ideologia. És clar, però, que abans d'arribar a ser un cracker cal ser un bon hacker. Però no tots els hackers es converteixen en crackers. Els crackers (mot inventat el 1985 pels propis hackers per a marcar les diferències) són, doncs, aquells hackers que fan servir els seus coneixements per a violar sistemes, entrar a ordinadors, robar informació o trencar la protecció i seguretat dels sistemes o programes no per a conèixer, sinó per a obtenir un profit material, normalment econòmic, o fer mal.

"Als marges de la comunitat *hacker* s'hi situen els *crackers*. Els *crackers*, temuts i criticats per la majoria de *hackers*, pel desprestigi que els comporten davant l'opinió pública i les empreses, són els qui utilitzen els seus coneixements tècnics per a pertorbar processos informàtics [Hafner i Markoff, 1995]. Hi ha molts tipus diferents de *crackers*, però no tinc en consideració els qui penetren a ordinadors o xarxes de manera il·legal per robar: aquests són lladres refinats, una vella tradició criminal. Molts

crackers pertanyen a la categoria de *script kiddies*, és a dir, bromistes de mal gust, molts d'ells adolescents, que penetren sense autorització en sistemes o creen i difonen virus informàtics per sentir el seu poder, per mesurar les forces amb els altres, per desafiar el món dels adults i per donar-se importància amb els seus amics o amb els seus referents a la xarxa. La majoria tenen coneixements tècnics limitats i no creen cap innovació, per la qual cosa són, en realitat, marginals al món *hacker*¹². D'altres *crackers*, més sofisticats, penetren en sistemes informàtics per desafiar personalment els poders establerts; per exemple, Microsoft o les grans empreses. I alguns utilitzen la seva capacitat tecnològica com una forma de protesta social o política, com una expressió de la seva crítica a l'ordre establert. Aquests són els qui s'introdueixen en sistemes militars, administracions públiques, bancs o empreses per retreure'ls alguna mala acció. Entre els atacs de *crackers* amb motivació política s'han de situar els practicats per moviments polítics o per serveis d'intel·ligència dels governs, com ara la guerra informàtica desenvolupada entre els *crackers* islàmics i israelians o entre els protxetxens i els serveis russos.”¹³

L'existència d'ambdós neologismes reflecteix no només un desig de diferenciació, sinó sobretot, una repulsa al vandalisme dels *crackers*. Segurament que tot hacker, en algun moment de la seva vida, ha jugat o ha utilitzat les tècniques de crackejar, però a partir d'un cert grau de maduresa ha bandejat aquests usos de la programació i només, excepcionalment, els pot fer servir, com per exemple, si cal passar per alt algun sistema de seguretat per a completar algun tipus de treball. Per tant, hackers i *crackers* tenen molt menys en comú del que la majoria de lectors, confosos per la premsa sensacionalista o el periodisme mal informat, poden suposar. A finals dels 80 Lee Felsenstein criticava la nova situació: “D'una missió col·lectiva d'exploració s'ha passat a una orgia d'egoistes que es vanaglorien d'haver penetrat en ordinadors militars” i Steven Levy ja parlava de l'abisme que encara avui en dia es manté: “En el primer grup, els que creen, en el segon els que destrueixen. El primer grup desitjava tenir el control dels seus ordinadors, però el segon vol el poder que li donen. El primer grup sempre va cercar com millorar i simplificar, el segon només explota i manipula. El primer grup era comunal, compartia obertament nous descobriments, el segon és paranoic, aïllat i secret.” La majoria de hackers comparteix l'ús i defensa del software lliure, especialment GNU/Linux; és una qüestió de principis, però també de confiar en el que ha creat un mateix i de tradició que es remunta a quan els programes

¹² Segons el servei d'informació SecurityFocus, “els experts en seguretat i les forces de la llei nordamericans promociónen cada cop més que s'eduqui sobre ètica a les escoles, davant l'augment d'atacs informàtics duts a terme per adolescents”. Són a aquests adolescents als qui els hackers anomenen, despectivament, *script-kiddies*.

¹³ Manuel Castells, *Hackers, crackers, llibertat i seguretat*. Lliçó inaugural del curs acadèmic 2001-2002 de la UOC <http://www.uoc.edu/web/cat/launiversitat/inaugural01/hackers.html>

s'intercanvien i es milloraven entre tots. Vinton Cerf explica: "Tim Berners-Lee no va patentà la World Wide Web. No li va posar copyright. El va oferir obertament. I aquest fou l'estímul per al gran desenvolupament de la xarxa i d'innovadores idees. Hi ha una ètica contínua en la comunitat, de retornar a la xarxa el que ella t'ha donat." Galano entén aquesta ètica com "ser coherent amb les coses que penso i en les que crec. Compartir, col·laborar, integrar, brindar, intercanviar... comunicar. Creiem en el software lliure, que pots copiar, distribuir, modificar i utilitzar al teu aire, sense limitacions. Creiem en la capacitat d'autoorganització dels individus que persegueixen objectius clars i justos"¹⁴. Compartir informació és un bé poderós i positiu. Com diu el diccionari *Jargon File*, "existeix un deure ètic entre els hackers de compartir la seva experiència, escrivint codi obert i facilitant l'accés a la informació i als recursos computacionals, sempre que sigui possible. Grans xarxes com la pròpia Internet poden funcionar sense control central per aquest pacte, en el que tots confien i que es reforça amb un sentit de comunitat que podria ser el seu recurs intangible més valuós"¹⁵, comunitat on "el que saps és el que ets".

Cal tenir en compte que el mot hacker ha tingut tres etapes: des dels anys 50 fins als 80, era un neologisme que aparegué al MIT amb el que s'autoanomenaven persones que tenien una gran passió per saber com funcionaven els ordinadors per dins. En aquest sentit, eren "apassionats per les màquines". Al principi dels anys 80, el mot hacker es va popularitzar entre la població no hacker gràcies al llibre ja clàssic d'Steven Levy i a pel·lícules com *War Games*. Durant la dècada dels 80, el mot va anar agafant connotacions negatives a mida que s'anaven coneixent intrusions en sistemes informàtics a través de mòdems i xarxes de comunicacions. Invariablement, el qui ho feia era un aficionat que s'autoanomenava hacker. També els professionals informàtics van començar a usar el mot de manera denigrant per definir la feina d'aficionats. Durant els noranta, el fenomen GNU/Linux va tornar a posar de moda el mot hacker entre els entesos, sobretot gràcies a Richard M. Stallman, "*the last real hacker*", un personatge que va viure l'època daurada del hacking al MIT i ha refusat abandonar-la, convertint el hackerisme en el moviment pel programari lliure. Per això va aparèixer el mot cracker per diferenciar uns d'altres. "Els hackers originals eren professionals informàtics que, a mitjan anys seixanta, adoptaren la paraula 'hack' com a sinònim de treball informàtic executat amb certa habilitat. En els setanta varen emergir els techno-hippies, que creien que la tecnologia era poder que havia de posar-se a mans de la gent. A la segona meitat dels vuitanta, va aparèixer l'anomenat underground, que va

¹⁴ Citat a Mercè Molist: *Algunos hackers buenos*, <http://ww2.gm.es/merce/hack1.html>

¹⁵ *The Jargon File* <http://catb.org/~esr/jargon/html/>

canviar els significats: 'hack' equivaldria a sabotejar un sistema informàtic."¹⁶ Actualment aquest terme integra tots els sentits que ha anat rebent des dels anys cinquanta, i per això podem considerar que un hacker és un bon programador, algú que té la mà trencada amb el hardware i l'electrònica, un especialista en (in)seguretat. "Quan ets un hacker, són les pròpies conviccions internes del teu estatut d'elit les que et capaciten per a trencar o excedir les regles. Sovint, les regles transgredides pels hackers no són importants, són les regles dels avariciosos buròcrates de les companyies de telecomunicacions i de l'estúpida plana dels governants".¹⁷

D'aquests antecedents se'n pot deduir que un hacker és una persona amb molts coneixements tècnics, un expert i apassionat per la informàtica, els ordinadors i els llenguatges de programació, que l'apassiona investigar, descobrir, treballar i desafiar els límits. I aquest treball el diverteix i el satisfà. "Els *hackers* han estat fonamentals en el desenvolupament d'Internet. Van ser *hackers* acadèmics els qui van dissenyar els protocols d'Internet. Un hacker, Ralph Tomlinson, treballador de l'empresa BBN, va inventar el correu electrònic el 1970, per a l'ús dels primers internautes, sense cap mena de comercialització. *Hackers* dels Bell Laboratories i de la Universitat de Berkeley van desenvolupar UNIX. *Hackers* estudiants van inventar el mòdem. Les xarxes de comunicació electrònica van inventar els taulers d'anuncis, els xats, les llistes electròniques i totes les aplicacions que avui estructuren Internet. I Tim Berners-Lee i Roger Cailliau van dissenyar el navegador/editor (*browser/editor*) *World Wide Web*, per la passió de programar, d'amagat dels seus caps en el CERN de Ginebra, el 1990, i el van difondre a la xarxa sense drets de propietat a partir del 1991. També el navegador que va popularitzar l'ús del *World Wide Web*, el Mosaic, va ser dissenyat a la Universitat d'Illinois per dos *hackers* (Marc Andreessen i Eric Bina) el 1992. I la tradició continua: en aquests moments, dos terços dels servidors de web utilitzen Apache, un programa servidor dissenyat i mantingut en programari obert i sense drets de propietat per una xarxa cooperativa. En una paraula, els *hackers* informàtics han creat la base tecnològica d'Internet".¹⁸

Quan l'activisme entra a Internet, s'anomena *ciberactivisme* i, com descriu molt bé Dorothy E. Denning¹⁹ al seu estudi "*Activism, Hacktivism and Cyberterrorism: The*

¹⁶ Gisle Hannemyr: *Technology and Pleasure. Considering Hacking Constructive* http://firstmonday.org/issues/issue4_2/gisle/index.html

¹⁷ Bruce Sterling: *The Hacker Crackdown*, <http://bufet Almeida.com/textos/hackercrack/libro.html>

¹⁸ Manuel Castells, *Hackers, crackers, llibertat i seguretat*. Lliçó inaugural del curs acadèmic 2001-2002 de la UOC <http://www.uoc.edu/web/cat/launiversitat/inaugural01/hackers.html>

¹⁹ Pàgina principal de Dorothy Denning, <http://www.cs.georgetown.edu/~denning/>

*Internet as a Tool for Influencing Foreign Policy*²⁰ⁿ, té dues grans branques: una és l'activisme internàutic de tota la vida i l'altra, més recent, el *hacktivisme*. L'activisme internàutic es refereix a utilitzar Internet per donar suport a una causa amb mètodes no destructius: crear una web amb informació de la lluita, enviar alertes per correu electrònic, utilitzar canals de xat i llistes de correu per comunicar-se entre activistes, etc. El hacktivisme, en canvi, és la unió del hacking i l'activisme. Consisteix a utilitzar Internet no només per transmetre informació, sinó també com a lloc de lluita, tot muntant accions a la xarxa. Encara que el hacktivisme ve de lluny, amb els virus que els anys vuitanta renegaven de les bombes nuclears o d'ETA, el nom se'l van inventar fa pocs anys un grup de hackers nord-americans, Cult of the Dead Cow²¹, que es dediquen a lluitar contra la censura a la xarxa Internet xinesa. La seva darrera acció ha estat crear un programa, anomenat Peekabooty, que se salta les barreres governamentals. Això no vol dir que els hacktivistes no utilitzin també les armes tradicionals del ciberactivisme, com la creació de webs informatives o l'ús de llistes de correu per reunir-se. Els hacktivisme és una opció més i cada grup decideix si l'usa o no. Existeix també un altre tipus de hacktivisme, autoanomenat *políticament incorrecte* perquè se salta una de les normes principals dels hackers: no destruir. Són el tipus d'accions practicades per un altre grup nord-americà, Electronic Disturbance Theatre, que predica la "desobediència civil electrònica". La seva especialitat són les manifestacions virtuals a favor de la causa zapatista. A Itàlia, on van néixer aquestes manifestacions, en diuen *netstrikes*: es convoca el major nombre de gent un dia i una hora perquè es connectin amb el seu navegador a la pàgina web que es vol atacar, un cop allà s'hi reconnecten un cop, i un altre, fins que no pot aguantar el bombardeig i acaba caient.²² Altres formes de hacktivisme políticament incorrecte són els virus que reivindiquen alguna cosa, els *mail-bombings* (fer que molta gent enviï missatges electrònics a la mateixa adreça, fins col·lapsar-la) o els *webdefacements* (introduir-se en una web i canviar-ne la portada per deixar-hi un missatge polític). Darrerament, s'hi han incorporat noves modalitats, com les *Googlebombs*: fer que al primer lloc d'una recerca al buscador Google aparegui la webprotesta.

Altres components de la subcultura de les xarxes i dels ordinadors són els phreakers, aquells que trenquen la seguretat dels sistemes telefònics i fan un ús il·legal i delictiu de les xarxes telefòniques, els lamers, individus que volen fer hacking o activitats

²⁰ Dorothy E. Denning: *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, <http://www.iwar.org.uk/cyberterror/resources/denning.htm>, font <http://www.nautilus.org/info-policy/workshop/papers/denning.html>

²¹ Seu de Cult of the Dead Cow, <http://www.cultdeadcow.com/>

²² *El manual de l'activista virtual* a <http://www.3xl.net/reportatges/rep105175927.htm>

pròpies dels hackers, però estan mancats de tot coneixement per a fer-ho i sovint fan el ridícul, i els carders, els que fan un ús il·legal de les targetes de crèdit.²³

2. Del Capità Crunch a Kevin Mitnick

Tota història té la seva pròpia proto-història, els seus precedents i precursors. Sembla lògic, doncs, voler fer memòria dels qui, amb el seu treball, teories i actitud, varen fer possible la revolució de la computació, i la configuració del que després es va anomenar l'ètica hacker. I això amb més motiu quan és una dona, Grace Hooper²⁴ la considerada com la primera hacker de la era de la informàtica. Treballava i investigava la computadora Mark I, durant la II Guerra Mundial, va ser la primera persona que va assegurar que els ordinadors no només servissin per a objectius bèl·lics, sinó que podrien ser molt útils per diversos usos a favor de la humanitat. Ella va crear el llenguatge de programació anomenat FlowMatic i anys després va inventar el famós llenguatge COBOL. Va rebre, paradoxalment, el títol d'Home de l'any en ciències de la computació atorgat pel *Data Processing Management Association*; també fou la primera dona nomenada membre distingit de la British Computer Society.

El punt de partida el podem situar, tanmateix el 1939, quan el matemàtic hongarès John Louis Von Neumann va escriure l'article "*Teoria i organització d'autòmats complexos*", on presentava la possibilitat de desenvolupar petits programes que en poguessin controlar altres de similar estructura. Deu anys més tard, als laboratoris de la Bell Computer, subsidiària de l'AT&T, tres joves programadors, Robert Thomas Morris, Douglas McIlroy²⁵ i Victor Vysotsky, varen crear, com un passatemps, el joc Corewar, inspirats en la teoria de Von Neumann, els fixers del qual executaven programes que anaven disminuint de mica en mica la memòria de l'ordinador i el guanyador era aquell que aconseguia eliminar-la totalment. Aquest joc fou motiu de concursos en diversos centres d'investigació com ara el de la Xerox i el MIT; però fou mantingut en l'anonimat atès que a la dècada dels cinquanta la computació estava a mans d'una petita elit d'intel·lectuals. Aquells tres joves foren els autors dels precursors dels virus informàtics.

²³ Si es vol tenir una visió àmplia de l'organització i topografia de l'underground informàtic cal consultar Gordon Meyer (1989), *The Social Organization of the Computer Underground*. Illinois. Tesi no publicada de la Universitat del Nord.
<http://sun.soci.niu.edu/theses/gordon>

²⁴ Grace Brewster Murray Hopper, <http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Hopper.html> i també <http://www.perantivirus.com/sosvirus/hackers/gracehoo.htm>

²⁵ M. Douglas McIlroy, <http://www.cs.bell-labs.com/who/doug/index.html>

A finals dels anys 50 i durant els 60, en els laboratoris del MIT es començava a treballar amb ordinadors, que llavors eren grans màquines que requerien habitacions senceres, amb centenars de transistors, vàlvules i targes perforades. El 1959 la institució va oferir el primer curs de programació i un grup d'estudiants varen quedar emmirallats pels ordinadors i pel que es podia fer amb ells. Aquest grup d'estudiants pertanyia majoritàriament al TMCR (*Tech Model Railroad Club*) i per la complexitat dels primers ordinadors poques vegades s'hi podia accedir directament. Quan va arribar al MIT l'ordinador TX-0, Jack Dennis, antic membre del TMCR i professor del MIT va facilitar als seus estudiants un accés il·limitat a aquest ordinador, que tenia un teclat per a introduir dades, i no les targes perforades que fins llavors es feien servir. El grup d'estudiants cada cop passava més temps davant l'ordinador i varen començar a fer coses que ni els enginyers que havien dissenyat l'ordinador mai havien sospitat. A partir d'aquest moment és quan el terme hacker es comença a aplicar a un grup d'estudiants fanàtics dels ordinadors que comencen a desenvolupar un treball que va més enllà del que aleshores es creia possible.

Altres autors indiquen que l'origen dels hackers s'ha de cercar en el món de les comunicacions, en els laboratoris de la Bell Telephone. Alguns tècnics d'aquests laboratoris varen començar a desenvolupar unes tècniques i uns invents que varen revolucionar el món de les comunicacions i la informàtica. Sembla que l'etimologia hacker prové del cop sec (un hack o destrallada) i contundent que un operari de telefonia donava a l'aparell de telèfon i amb això aconseguia que funcionés. El terme hacker seria, doncs, un terme d'argot d'impossible traducció. També durant aquests anys va néixer l'ètica hacker i la recerca del hack²⁶, terme que es refereix al fet de modificar un programa o sistema per tal que faci alguna cosa per a la que no va ser dissenyat, des de fer més ràpid un ordinador modificant la velocitat del rellotge intern, fins obligar un sistema de seguretat a lliurar les seves contrasenyes.

El primer hack clàssic no té res a veure amb els ordinadors, sinó amb els sistemes telefònics. John T. Draper²⁷, el 1972, va descobrir que el xiulet que venia amb les caixes de cereals Cap'n Crunch²⁸ donava el to 2600 HZ que era exactament el to de control dels sistemes de telefonia a llarga distància. Practicant amb el xiulet va reproduir les seqüències de control i així podia realitzar trucades de llarga distància gratuïtes. Aviat va descobrir com parlar amb ell mateix (una trucada que donava la volta al món trigava 20 segons). Draper es va autoanomenar *Captain Crunch* i es va

²⁶ *A little bit of hacker history*, <http://www.cs.utah.edu/%7Eelb/folklore/afs-paper/node3.html>

²⁷ Pàgina principal de John T. Draper (AKA Captain Crunch), <http://www.webcrunchers.com/crunch/>

²⁸ Pàgina d'enllaços a Cap'n Crunch, <http://cg.scs.carleton.ca/~morin/misc/capn/>

convertir en un expert a construir i ensenyar a construir aparells, anomenats *blue box*, *red box*, *black box*, que bàsicament emetien sorolls que permetien fer trucades sense pagar. El hack no consisteix, però, a fer trucades telefòniques gratuïtes, sinó a poder fer servir un xiulet per a tenir accés a tot el sistema telefònic. Actualment es coneix com a phreaker l'expert a entrar en els sistemes telefònics i sistemes de comunicació. El títol de la revista *2600*²⁹ de la comunitat hacker es va posar per recordar aquest fet. A partir d'aquí va néixer la idea d'explorar els sistemes i descobrir efectes i propietats que els dissenyadors mai havien imaginat. Un dels seguidors d'aquest hacker pioner (a qui tothom coneix ara com a Capità Crunch) va ser Steve Wosniak³⁰, el fundador d'Apple³¹. Entre els experts es considera que el millor hack de tots els temps és UNIX³² desenvolupat per Ken Thompson³³ i Dennis Ritchie³⁴, el sistema operatiu que suporta la major part d'Internet.

A la dècada dels 80 les xarxes es van començar a comercialitzar i la informació a restringir, creant sistemes per a protegir els programes contra la còpia. Per als hackers, que tenien en la llibertat d'informació el fonament de la seva ètica, això era intolerable, i alguns van esmerçar molts esforços per aconseguir trencar els esquemes de protecció. Però a més d'aquestes activitats, van aparèixer els primers virus. Tot va començar, com ja hem vist, amb un joc, el Core War³⁵, dos programes que s'intenten destruir mútuament, mentre els seus creadors es limiten a observar. No juguen dos individus, sinó dos programes. D'aquí va néixer la idea de virus i cucs³⁶, que si en un primer moment no eren més que conceptes teòrics, aviat es varen estendre per la xarxa. Sembla ser que fou Bulgària la gran fàbrica de virus. S'explica que en la dècada dels 80 el govern de Bulgària va decidir apostar per la informatització, es formaren centenars de programadors i es va encarregar la creació de software nou; però no tenia sentit reinventar el que ja estava escrit, i els programadors es varen dedicar a

²⁹ 2600 The hacker Quarterly, <http://www.2600.com/>

³⁰ Seu de Woz.org, <http://www.woz.org/>

³¹ Seu d'Apple, <http://www.apple.com/>

³² Free Software Foundation, <http://www.gnu.org/home.ca.html>; veure Unix history a <http://virtual.park.uga.edu/hc/unixhistory.html>

³³ Ken Thompson, <http://www.bell-labs.com/news/1999/march/25/1.html>

³⁴ Dennis Ritchie, <http://www.cs.bell-labs.com/who/dmr/>

³⁵ Core War, <http://homepages.paradise.net.nz/~anton/cw/corewar-faq.html>

³⁶ El que genèricament es denomina virus informàtic, són peces de codi executable per un ordinador que han estat realitzades per destorbar el funcionament normal dels ordinadors. Hi ha moltes classes d'aquests codis. Pròpiament, els virus informàtics, són el conjunt d'aquests codis que s'afegeixen a fitxers que contenen programes executables ja existents.

També podem trobar cucs o troians que també són denominats virus. Els cucs són els codis que utilitzen els recursos de l'ordinador infectat per enviar-se a altres ordinadors. Habitualment els recursos utilitzats són el correu i les carpetes compartides. Els troians reben el nom pel cavall de Troia. Són programes que tenen l'aparença de ser útils o interessants (un salvapantalles, una fotografia, un programa antivíric, etc...) i en realitat realitzen una altra funció quan són executats (esborren fitxers, obren vies d'accés a l'ordinador, recullen informació de l'usuari, etc...). Centre de Tecnologies de la Informació, http://www.uib.es/servei/sci/manuals/virus.xml?p_seccio=ALT&p_apartat=1

crackejar els programes comercials de l'Europa occidental i dels estats Units, i a aplicar el que s'anomena enginyeria inversa per a entendre els equips de computació.

Aviat, molts programadors varen arribar a conèixer els programes millor que els seus dissenyadors, però Bulgària no tenia infraestructura per aplicar tot aquest coneixement; a més, només els caps de l'aparell burocràtic estatal tenien ordinadors, que eren més símbol d'estatut que eines de treball. En no poder aplicar els seus coneixements, els programadors varen començar a escriure virus, com un exercici intel·lectual i una forma indirecta de lluita contra el sistema. Però aviat els virus varen sortir dels límits de Bulgària, esdevingueren una epidèmia i obtingueren un gran ressò mediàtic. Diu l'anècdota que una periodista que va entrevistar a l'autor d'un virus conegut com Dark Avenger³⁷ es va trobar, de retorn al seu país, recompensada amb un virus que duia el seu nom. El 1988 va ser creat a Bulgària el Dark Avenger, el primer virus polimòrfic³⁸ i stealth³⁹ de la història. Fou descobert i aïllat pel Dr. Vesselin Bontchev⁴⁰ que dirigia el Laboratori de Virologia de l'Acadèmia de Ciències de Bulgària. El Dark Avenger va ser perfeccionat el 1989 i després d'expandir-se per Europa va arribar a la Universitat de Califòrnia a Davis. Per la seva perillositat va rebre l'atenció de científics i estudiosos; infectava arxius com, exe i el command.com. Cada cop que s'obria o llegia un arxiu l'infectava i afectava immediatament tots els altres arxius associats, com els d'un mateix programa dins d'un mateix directori, i cada cop que es cridava un altre executable infectat, com el command.com, per exemple, estenia els seus micro codis mutants. Tanmateix, el programador d'aquest virus va preveure que en algun moment apareixeria un antivirus i va prendre la precaució que, a més d'infectar el màxim nombre d'arxius, escrivia 512 bytes addicionals del seu micro codi viral en un o més sectors del disc, utilitzant la tècnica stealth. El 1990 i 1991 diversos antivirus detectaven el Dark Avenger, però no podien descobrir els 512 bytes escrits aleatòriament al disc, ja que aquests mai eren els mateixos pel fet de tenir una estructura polimòrfica. El micro codi remanent mostrava les següents paraules: "*Eddie still lives, some place in the world...*" (Eddie encara viu en alguna part del món...). Els usuaris afectats per aquest virus en aquella època no tenien més remei que reformatejar el seu disc dur.

³⁷ Dark Avenger el primer virus polimòrfico, <http://www.perantivirus.com/sosvirus/virufamo/darkaven.htm>

³⁸ Un virus polimòrfic és aquell que modifica en forma seqüencial els seus valors en la programació cada cop que s'auto-encripta, de tal manera que les seves cadenes no són les mateixes. Produeix diverses però diferents còpies d'ell mateix, mantenint operatiu el seu micro codi viral.

³⁹ Un virus stealth és aquell que quan està activat amaga les modificacions fetes als arxius o al sector d'arrancada que estan infectats. Aquesta tècnica fa servir tots els mitjans possibles per tal que la presència del virus passi totalment desapercebuda.

⁴⁰ Vesselin Bontchev, <http://victoria.tc.ca/int-grps/books/techrev/vess.htm>

El 1984 Fred Cohen⁴¹ publica "*Virus informàtics: teoria i experiments*"⁴², i s'alcen les primeres veus d'alarma per programes que n'infectaven d'altres. Entre 1985 i 1987 es detecta el primer virus en el *boot* d'un disquet, s'escriuen els primers virus experimentals: Vienna i Lehigh i apareix (c)Brain. No serà, però, fins el 1998 quan es produiran les primeres infeccions importants, Cascade, Jerusalem, i apareixeran els primers fabricants de programes anti-virus, com Dr. Salomon, i les primeres infeccions massives de 1999 amb Datacrime i Fu Manchú. A finals de 1990 hi havia catalogats més de 150 virus.

De gran impacte va ser la pel·lícula, *War Games* [Jocs de guerra] (1983), en la que Matthew Broderick feia el paper d'un adolescent expert en informàtica i molt curiós que, des de l'ordinador de casa seva i amb un prehistòric mòdem, entrava als sistemes de defensa nord-americans i gairebé provocava la Tercera Guerra Mundial. Per primer cop no es tractava de la caricatura d'un geek, sinó que el protagonista-hacker era presentat com una mena d'heroi romàntic que al final ho soluciona tot i es quedava amb la noia. Fou una mena de tret de sortida per a molts joves que es varen dedicar a entrar a seus governamentals per a sentir-se hackers i a moltes revistes d'ordinadors s'anunciava la venda d'equips informàtics "iguals al de la pel·lícula". La imatge del hacker en va sortir molt perjudicada perquè era associada a jove mancat d'habilitats socials, que destruïa sistemes molt complexos i que ho feia per pura diversió.

El 1989, va tenir lloc als Estats Units l'anomenat *The Hacker Crackdown*, que Bruce Sterling⁴³ explica en un llibre del mateix nom. El desencadenant va ser la guerra⁴⁴ entre dos grups de hackers, els Legion of Doom i els Masters of Deception, que es dedicaven a gaster-se bromes com entrar a la companyia telefònica per canviar l'import de la factura d'un rival o assaltar els sistemes d'un banc per posar a zero el compte corrent de l'enemic. Cada grup tenia la seva pròpia BBS, en què l'FBI es va infiltrar i va acabar detenint-ne els més destacats. Tot i que, finalment, el jutge va exculpar la majoria de detinguts, el *Hacker Crackdown* va commocionar tota la comunitat. Arran d'aquest fet es va crear la reconeguda Electronic Frontier Foundation⁴⁵, per defensar els drets de la gent del món digital, a iniciativa del

⁴¹ Fred Cohen, <http://www.cdt.org/security/dos/000223senate/cohen.html>

⁴² Fred Cohen i la classificació dels virus, <http://www.perantivirus.com/sosvirus/general/gusano.htm>

⁴³ Bruce Sterling: *The Hacker Crackdown* (La caza de Hackers) Ley y desorden en la Frontera electrónica. <http://bufetalmeida.com/textos/hackercrack/libro.html>

⁴⁴ Michelle Slatalla i Joshua Quittner: "Gang War in Cyberspace". *Wired magazine*, desembre 1994 <http://www.wired.com/wired/archive/2.12/hacker.html>

⁴⁵ Electronic Frontier Foundation, <http://www.eff.org/>

periodista John Perry Barlow i el programador Mitch Kapor, amb una important contribució econòmica de l'inventor d'Apple, Steve Wozniak.⁴⁶

En els noranta, i per a mantenir la seva ètica i reputació, els hackers van crear la paraula cracker per a referir-se i distanciar-se tant dels creadors de virus com de les pràctiques de sabotatge informàtic. Simultàniament, les BBS varen entrar en decadència per la popularització d'Internet, amb el que les comunitats esdevingueren molt més àmplies. Era el moment en el que Kevin Mitnick⁴⁷ penetrava diversos sistemes de computació i era buscat pel FBI. Arrestat i sentenciat, fou acusat de danys multimilionaris (que no es pogueren documentar), condemnat a la presó i se li va prohibir apropar-se a qualsevol equip d'ordinadors o de televisió per cable. Tot i que les seves pràctiques eren més pròpies dels crackers, molts hackers que no aprovaven les seves accions li varen donar suport i començaren a protestar de la millor manera que sabien: hackejar pàgines d'Internet de les companyies per a burlar-se de la seva seguretat o posar a les seves pàgines principals el rètol "Alliberin a Kevin". El punt culminant de la ruptura dels hackers amb els crackers va tenir lloc el 1994, quan un grup de hackers liderats pel "hacker rus" va penetrar en els sistemes informàtics de Citibank i va robar 10 milions de dòlars. La confusió va durar encara força temps, sobretot per la presència dels script Kiddies⁴⁸, que s'aprofiten de la llibertat d'informació propugnada pels hackers per a recopilar informació sobre virus, fallades de seguretat dels sistemes... i actuar sense saber, molt sovint, les conseqüències de les seves accions.

3. La construcció del discurs hacker

"*La consciència d'un hacker*"⁴⁹, text escrit el 1986 per The mentor, ha esdevingut el manifest hacker per excel·lència; la seva rebel·lia, la crítica a l'escola, l'avorriment davant l'aprenentatge tradicional, l'emoció davant l'ordinador, la sensació de formar part d'un col·lectiu, la necessitat de comunicació, la passió i el desig de coneixement, l'esperit d'exploració, la crítica contra el sistema, el sentir-se iguals als altres, en són els components bàsics d'aquesta nova consciència. D'aquí l'interès a reproduir-lo.

⁴⁶ Veure l'article de Mercè Molist: *25 anys d'underground informàtic* <http://www.3xl.net/reportatges/rep104234039.htm>

⁴⁷ Kevin Mitnick: *An excerpt from Takedown*. <http://www.takedown.com/bio/mitnick.html>

⁴⁸ S'anomenen així als nou vinguts que fan servir les eines dels hackers però sense tenir els coneixements tècnics d'aquests, i són els responsables de molts atacs sense sentit. Per a confondre la premsa s'autoanomenen hackers.

⁴⁹ *The Conscience of a Hacker* by Mentor Written on January 8, 1986 <http://zenorone.tripod.com/cohack.htm>

“Un altre ha estat capturat avui, surt a tots els diaris. ‘Adolescent arrestat en un escàndol per crims informàtics’. ‘Hacker arrestat després de traspasar les barreres de seguretat d'un banc’. Maleïts xavals. Tots són iguals. Però tu, en la teva psicologia partida en tres y el teu tecnocervell del 1950, alguna vegada has observat què hi ha darrere els ulls d'un Hacker? Algun cop t'has preguntat què el mou, quines forces l'han format i quines el van poder moldejar? Sóc un Hacker, entra al meu món... El meu món comença a l'escola... Sóc més intel·ligent que la majoria dels altres xavals, aquesta porqueria que ens ensenyen m'avorreix... Maleïts perdedors. Tots són iguals. Estic en un curs preuniversitari o al parvulari? He sentit explicar als professors per quinzena vegada com reduir una fracció. Jo ho entenc. ‘No, senyoreta Smith, no tinc els deures fets, els he fet al meu cap’. Maleït xaval. Ho deu haver copiat. Tots són iguals. Avui he fet un descobriment. He trobat un ordinador. Espera un moment, això mola! Fa el que jo li dic. Si comet un error, és perquè jo m'he equivocat. No perquè no li agrada... O se sent amenaçat per mi... O pensa que soc un cregut... O no li agrada ensenyar i no hauria d'estar aquí... Maleït xaval. Només sap jugar. Tots són iguals. I llavors va succeir... Una porta oberta al món... Corrent a través de les línies telefòniques com l'heroïna a través de les venes d'un drogoaddicte, s'envia un pulsació electrònica, un refugi per a les incompetències del dia a dia és buscat... Una taula de salvació és trobada. "Aquest és... Aquest és el lloc al qual pertanyo". Conec a tothom aquí... encara que no els conegui, encara que mai hagi parlat amb ells, encara que no els torni a veure mai més... Els conec a tots... Maleïts xavals. Enllaçant les línies telefòniques una altra vegada. Tots són iguals... Apostat el cul que tots som iguals... A nosaltres ens han estat donant farinetes digerides per a bebè quan teníem ganes de menjar carn. Els trossets de carn que a vosaltres se us han caigut estaven mastegats i sense gust. Nosaltres hem estat dominats per sàdics, o ignorats pels apàtics. Els pocs que tenen alguna cosa a ensenyar-nos són alumnes complaents, però aquests pocs són com gotes d'aigua en el desert. Ara aquest és el nostre món... El món de l'electró y el commutador, la bellesa del baudi. Nosaltres fem ús d'un servei que ja existeix i que podria estar tirat de preu si no estigués a mans d'avariciosos assedegats de més guanys, i vosaltres ens anomenau criminals. Nosaltres explorem... i vosaltres ens anomenau criminals. Anem rere el coneixement... i vosaltres ens anomenau criminals. Nosaltres existim sense color de pell, sense nacionalitat, sense prejudicis religiosos... i vosaltres ens anomenau criminals. Vosaltres vàreu construir bombes atòmiques, vàreu fer la guerra, vàreu assassinar, vàreu enganyar i ens vàreu mentir tractant de fer-nos creure que era per al nostre bé, i ara nosaltres som els criminals. Si, sóc un criminal. El meu crim és la curiositat. El meu crim és jutjar les persones pel que diuen i pensen, no pel que aparenten. El meu crim és ser més intel·ligent, una cosa que mai em

perdonaràs. Sóc un Hacker i aquest és el meu manifest. Tu podràs parar un d'aquests, però no ens podràs para a tots... Després de tot, tots som iguals.”⁵⁰

Un dels documents bàsics del món hacker és el *Jargon File*⁵¹, “el patrimoni col·lectiu de la cultura hacker” escrit o recopilat per Eric S. Raymond, que defineix els hackers com aquells que reuneixen una o vàries de les següents característiques: persona que frueix investigant sistemes operatius, llenguatges de programació i sap treure'n el màxim profit (es diferencien de l'usuari normal perquè aquest es limita a conèixer el mínim i imprescindible d'un programa); és entusiasta de la programació que, de vegades, l'arriba a obsessionar; aprecia el valor de hackejar, que significa buscar un ús no documentat o previst d'alguna cosa; és molt bo programant; expert en un programa o sistema operatiu concret (per exemple, Unix); expert o entusiasta de tota mena; algú que frueix amb un repte intel·lectual i l'intenta resoldre de manera autodidacta, creativa i lúdica.

El 1984 es va publicar un treball important que perfila prou bé l'ideari hacker. Steven Levy, en el seu text *Hackers: heroes de la revolució*⁵², explica la història del neologisme hacker i dels qui n'estan orgullosos de dir-se'n i la història de la revolució social dels ordinadors personals, una història que fa començar el 1958, quan Peter Samson, Alan Kotok, Bob Saunders i altres van arribar al Massachusetts Institute of Technology i van descobrir la sala on hi havia instal·lada la IBM 407. El 1959 es va impartir al MIT un curs dirigit per John McCarthy, un dels pares de la Intel·ligència Artificial, que havia anat abandonant un programa d'escacs per a dedicar-se a desenvolupar el nou llenguatge LISP; el grup de Kotok i Samson es varen fer càrrec del joc i esdevingueren els principals usuaris de la gegantina IBM 704 i de les seves successores, la 709 i la 7090. Un temps després, Jack Denis, un ex-alumne, dugué al MIT un ordinador en el que hi havia estat treballant al Lincoln Lab, el TX-0m que en lloc de vàlvules funcionava amb transistors i no feia servir targetes, sinó que podia ser programada amb un dispositiu de perforació de cintes de paper. La Tixo, com l'anomenaven els seus usuaris, fou la màquina al voltant de la qual s'anaren constituint els primers hackers, joves brillants i experts programadors que es passaven 36 hores seguides programant, en descansaven 12, i tornaven a la feina. Un d'ells era Peter Deutsch, que amb els seus dotze anys es va convertir en el membre més jove del grup, i que va despertar els odis i les enveges dels estudiants avançats de sistemes perquè els explicava els

⁵⁰ The Mentor: *Manifiesto hacker*, http://cfbsoft.iespana.es/cfbsoft_es/seguridad/manifiesto.htm

Manifest Hacker The Mentor http://cfbsoft.iespana.es/cfbsoft_es/seguridad/manifiesto.htm

⁵¹ *The Jargon File* versió 4.4.4 <http://catb.org/esr/jargon/> <http://www.catb.org/~esr/jargon/html/index.html>

⁵² Levy, Steven (1984). *Hackers. Heroes of the computer revolution*. New York. Penguin.

errors que feien en els seus programes. La manca de software de la Tixo obligava a aquests primers hackers a construir els seus propis utilitaris de sistemes i els permetia dotar l'ordinador de noves funcionalitats. No només el van reconfigurar, sinó que el varen redescobrir. Samson, per exemple, un fanàtic de la música clàssica, se'n va adonar que l'altaveu que tenia Tixo per emetre els seus beeps podia ser manipulat per a produir diferents sons, i va desenvolupar un programa que tocava fugues de Bach; i Stewart Nelson va fer servir la idea de Samson per a connectar l'altaveu de l'ordinador directament a la línia telefònica. Hi havia treball, passió, comunicació i una ètica que Levy descriu amb detall i molts exemples, i que resumeix en sis normes que estan a la base de tot aquell que es consideri hacker: lliurar-se sempre a l'imperatiu de transmetre! L'accés als ordinadors i a qualsevol cosa que pugui ensenyar-te com funciona el món ha de ser il·limitat i total: tota la informació ha de ser lliure; desconfiar de l'autoritat, promoure la descentralització; els hackers han de ser jutjats per les seves accions no per criteris falsos com l'edat, raça o posició; es pot crear art i bellesa en un ordinador; els ordinadors poder canviar la teva vida a millor.

El llibre de Levy ens parla, doncs, de la personalitat d'aquelles persones que han fet de la indústria informàtica allò que és avui en dia: des dels primers dies al MIT a mitjans dels 50 fins als dissenyadors de jocs de mitjans dels 80. Hi trobem la primera generació de hackers, els estudiants del MIT que lluitaven contra el sistema: els ordinadors d'IBM amb funcionament en modalitat per lots, controlats per una elit que eren els únics autoritzats a manipular aquestes màquines sagrades. Aquesta generació de hackers va pensar que els ordinadors havien d'estar a l'abast de tothom i no només d'aquells que només pensaven com mantenir-los lluny de la massa. També es parla de la generació de hackers "filòsofs" de finals dels 60 i començaments dels 70 que estaven convençuts que els ordinadors permetrien canviar el món. I dels hackers especialitzats en hardware de finals dels 70 que construïen els seus propis ordinadors domèstics a partir de materials de segona ma. A la dècada dels 80, amb la introducció dels ordinadors domèstics a un preu assequible, la nova generació de hackers va estar representada per aquells programadors de jocs que es convertien en milionaris tot just amb 20 anys [cal recordar, aquí, el capítol dedicat a la convergència de les metanarratives en els jocs].

El llibre assoleix un cert clímax èpic quan parla de Richard Greenblatt, el hacker dels hackers, i de Bill Gosper, que va donar forma i teoria a l'ètica del hacking, va reinventar els mètodes de càlcul de quasi tot, va aprendre xinès per a llegir el menú dels restaurants i va invertir mesos de feina en el *Life*, un joc de simulació d'autòmats

cel·lulars construïts a base de complexos models matemàtics. I tot plegat per entusiasme i diversió. Al voltant de Marvin Minsky, reconegut com el pare de la Intel·ligència Artificial, el laboratori del MIT va acollir els principals hackers de la seva generació que varen construir, sobre els seus impressionants ordinadors, comunitats que lluitaven, sense esperar res a canvi, pel somni d'estendre el poder de les màquines. Però la veritable revolució va arribar amb els hackers del hardware, que varen permetre que els ordinadors arribessin a les taules dels nostres escriptoris i estudis. Revolució que va començar amb Altair, el primer ordinador que ja es podia tenir a casa, i que va aglutinar al seu voltant a molts joves experts en programació, dels que cal citar un grup que es va autoanomenar *Homebrew Computer Club*, del qual van sortir alguns dels pioners com Stephen Wozniak, un dels creadors d'Apple. És una època en la que es barregen l'esperit hippie amb les accions anti-bèl·liques, les corporacions gegantines que tot just duraven un parell d'any amb l'entusiasme i l'agitació davant la revolució de tenir un ordinador a l'abast de milers de persones. Però és també el moment en el que comencen a emergir interessos menys ingenus, és quan neix i es popularitza el Basic i el software deixa de ser un motiu d'orgull per a esdevenir una cosa per la que cal pagar; és el moment d'aquell jove programador que va trencar les normes no escrites per tal d'evitar que els altres hackers poguessin fer servir el seu software de forma lliure, i que va començar a atacar a través de la premsa als qui el copiaven en lloc de pagar-lo: el seu nom, Bill Gates.

La dècada dels vuitanta està dedicada als hackers de jocs, les noves "stars" del software, amb els seus contractes milionaris amb empreses sorgides pràcticament del no res. És l'època de Sierra On-Line, una creació de Ken Williams, un programador de sistemes que va descobrir un joc d'aventures i, animat per la seva esposa, va crear una versió per a l'Apple II. És també l'època de Broderbund, de Sirius i d'altres empreses sorgides al voltant de l'Apple II i Atari 800, i d'autors famosos com John Harris. Al final del llibre, i amb un cert deix de tristesa, ens descriu com de mica en mica el somni hacker va anar sent vençut per la burocràcia, el control, els secrets, la seguretat, els beneficis, però ho fa sense criticar-ne cap aspecte; això ho deixa a la responsabilitat del lector.⁵³

Un altre text fonamental en l'ideari hacker és *La catedral i el Bazar*⁵⁴, potser l'assaig més interessant per entendre el codi obert. Escrit el 1997 per Eric Raymond ha estat revisat a principis del 2001. El text parteix de la contraposició entre dos models de

⁵³ Veure Martín Salías: *Los orígenes del hacking*, a <http://www.ubik.to/vr/vr20/hackers.htm>

⁵⁴ *The Cathedral and the Bazaar* <http://www.catb.org/~esr/writings/homesteading/cathedral-bazaar/>

desenvolupament. Al principi Raymond pensava que el desenvolupament de qualsevol programa informàtic havia de seguir un mètode similar a la construcció d'una catedral, és a dir, en la construcció d'un temple petits grups d'artesans, vidriers, marbristes, picapedrers, escultors feien el seu tros de treball de manera aïllada i independent, sense cap interrelació entre ells i la suma de tots els treballs era la catedral. Pensava que en el desenvolupament d'un programa el millor mètode de treball era el dels savis individuals o petits grups de treball, fent el seu treball aïlladament, però el desenvolupament de Linux li va fer canviar el plantejament.

Raymond constata que la interrelació, la fi de l'aïllament, l'intercanvi constant, quasi la promiscuitat entre els membres del grup de treball, dona millors fruits. A partir de la metàfora del basar afirma que l'èxit d'un projecte es fonamenta en l'intercanvi permanent, en una relació alegre, desordenada i eficient de tots els qui treballen en el projecte. Afirma que és molt més eficaç el model del basar que el de la catedral, és a dir, resulta més productiu desenvolupar projectes en un entorn de comunitat oberta que en un sistema tancat. La col·laboració i la revisió crítica constant per múltiples interlocutors assegura una qualitat final molt superior. Aquest text ha esdevingut una de les pedres angulars del moviment a favor del codi obert, que pretén canviar radicalment el model imperant de desenvolupament tecnològic del software. El moviment de codi obert parteix de la premissa que ningú és propietari del codi font del programa, que qualsevol usuari pot utilitzar-lo, millorar-lo i redistribuir-lo i es contraposa al model del codi propietari, en el que l'usuari no té cap dret sobre un programa, només un dret d'ús. Aquest és el debat entre el model Linux i el model Microsoft, els dos extrems més emblemàtics de cada línia.

Un altre text bàsic d'Eric S. Raymond és *How To Become A Hacker*⁵⁵, escrit, segons l'autor, per a respondre les consultes, que sovint li fan entusiàstics novells de la xarxa, sobre com esdevenir un hacker. Abans, tanmateix, ens clarifica el que cal entendre per hacker. "Hi ha una comunitat, una cultura compartida, de programadors experts i mags de les xarxes que remunta la seva història dècades enrera als primers miniordinadors de temps compartit i els primers experiments d'ARPAnet. Els membres d'aquesta cultura van originar el terme 'hacker'. Els hackers van construir la Internet. Els hackers van fer del sistema operatiu Unix el que és avui. Els hackers fan funcionar Usenet. Els hackers fan funcionar la World Wide Web. Si ets part d'aquesta cultura, si hi has contribuït i altra gent que hi estan ficats saben qui ets i et diuen hacker, ets un hacker.

⁵⁵ Eric Steven Raymond: *How to become a Hacker*, <http://catb.org/~esr/faqs/hacker-howto.html> Traducció catalana a Com convertir-te en un hacker http://dilvert.com/andreu/hacker_howto.html

La mentalitat del hacker no està pas confinada a aquesta cultura software-hacker. Hi ha gent que aplica l'actitud hacker a altres coses, com l'electrònica o la música –de fet, pots trobar-ho als nivells més elevats de qualsevol ciència o art. Els hackers del software reconeixen aquests esperits emparentats en qualsevol lloc i també els poden anomenar "hackers"– i alguns sostenen que la naturalesa hacker és realment independent del mitjà particular en que el hacker treballa. (...). Hi ha un altre grup que s'anomenen a si mateixos hackers, però que no ho són. Aquesta gent (majoritàriament adolescents) que els agafa la fal·lera entrant en altres ordinadors i piratejant el sistema telefònic. Els veritables hackers anomenen aquests individus `crackers' i no hi volen tenir res a veure. Els hackers de veritat, sobretot pensen que els crackers són ganduls, irresponsables, i no gaire brillants, i argumenten que ser capaç d'entrar en un altre ordinador no et fa un hacker pas més que ser capaç de fer un pont a un cotxe et fa enginyer industrial“. I així resumeix l'actitud hacker: “Els hackers resolen problemes i construeixen coses, i creuen en la llibertat i l'ajut mutu voluntari.” Si vols ser hacker has de creure les següents afirmacions: el món està ple de problemes fascinants que esperen ser resolts; cap problema no hauria de ser resolt mai dues vegades; l'avorriment i l'obligació són demoníacs; la llibertat és bona; l'actitud no és un substitut de ser competent. I entre les habilitats bàsiques del hacker s'hi troben la de saber programar, la de saber fer servir el Unix de codi obert, la d'escriure HTML, i la de tenir un bon nivell d'anglès. I les coses que s'han de fer per a ser respectat pels altres hackers són escriure programari de codi obert, ajudar a provar i depurar programari de codi obert, publicar informació útil, ajuda a mantenir la infraestructura i servir a la cultura hacker.

En els darrers anys han proliferat els llibres sobre seguretat informàtica que han servit, sobretot, per a estigmatitzar, en nom de la tècnica i de la seguretat, l'activitat hacker. És el cas del llibre de Tsutomu Shimomura i John Markoff, *Takedown*⁵⁶, un llibre per a informàtics que, com el seu títol indica, és el relat de la persecució d'un hacker. La història comença la tarda de Nadal de l'any 1994. Un hacker entra a les màquines de Tsutomu Shimomura i copia diversos programes i el seu correu electrònic. Des del moment en que l'autor del llibre té coneixement d'això, comença una gairebé obsessiva tasca de conèixer, en primer lloc, com han entrat i després què s'ha fet dels seus fitxers. Durant uns mesos la resta d'activitats passen a un segon terme. En disset capítols, els autors parlen en primera persona de tot el que fan. En primer lloc, la reconstrucció de l'atac (un atac de suplantació de l'adreça IP seguit d'un segrest d'una

⁵⁶ Tsutomu Shimomura i John Markoff (1997), *Takedown*. Persecución y captura de Kevin Mitnick, el forajido informático más buscado de Norteamérica. Una crónica escrita por el hombre que lo capturó. Madrid. El País Aguilar <http://www.takedown.com/>

sessió TCP establerta) i com fan servir *sniffers* per analitzar el tràfic de la xarxa i descobrir quina és l'activitat del personatge que suposadament és l'autor de l'accés no autoritzat als ordinadors durant la tarda de Nadal. Un cop identificat un sospitós, la següent part és identificar on es troba per tal de detenir-lo. La utilització de telèfons mòbils analògics per connectar a Internet facilita la detecció: la connexió és altament inestable i sovint es talla. Això permet identificar l'estació repetidora des d'on es reben les trucades: Raleigh, la capital de Carolina del Nord. Un cop a Raleigh, cal saber des d'on es fan les trucades. Per això s'aprofiten de material d'escolta (un de propi de Tsutomu Shimomura construït amb un ordinador de butxaca HP 200LX i un telèfon mòbil) i equipament propi de l'FBI i les companyies telefòniques. Tot això finalitza la nit del catorze de febrer de 1995. Kevin Mitnick és arrestat per agents de l'FBI.

És el mateix cas que el llibre de John Chirillo, *Hack Attacks Revealed*⁵⁷ que pretén mostrar com es fan els atacs dels hackers, partint de l'explicació de la base necessària sobre el funcionament de la pila de protocols TCP/IP (i altres protocols, com ara NetBIOS i IPX) que cal conèixer per tal de comprendre moltes de les eines que més endavant descriurà. A continuació explica els fonaments de sistemes operatius, sistemes de defensa perimetrals, etc. El CD que acompanya al llibre inclou una bona recopilació de les principals eines genèriques utilitzades per a la realització d'"atacs" a sistemes, tant per part dels professionals de la seguretat informàtica com pels hackers malèvols. Un cop més, doncs, la seguretat es prioritza per damunt de la llibertat. Les repercussions de l'11 de setembre als Estats Units en matèria de restriccions de la llibertat i de controls que fregaven la inconstitucionalitat, n'és una prova més.

La majoria dels últims llibres publicats sobre seguretat estan centrats en temes com poden ser la seguretat de Windows, la seguretat de Cisco o la seguretat TCP/IP. Si bé ningú no posa en dubte que la seguretat dels punts finals és important, és evident que centrar-se en la seguretat dels extrems no necessàriament ha de millorar el nivell global de seguretat. Per aconseguir aquest objectiu cal treballar en la integració de les mesures de seguretat dels diversos punts de la xarxa. Durant l'any 2001 han anat sorgint diversos llibres que no es limiten a discutir les mesures de seguretat concretes de cada sistema sinó que miren d'analitzar la xarxa a nivell més global. *Counter Hack*⁵⁸ d' Ed Skoudis n'és un bon exemple. El llibre es presenta com la "nova generació" de llibres per a hackers. No es centra en analitzar una tecnologia concreta sinó que l'autor

⁵⁷ John Chirillo (2001) *Hack Attacks Revealed: A complete reference with custom security hacking toolkit*. John Wiley & Sons.

⁵⁸ Ed Skoudis (2001), *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice May.

presenta les mesures que cal prendre per tal de defensar les xarxes d'ordinadors contra els diversos atacs que poden patir. Per a realitzar aquesta preparació, es separa el procés en cinc categories: reconeixement, anàlisi, obtenir accés, mantenir l'accés, cobrir els passos i ocultació. L'aspecte més important d'aquest llibre és valorar l'impacte real de les amenaces i, especialment, no menysprear als adversaris. I cal tenir en compte que els "adversaris" no són únicament aquells que s'associen als "hackers", sinó que és un grup difós que abasta des d'empleats, membres del crim organitzat, clients, empreses de la competència, organitzacions d'intel·ligència, etcètera. El llibre comença amb una introducció a com funciona el protocol TCP/IP, que la majoria de lectors amb experiència podran ignorar. Els següents dos capítols són un resum dels sistemes operatius Unix i Windows NT/2000 (els sistemes operatius més freqüents a l'actualitat). El llibre no analitza les vulnerabilitats específiques de cada sistema sinó que més aviat es centra a conèixer quines són les implicacions a nivell de seguretat que comporta la seva utilització. A continuació es fa una anàlisi de com els adversaris intenten obtenir informació sobre les nostres xarxes com a pas previ a l'obtenció d'accés. El capítol 7 analitza els atacs a nivell d'aplicació i sistema operatiu. Inclou una molt bona explicació dels atacs de desbordament de memòria intermèdia i com evitar-los. Per últim s'expliquen els diversos sistemes utilitzats en els atacs: cavalls de troia, portes secretes (*backdoors*), *root kits*. És de destacar que cada vegada que es cita una eina d'aquestes, s'inclou la descripció de la mateixa i com pot ser utilitzada en els atacs contra xarxes d'ordinadors. També cal destacar el gran nombre d'històries explicades en primera persona. Es realment un plaer veure que l'autor del llibre és un professional amb experiència real i no senzillament una persona que associa el fet d'escriure un llibre original a copiar el text dels diversos RFC.

Al costat d'aquestes obres en les que el component informàtic i l'objectiu de la seguretat en són els eixos vertebradors, el 2001 va veure també la publicació del llibre de Pekka Himanen, *L'ètica del hacker*⁵⁹, que descriu el model de treball i les opcions ètiques implícites en el context de la societat de la informació. Ja Eric Raymond definia l'ètica hacker com una cultura del coneixement, una meritocràcia basada en l'habilitat, en el regal com a forma de guanyar reputació, la col·laboració enfront de la competència. "Cap node és indispensable. Un altre farà el que tu deixis. Aquesta ecologia té una resposta més ràpida a les demandes del mercat i més capacitat de resistir i regenerar-se". I encara que no formi part de l'ètica en sentit estricte, molts hackers coincideixen en les seves idees socials alternatives. Per a Raúl Sánchez del col·lectiu TrabajoZero "en ells tenim el paradigma d'una força de treball indistingible

⁵⁹ Se li dedica el capítol 10 de l'apartat V del present estudi

d'una subjectivitat singular, d'una constel·lació ètica, d'una llegenda sempre oberta a la innovació i d'una capacitat de teixir comunitats, que afirmen la seva independència i reproduïen la seva potència creativa i alliberadora. No cal furgar massa per a veure la politicitat intrínseca que presenten. Ens trobem davant d'un subjecte que es forma independentment i clandestinament en relació al sistema de producció i reproducció de la força de treball capitalista". Ho reconeix Jesús Cea: "Cert esperit de rebel·lia, en general, sí que hi ha. Un hacker és un curiós, algú que fa una cosa teòricament impossible, que pensa de manera diferent". I segueix Galeano: "El hacker és potencialment un hacktivista, ja que la consciència forma part d'ell"⁶⁰. L'ètica hacker implica una determinada idea del treball cooperatiu i proposa que la societat xarxa sigui transparent i que el dret a la comunicació no sigui limitat en cap àmbit. Com diu Alcoberro, repensar els elements ètics implícits a les tecnologies de la informació i la comunicació significa fer possible nous àmbits de llibertat i de creativitat. Es tracta de donar més llibertat a més gent, però en l'àmbit de la tecnociència, on l'imperatiu de produir no pot separar-se del nou imperatiu hacker: transmetre.⁶¹

*Hackers Beware*⁶² escrit per Eric Cole, un dels principals instructors de SANS Institute, presenta les diverses tècniques utilitzades habitualment pels atacants malèvols (crackers) però ràpidament comença l'anàlisi en profunditat d'atacs específics. Evidentment, també indica quines mesures de prevenció cal prendre per tal d'evitar cadascun dels atacs. Possiblement aquest és el gran factor diferencial d'aquest llibre, allò que el fa realment únic: ens parla de diversos problemes, els explica i analitza els *exploits* existents i ho fa d'un gran nombre de situacions. Això permet al lector comprendre exactament quin és l'abast real de les diverses amenaces de seguretat. Pels usuaris de sistemes de detecció d'intrusos, a més, el llibre facilita la signatura específica de cada *exploit* analitzat.

Per a recuperar el discurs hacker en positiu, cal esmentar l'obra d' Ankit Fadia⁶³, *The Unofficial Guide to Ethical Hacking*⁶⁴, escrit per un noi de setze anys, estudiant d'una escola pública de Delhi. Molts *hackers* realment són uns adolescents. El llibre ens sorprèn en primer lloc per les seves dimensions: més de 700 pàgines on tracta de quasi tots els tipus de vulnerabilitats que habitualment s'utilitzen per atacar els ordinadors: configuracions errònies de Windows, contrasenyes poc segures, esborrar

⁶⁰ Citat a Mercè Molist: *Algunos hackers buenos*, <http://ww2.grn.es/merce/hack1.html>

⁶¹ Ramón Alcoberro: *Ética hacker y empresa: el reto de las TIC en los valores de empresa*, a <http://etpclot.jesuitescat.edu/~37272647/arxiu.htm>

⁶² Eric Cole (2001), *Hackers Beware* New Riders Publishing.

⁶³ Ankit Fadia, http://www.evh.ieee.org/sb/bombay/amrutvahini/events/ankit_seminar_files/Ankit_Information.htm

⁶⁴ Ankit Fadia (2002), *The Unofficial Guide to Ethical Hacking*. Premier Press.

la CMOS d'un ordinador sense haver d'obrir-lo, atacs de denegació de servei, accés a encaminadors, virus de tota mena, etcètera. L'autor deixa ben clar, al començament del llibre, que aquest és un manual de referència per al *hacker* ètic. No tracta de temes com poden ser la falsificació de targetes de crèdit, que són d'interès per aquells que volen aprofitar-se de les tècniques de *hacking* amb finalitats lucratives. A l'apèndix s'hi recull una impressionant col·lecció de contrasenyes per defecte d'una gran quantitat de dispositius, des de *mainframes* fins a encaminadors, ordinadors, sistemes operatius, bases de dades...

4. El hacktivisme com a moviment social

Tot i que les seves activitats han estat criminalitzades, sobretot per la premsa nordamericana i en relació a la llei Constitucional dels Estats Units, la subcultura hacker ha jugat i juga un paper vital en la progressió de la tecnologia i, alhora, realitza una funció reguladora de control social, protestant i minant subtilment el control estatal i corporatiu mitjançant els ordinadors i les tecnologies telemàtiques.

Estudiar què és el hacking, com funciona i què representa per als seus participants és força complicat, ja que les comunicacions de hackers a les BBS's (Bulletin Board Systems)⁶⁵, un dels canals més utilitzats per a intercanviar-se informacions, són privades, molt protegides i canvien sovint d'adreça, i, a més, si s'hi detecta que algú no és expert en programació i que, per tant, pot ser un infiltrat, automàticament se'l dona de baixa de la BBS.

Accedir a una d'aquestes BBS és complicat; cal omplir qüestionaris, que sempre inclouen preguntes tècniques, per a comprovar l'expertesa del nou usuari, al qual se li fa, sovint, una petita prova, com trobar el número de telèfon no llistat d'un determinat ordinador, o bé la contrasenya d'algun sistema corporatiu segur. Aquestes proves funcionen com a filtres per als nous membres potencials, i és una forma de garantir-ne

⁶⁵ Mercè Molist explica que una BBS bàsicament consisteix en un ordinador i un nombre més o menys gran d'usuaris que es connecten a la BBS per mòdem i trucada directa local, interprovincial o internacional, segons l'ordinador al qual es truqui. A la BBS hi ha programes, butlletins, fòrums, xats, correu electrònic... Normalment es demana que els usuaris s'identifiquin amb el nom real i que aportin a la BBS tants arxius com es baixen. Segons el grau de participació en la comunitat, segons el mèrit i qualitat de la informació compartida o segons l'amistat amb el propietari de la BBS, anomenat "sysop" (System Operator), els usuaris tenen diversos nivells i privilegis d'accés. La primera BBS, nascuda el 16 de febrer del 1978, va ser el Chicago Bulletin Board System, obra de Ward Christensen i Randy Suess, que funcionava amb un mòdem de 300 baudis. La majoria d'aquells pioners, avui veterans, eren gent jove que tenia muntada la BBS a la seva habitació i que conformava el primigeni "underground informàtic". Els 80 van ser l'edat d'or de les BBS, que amb la popularització d'Internet van decaure, però no desaparèixer, especialment per la seva qualitat davant formes de comunicació massives com els grups de notícies i llistes de correu d'Internet. Tot i això, moltes han abandonat la vella fórmula de la connexió directa i l'usuari pot entrar-hi a través d'Internet.
<http://www2.grn.es/merce/2003/25bbs.html>

la selecció. Si un operador de sistema (anomenats *sysop* –el qui manté la BBS) no selecciona correctament els usuaris, s'hi podria arribar a infiltrar un policia o un agent del govern. És també responsabilitat del *sysop* donar de baixa a qui no contribueix compartint informació a la BBS; a qui només copia arxius i es descarrega informació (se'ls anomena “esponges”) és esborrat de la BBS. Aquesta desconfiança envers els nous usuaris de les comunitats hackers és fruit dels intents de la policia d'accedir a les BBS's; per això, quan algú al·lega que és periodista o un investigador, se l'expulsa immediatament i passa a formar part de la llista negra que és compartida amb d'altres BBS's de hackers. D'aquí la dificultat d'analitzar el fenomen hacker, i per això cal recórrer a les publicacions i newsletters de hackers, i a articles, així com a comentaris i anàlisis de diversos autors.⁶⁶ Sense voler ser exhaustius, caldria tenir en compte, pel cap baix, els següents directoris o seus web: *Phrack*⁶⁷, contracció de les paraules Phreak i Hack, és la publicació hacker més antiga que existeix (1985) i és reconeguda com la publicació electrònica oficial; l'altra “oficial” és *2600: The Hacker Quarterly*⁶⁸. *Computer Underground Digest*⁶⁹, coneguda com CuD, és una newsletter electrònica setmanal que recull tant articles acadèmics com comentaris de membres de la comunitat underground; es va començar a publicar pel març de 1990; *Digital Murder*⁷⁰, nascuda a l'octubre de 1991 és una newsletter de hacking/phreaking en general; *FBI* (Freaker's Bureau Incorporated)⁷¹ és també una newsletter general. *Hackers Unlimited*⁷² va començar el desembre de 1989; *MAGIK* (Master Anarchists Giving Illicit Knowledge)⁷³, del 1993; *The New Fone Express*⁷⁴, del juny de 1991; *P/HUN*: (Phreakers/Hackers Underground Network)⁷⁵, és una de les més conegudes i antigues, ja que va començar el 1988; *NARC* (Nuclear Phreakers/Hackers/Carders)⁷⁶, també és de les antigues, del 1989; *TAP ONLINE* (Technical Assistance Party) es va establir el 1972 com a *YIPL* (Youth International Party Line) por Abbie Hoffman, y poc després va canviar el seu nom per TAP, per a Meyer⁷⁷ és l'àvia de les publicacions

⁶⁶ Veure, per exemple, Jeff Humphrey i Bruce C. Gabrielson: *Phreaks, Trashers and Hackers*, Presented at AFSEA INFOSEC Engineering Course, June 1995, Burke, VA. <http://www.blackmagic.com/ses/bruceg/hackers.html>, o bé *Hacking Answering Machines* 1990 by: Predat0r of Blitzkrieg Bbs 502/499-8933 <http://www.undergroundnews.com/files/texts/underground/hacking/amhack.htm>

⁶⁷ Phrack, <http://www.phrack.org/>

⁶⁸ 2600 The Hacker Quarterly, <http://www.2600.com/>

⁶⁹ Cu digest, <http://www.soci.niu.edu/~cudigest/>. Veure la Computer Underground Digest Archives a <http://www.etext.org/CuD/>

⁷⁰ Digital Murder a <http://www.digitalmurder.org/>

⁷¹ Electronic Magazines: *Freaker's Bureau Incorporated* <http://www.textfiles.com/magazines/FBI/>

⁷² <http://www.geocities.com/newhuo2002/mainwindow1024.html>

⁷³ MAGIK Master Anarchists Giving Illicit Knowledge April 23, 1993 <http://www.etext.org/CuD/Magik/magik-2>

Electronic Magazines: *Master Anarchists Giving Illicit Knowledge* <http://www.textfiles.com/magazines/MAGIK/>

⁷⁴ The New Fone Express, <http://www.etext.org/CuD/NFX/nfx-3>

⁷⁵ P/Hun, <http://www.etext.org/CuD/Phun/phun-1> i també http://www.flashback.se/archive/phun_1

⁷⁶ Electronic Magazines: *Nuclear Phreakers Hackers Carders* <http://www.textfiles.com/magazines/NARC/> i també <http://www.etext.org/CuD/NARC/narc-1>

⁷⁷ Gordon R. Meyer (1989), *The social organization of the computer underground*. Northern Illinois University. <http://sun.soci.niu.edu/theses/gordon>

hackers. Entre les més recents cal esmentar TPP (The Propaganda Press)⁷⁸ del 1999, i NIA (Network Information Access); *LOD/H TECH JOURNALS*⁷⁹ són les publicacions tècniques de LOD/H⁸⁰, el grup d'elit de Legión of Doom. Totes aquestes publicacions poden donar una visió de la diversitat de la cultura informàtica underground, de les seves ètiques, creences i valors, i una part de l'interès radica en el fet que els articles de la majoria d'aquestes publicacions estan redactats pels hackers d'elit.

Per a analitzar la subcultura hacker com una forma de moviment social organitzat, farem servir la teoria de moviments socials desenvolupada per Stewart, Smith i Denton⁸¹, que perfila sis requeriments essencials per a l'existència d'un moviment social. Un grup o activitat es pot definir com a moviment social si té, pel cap baix, una mínima organització, és un col·lectiu no institucionalitzat, proposa un programa per a canviar normes o valors, és contrari a un ordre establert, és ampli en abast, i té la persuasió com a eina bàsica de negociació. Seguint el text probablement anònim de *Rebels amb causa*, atribuït a Tanja Rosteck⁸², apliquem aquests criteris a la subcultura hacker per tal de veure que, certament, constitueix un moviment social.

La cultura hacker té una mínima organització vertebrada per uns pocs líders, que solen ser experts en programació i al voltant dels quals s'ha creat una petita llegenda sobre els seus coneixements i activitats, i una munió de participants que sovint formen grups propis, amb xarxes de connexió a altres grups a través de diversos canals de comunicació. Gordon Meyer⁸³ ha estudiat com els hackers i els membres de l'underground informàtic s'organitzen a través de les BBS's o mitjançant canals il·lícits de comunicació com ara bases de *voice-mail* corporatives i "ponts" telefònics. Aquests mètodes permeten als hackers compartir informació com ara qui ha estat detingut, quins sistemes s'han tancat, nous números a provar, forats de seguretat que han estat descoberts... Tot i que el hacking és una activitat solitària, l'intercanvi d'informació és vital per a poder realitzar les seves pràctiques i tenir sensació de comunitat, per això es troben sovint o bé en petits grups o bé en grans concentracions estatals anomenades "cons" (convencions), organitzades per grups d'elit, que s'anuncien a les BBSs underground o a les publicacions de hackers. Cada convenció té un nom, com la

⁷⁸ The Propaganda Press, <http://www.eiu.org/press/>

⁷⁹ The Syndicate Report, <http://www.etext.org/CuD/Synd/synd-15b>

⁸⁰ Legion of Doom Technical Journals, <http://kontek.net/pi/lod-tj/lod-tj.html>

⁸¹ Charles Stewart, Craig Smith i Robert E. Denton (1984), *Persuasion and Social Movements*. Illinois. Waveland Press.

⁸² Autor desconegut o Tanja S. Rosteck, *Hackers: Rebeldes con Causa*

http://www.internautas.org/documentos/hack_rebe.htm. Veure també

http://cibersociedad.rediris.es/congreso/g11_t1.pdf, que forma part del 1r Congrés online de l'Observatori per a la Cibersocietat.

⁸³ Gordon Meyer (1989), *Social Organization of the Computer Underground* <http://secinf.net/uplarticle/16/gordon.txt>

HoHoCon a Houston, PumpCon a Halloween, o DefCon. Vet aquí un breu extracte dels problemes viscuts a la PumpCon de l'octubre de 1992: "Divendres, 30 d'octubre de 1992, va començar PumpCon, al pati del Marriot, a Greenburgh, Nova York. Fet i fet, es varen concentrar uns 30 hackers, i s'ho varen passar molt bé. Pel cap baix fins la nit del 31 d'octubre, quan 8 o 10 membres de la policia de Greenburgh varen irrompre i varen fer una batuda al Con. A l'hora de la incursió hi havia entre 20 i 25 hackers a l'hotel. Tres de les quatre habitacions llogades per Con foren atacades. Els inquilins d'aquestes habitacions foren duts a la sala de conferències i a l'habitació 255 on els interrogaren durant 6-8 hores. (...) Uns quants hackers que havien sortit a donar un tomb en cotxe mentre tenia lloc la incursió varen tornar unes hores més tard, i la policia els dugué immediatament a la 255 per a interrogar-los (estaven a la recepció quan un poli va aparèixer i els va portar a una habitació). La policia els va preguntar si eren hackers, i en no rebre resposta, un oficial de policia va treure de la butxaca de l'abric d'un d'ells un sintonitzador automàtic. N'hi havia prou per a enviar-los a l'habitació 255 amb la resta de hackers detinguts per a ser interrogats. La meua pregunta és: no és il·legal això? Cerca i captura sense cap causa aparent o una ordre judicial? Ooops –se m'oblidava– som Hackers! Som tots dolents! Estem sempre violant la llei. No tenim drets! L'habitació 255 va ser clausurada. No era permès fumar i tots estàvem molt nerviosos. Foren cridats d'un a un per a ser interrogats, algunes entrevistes duraven 5 minuts, d'altres 30 o 45. (...) Malgrat que la situació era molt seriosa, alguns encara feien bromes dient PumpCon '93 no es farà aquí, oi?".⁸⁴

Com a col·lectiu sense institucionalitzar, el moviment social és sempre un grup marginal i és criticat per no fer servir els canals i procediments adequats. Els hackers han estat considerats sempre un grup marginal en la societat, i sovint es parla d'ells com a solitaris i mancats d'habilitats socials, o són directament perseguits pel poder. "Sóc un hacker". Si alguna vegada ho dic a algú, immediatament es pensarà que sóc dolent, vandàlic, lladre, un pseudo-terrorista que s'apropia dels ordinadors dels altres en benefici personal o probablement per a obtenir alguna satisfacció morbosa esborrant megues i megues de dades valuoses. Se m'associa a l'underground informàtic. Si algun cop ho dic a algú hi haurà un esclat d'associacions estúpides en la ment d'aquesta persona entre jo i la Màfia, amb Saddam Hussein, Síria, Líbia, Abu Nidal i qui sap què més. Quasi sempre, entre la majoria ignorant, nosaltres els hackers som considerats com a brètols perillosos l'únic propòsit dels quals a la vida és el de causar tant dany com ens sigui possible en el menor temps possible al més gran

⁸⁴ PUMPCON BUSTED!!! 10/31/92 written by someone who was there who wishes to remain anonymous
<http://textfiles.fisher.hu/hacking/CONVENTIONS/pumpcon.txt>

nombre de persones. Segur que hi ha aquestes petites criatures (físicament i mentalment) que es fan anomenar hackers i que concorden amb la descripció que acabo de fer. També hi ha gent que es fan dir 'éssers humans' que violen, assassinen, enganyen, menteixen i roben a cada pocs minuts (o són segons ara?). Significa això que tots els éssers humans haurien d'anar a la presó?"⁸⁵. Com s'esdevé en qualsevol grup minoritari, els hackers són tinguts com a proscrits i se'ls nega els recursos socials, econòmics i polítics necessaris per a dur a terme les seves pràctiques. La cultura hacker no forma part de cap institució establerta, tanmateix alguns hackers hi voldrien treballar, per a deixar de ser perseguits i en benefici del propi moviment que deixaria de ser vist com un perill públic.

Com a moviment social, la cultura hacker proposa canvis, en particular volen modificar les actituds del públic massiu envers la tecnologia i creuen, sobretot, que la informació i el coneixement és poder⁸⁶. Si la gent no vol aprendre tot el que pugui sobre tecnologia, estan permetent que l'estat i el poder corporatiu els controli. Recordem que el lema de la publicació de hackers NIA (*Network Information Access*) és "*Ignorance, There's No Excuse*" (Ignorància, no hi ha excusa)⁸⁷. Es fa, doncs, una crida per tal que la gent s'autoeduqui en el tema de la tecnologia, per tal que no sigui utilitzada per a controlar-los. "El sistema informàtic ha estat només a les mans de grans negocis i del govern. El meravellós aparell pensat per a enriquir la nostra vida ha esdevingut una arma que deshumanitza la gent. Per al govern i les grans empreses, la gent no és més que un espai en el disc, i el govern no fa servir els ordinadors per a tenir ajut pels pobres, sinó per a controlar mortals armes nuclears. L'americà mitjà només pot tenir accés a un petit microprocessador que només és una fracció del que paga. Les empreses mantenen els seus equips de luxe fora de l'abast de la gent darrere un mur d'acer de valor i burocràcia increïblement alt. Va ser a causa d'això que va néixer el hacking"⁸⁸. "Molts, si no tots, de nosaltres considerem que la informació hauria de ser intercanviada lliurement (...) si tot el món es manté al dia sobre les noves tecnologies, aleshores tothom se'n podrà beneficiar (...) Com més en sapiguem cadascun de nosaltres, menys errors del passat repetirem, una major base de coneixements tindrem per als desenvolupaments futurs."⁸⁹

⁸⁵ From: Toxic Shock Subject: *Another view of hacking* Date: Sat, 06 Oct 90 03:04:57 EDT The Evil That Hackers Do. "I am a hacker." <http://www.skepticfiles.org/hacker/cud206.htm>

⁸⁶ Dorothy E. Denning (1990), *Concerning Hackers Who Break into Computer Systems*. Proceedings of the 13th National Computer Security Conference, Washington, D.C., Oct., 1990, pp. 653-664. <http://www.cs.georgetown.edu/~denning/hackers/Hackers-NCSC.txt>

⁸⁷ N.I.A. Network Information Access . 15DEC89. *Guardian Of Time*. File 1. <http://www.flashback.se/archive/nia-1>

⁸⁸ Doctor Crash (1986), The Techno-Revolution. *Phrack* 1:6, 10 juny, <https://www.phrack.com/phrack/6/P06-03>

⁸⁹ Toxic Shock, *op. cit.*

Ha quedat ja palès que la cultura hacker és contrària a l'ordre establert, i que l'enemic dels hackers són els qui els volen oprimir, l'estat i les grans corporacions; el hacking, com una forma de protesta socio-política, és difamat i denunciat en els *mass media* per aquestes dues institucions. Insisteixen tant en el tema de la incomprensió com a denunciar l'opressor, oposant-li simplement la passió per aprendre, la creació de coneixement i l'intercanvi d'informació. "Però, fins i tot quan escric això, me'n adono del per què som un grup tan temut... som incompresos per la majoria... No pots entendre a algú que jutja els altres pel que diuen, pensen i fan, en lloc de fer-ho per la seva aparença externa o pel seu gran salari. No pots entendre a algú que vol ser honest i generós, en lloc de mentir, robar i enganyar. No pots entendre'ns perquè som diferents. Diferents en una societat on el conformisme és l'estàndard desitjat. Mirem d'alçar-nos per damunt de la resta, i després ajudar-los a pujar a la mateixa alçària. Mirem d'innovar, d'inventar. Volem, seriosament, anar on ningú ha anat abans. Som incompresos, malinterpretats, desvirtuats. Tot perquè simplement volem aprendre. Nosaltres senzillament volem augmentar el flux d'informació i coneixement, per tal que tothom pugui aprendre i beneficiar-se'n."⁹⁰ Durant el 1989 i 1990 es dugueren a terme massives mesures dràstiques contra els hackers als Estats Units, contra les quals s'aixecaren les veus de nombroses publicacions i butlletins anarquistes que començaren a circular aquests mateixos anys. Les cases de hackers sospitosos foren assaltades, els equips confiscats i moltes sancions imposades. Una de les batudes més espectacular fou duta a terme a Steve Jackson Games, una companyia que produïa jocs de rol de simulació; el llibre que acompanyava un d'aquests jocs, GURPS Cyberpunk, fou confiscat per les autoritats legals acusat de ser un manual per al crim informàtic.⁹¹ Aquestes actuacions policials i judicis contra hackers foren seguits de ben a prop per l'*Electronic Freedom Foundation*, un grup de pressió fundat com a resposta a aquestes mesures repressives.⁹²

L'abast del moviment hacker i el seu nivell d'operativitat és difícil de comptabilitzar, degut sobretot a la manca de rastres que deixen en els sistemes. Tanmateix, s'han fet algunes estimacions sobre el nombre de BBSs que operen actualment –aproximació força imprecisa perquè la majoria de les BBSs hacker són underground i els números de telèfon no estan disponibles– i s'han donat com a xifres aproximades l'existència d'uns pocs centenars de BBSs només als Estats Units (pensem que n'hi ha milers de no undergrounds). El hacking és un fenomen internacional i els seus membres no fan

⁹⁰ Toxic Shock, *op. cit.*

⁹¹ Bruce Strling (1992), *A Statement of Principle*. *Computer Underground Digest* 4:47, 30 setembre 1992
<http://lib.novgorod.net/STERLINGB/catscan10.txt>

⁹² Un estudi de les batudes, acusacions i conflictes legals contra els hackers es pot trobar a Bruce Sterling (1992) *The Hacker Crackdown*, <http://bufetalmeida.com/textos/hackercrack/libro.html>

cap distinció ètnica ni de gènere. De vegades només surten a la llum quan, per la premsa, ens assabentem que un determinat grup ha estat perseguit per la policia o s'han dut a terme interrogatoris o batudes en diferents cases. És el cas del col·lectiu europeu Chaos Computer Club⁹³ amb grups a França, Alemanya i Holanda, força ben organitzat, i considerat com una base de recursos per als altres hackers. Mancats de dades, només ens queda poder llistar els hackers més importants⁹⁴, no tant per establir cap jerarquia, sinó senzillament per a intuir-ne el seu abast: Richard Stallman⁹⁵, Markus Hess⁹⁶, Dennis Ritchie⁹⁷, Ken Thompson⁹⁸, John Draper⁹⁹, Mark Abene¹⁰⁰, Robert Morris, Kevin Mitnick¹⁰¹, Kevin Poulsen¹⁰², Johan Helsingius¹⁰³ i Vladimir Levin¹⁰⁴.

Tot moviment social sense institucionalitzar i amb una mínima organització, ha de posseir una potent força de persuasió per a mantenir als seus membres fidels a la seva ètica i principis. En el cas dels hackers la recompensa és el reconeixement dels iguals; el càstig, la burla i l'expulsió del grup. Així, per exemple, l'Inner Circle, un grup de hackers d'elit creat per Bill Landreth, comparteix unes normes, similars a l'ètica del hacker, estrictament imposades, com el principi bàsic del respecte a la propietat i a la informació d'altra gent i la consegüent prohibició de fer malbé arxius d'ordinadors. La cultura hacker està fent esforços per apropar-se a la indústria corporativa, oferint-se a compartir els seus coneixements i habilitats per a crear una millor tecnologia per a tothom; però només s'han fet alguns experiments amb la contractació de hackers per part de companyies per a comprovar els seus sistemes, amb resultats molt positius. Si aquesta col·laboració no s'estén, no té altra causa que les relacions de poder i el control econòmic i polític.

Ens trobem, doncs, davant d'un col·lectiu, nou i poc estudiat que, malgrat la seva marginalitat, aporta un desig intel·lectual, una recerca de coneixement, una expertesa informàtica, i una ètica basada en el fet de prioritzar la llibertat de la informació i la passió creativa per davant dels diners i el treball, que caldria incorporar en la

⁹³ <http://berlin.ccc.de/> (pàgina temporalment tancada). Veure *Manifestations contres les Brevets Logiciels*, Brussel·les 27 août <http://swpat.ffii.org/news/03/demo0819/index.fr.html>, <http://www.ccc.de/camp/>

⁹⁴ Hackers – Hall of Fame, <http://www.mat.uni.torun.pl/~kombo/hack/hof.html>

⁹⁵ Pàgina principal de Richard Stallman <http://www.stallman.org/>

⁹⁶ Pàgina principal de Markus Hess, <http://www.namebase.org/main3/Markus-Hess.html>

⁹⁷ Pàgina principal de Dennis M. Ritchie <http://www.cs.bell-labs.com/who/dmr/>

⁹⁸ De l'enciclopèdia Wikipedia http://es.wikipedia.org/wiki/Ken_Thompson Entrevista 1999 <http://www.computer.org/computer/thompson.htm>

⁹⁹ Pàgina principal de John Draper <http://www.webcrunchers.com/crunch/>

¹⁰⁰ Pàgina principal de Mark Abene, http://livinginternet.com/?i/ia_hackers_abene.htm

¹⁰¹ <http://www.freekevin.com/> i també <http://www.takedown.com/bio/mitnick.html>

¹⁰² Free Kevin, www.kevinpoulsen.com/ i també http://livinginternet.com/?i/ia_hackers_poulsen.htm

¹⁰³ Johan Helsingius, <http://www.julf.com/> Entrevista a *Wired*

<http://www.wired.com/wired/archive/2.06/anonymous.1.html>

¹⁰⁴ Vladimir Levin: *Internet Hackers*, http://livinginternet.com/i/ia_hackers_levin.htm

construcció de la societat de la informació si es vol que aquesta sigui lliure i democràtica. “Ho sàpigues o no, si ets un hacker, ets un revolucionari”.¹⁰⁵

5. Art, tecnologia i activisme artístic

Des de sempre, l'esdevenir de l'art, el seu significat i funció, han estat interrelacionats amb els avenços científics i el desenvolupament tecnològic. Recordem només com les lleis de la perspectiva, l'estudi de la llum i la fotografia o la relativitat i la teoria de la complexitat han incidit en el Renaixement, l'impressionisme, les avantguardes o la postmodernitat. No només es tracta de fer servir una determinada eina o d'estar al dia utilitzant el darrer avenç tècnic: la interacció tecnologia-art no es limita a l'adopció d'un mitjà de producció que ofereix més possibilitats constructives o destructives, sinó a la formulació del nou llenguatge que porta associat, i a la cerca de significació dins dels nous contextos socials. L'emergència d'una nova teoria científica o l'apropiació social d'una determinada tecnologia sol anar acompanyada de noves formes de pensament i d'una percepció diferent de la realitat. I l'artista també pot participar en la construcció i investigació d'aquesta nova realitat mitjançant l'ús de les noves eines i conceptes.

Recordem l'anàlisi que Walter Benjamin fa a la seva *Petita història de la fotografia*, on descriu, a partir de la popularització de la tècnica fotogràfica, un retrat canviant de la societat de la segona meitat del segle XIX, tant pel que fa al comportament de les classes socials com a la convulsió que va provocar entre els artistes (entre els partidaris de l'ús del nou mitjà com a eina prèvia al quadre i els detractors que negaven validesa artística a una imatge feta per la llum i no per la mà de l'home). El retrat, per exemple, va deixar de ser un privilegi de l'alta burgesia per a esdevenir un objecte accessible a tothom, i les fotografies podien arribar a tots els públics gràcies a les reproduccions.

Quan el 1936 Benjamin va escriure *L'obra d'art a l'època de la seva reproductibilitat tècnica*, prenia precisament les possibilitats de reproductibilitat de la fotografia per articular un discurs sobre la funció política de l'art. En un context de domini del feixisme i d'un capitalisme monopolista deshumanitzat, i tenint en el marxisme el referent ideal de realització dels principis de solidaritat, igualtat i democratització, escrivia en el Prefaci: “El capgirament de la superestructura, que avança més lentament que no pas el de la infraestructura, ha hagut de menester més de mig segle per fer

¹⁰⁵ Doctor Crash (1986), The Techno Revolution. *Prack* 1:6, 10 juny <http://www.chscene.ch/ccc/phrack/006/003.htm>

palès en tots els camps de la cultura el canvi de les condicions de producció. (...) Els conceptes que en tot el que se segueix són introduïts per primera vegada en la teoria de l'art es distingeixen dels usuals pel fet de ser del tot inutilitzables amb vista a les finalitats del feixisme. Per contra, són utilitzables per a la formació d'exigències revolucionàries en el camp de la política cultural.”¹⁰⁶

La tecnologia i la possibilitat que atorga de còpia il·limitada, eliminaria molts dels atributs que havien fonamentat històricament el valor de l'obra d'art i, amb ells, el caràcter elitista restringit a les classes dominants. Gràcies a les possibilitats de còpia i multidifusió, l'art perdria els seus atributs burgesos d'autenticitat, de valor de canvi, de ritual i de culte, en definitiva, la seva aura; es perdria la unicitat de l'objecte, es produiria un canvi estètic i es redefiniria la funció social de l'art. Amb la reproductibilitat, l'obra perdria, doncs, el seus atributs associats al capital ja que en ells residia el seu valor de canvi i, alhora que disminuiria el seu valor comercial, permetria el coneixement més ampli i la democratització en l'ús i fruïció gràcies a la seva difusió. Per a Benjamin, l'elecció del mitjà implicava un posicionar-se políticament, i l'artista compromès havia d'assumir els nous mecanismes i processos.

Fou el cas del moviment dels anys 70 “Guerrilla TV” inspirat en el llibre de Michael Shamberg i Raindance Corporation¹⁰⁷. Els activistes del vídeo varen lluitar contra el poder polític i institucional dels 70, però, sobretot, contra el poder mediàtic de la TV; i ho varen fer amb les seves mateixes armes, fent servir una tecnologia i uns canals, fins aleshores exclusius del poder. Molts varen creure que el vídeo esdevindria l'eina definitiva per a l'art democràtic; malgrat tot, una dècada més tard, la seva rebel·lió es va anar diluint entre els entramats del poder. Actualment, el potencial comunicatiu i artístic de la xarxa és utilitzat de manera crítica pels activistes. Després de l'eclosió d'Internet, moltes veus –a més d'enunciar la caducitat del vídeo-art- han profetitzat que la xarxa transformarà pregonament l'art i la literatura, així com les figures de l'autor, del receptor, dels museus... Gene Youngblood puntualitzava: “Aquest serà un art de conseqüències diàries, útil, integrat amb la vida de forma utilitària al mateix temps que segueix sent reconegut com a art, independentment de les seves diferències amb qualsevol art conegut fins el moment. La nova pràctica integrarà art, ciència i tecnologia, i per tant, els transcendirà. No serà art ni ciència, sinó una disciplina híbrida per a la qual les distincions no seran rellevants. Involucrarà la investigació estètica en àmbits que abans no eren considerats com pertanyents a l'esfera de l'activitat estètica.

¹⁰⁶ Walter Benjamin: *L'obra d'art a l'època de la seva reproductibilitat tècnica*. Barcelona. Ed. 62. clàssics del pensament modern 9, pàgs. 31-32

¹⁰⁷ *Guerrilla Television*, Michael Shamberg & "Raindance Corporation"; Holt, Rhinehart and Wiston, New York, 1971

Salvarà el cisma existent entre l'art i el món en general, i contribuirà directament a la transformació d'aquest. El paper social del nou artista serà definit d'acord amb les funcions que mantenen unida a la societat; i el nou artista exercirà, certament, un paper vital en l'anticipació del proper pas en la història social".¹⁰⁸

Sense entrar en els aspectes utòpics d'aquestes declaracions, ens cal analitzar com la revolució digital i l'expansió d'Internet ha dotat d'un nou escenari les manifestacions artístiques que centren el seu interès en contextos socials i polítics, és a dir, com, a partir d'Internet, es reconfigura la relació art-política-tecnologia.

Quan parlem d'activisme artístic a Internet no ens referim a obres artístiques que siguin representacions plàstiques o multimèdia per a ser consultades en xarxa, sinó a obres concebudes i realitzades en i per a Internet amb un clar contingut polític; ens referim a fenòmens com el hacktivisme, una forma de protesta política o una performance, que només pot donar-se a la xarxa. "Si et pares en el terme hack ràpidament descobreixes que el hacking és una manera artística de treballar amb un ordinador. En realitat els hackers són artistes (i alguns artistes solen ser hackers)".¹⁰⁹

L'"artivisme" esdevé una tendència cada cop més definida gràcies a projectes com *CCTV (Close Circuit Television)*¹¹⁰ de Heath Bunting¹¹¹, que invita a la reflexió sobre l'ús de les càmeres de vigilància i que permet a l'internauta esdevenir i transformar-se en policia. En la seu d'*irational.org* hi trobem una llarga llista des d'on enllaçar amb projectes interactius, documents sobre artistes, enllaços a altres projectes (Carey Young, Daniel Andujar, Luciana Haill, Marcus Valentine, Rachel Baker). Sovint subversiu, humorístic, filosòfic i poètic, l'artista qüestiona diferents aspectes d'Internet mitjançant els propis mitjans de la xarxa. Hi trobem de tot: hipertext, consum, l'spam, la seguretat, l'explotació del sexe, l'exactitud de la informació, la difusió, la interactivitat... Amb el nom col·lectiu de Glorious Ninth¹¹², Kate Southworth et Patrick Simons, produeixen obres digitals vinculades a l'activisme. La majoria d'artistes d'aquest àmbit tendeixen a utilitzar mitjans subversius en l'expressió d'idees radicals més que no pas una aproximació, més militant, feta de declaracions i d'afirmacions sostingudes. *Who_Owns_Them_Controls*¹¹³ (2001) a l'igual que altres realitzacions de Glorious

¹⁰⁸ Gene Youngblood: "Electronic Café International. El desafío de crear al mismo nivel que destruimos", a Claudia Giannetti (ed) (1998), *Ars Telemática*. Barcelona. L'Angelot. pàg. 43.

¹⁰⁹ Declaració de Cornelia Sollfrank recollida per Tilman Baumgaertel a "Art a Internet: part II", a www.internet.com.uy/vibri/artefactos/art_on_the_internet2.htm

¹¹⁰ CCTV – World Wide Watch, http://www.irational.org/cgi-bin/cctv/cctv.cgi?action=main_page

¹¹¹ Pàgina principal de Heath Bunting, <http://www.irational.org/cgi-bin/cv/cv.pl?member=heath>

¹¹² Seu de Glorious Ninth, <http://www.gloriousninth.com/>

¹¹³ Glorious Ninth: *Who_Owns_Them_Controls*, http://www.gloriousninth.com/who_owns_them_controls.html

Ninth, està constituïda de sons i paraules agrupades en frases que evoquen eslògans. L'obra s'assembla a un cartell polític i des del punt de vista visual recorda un plafó electrònic; des d'aquesta perspectiva, aquesta obra es situa a les antípodes dels plafons publicitaris exteriors que disfressen amb el seu bombardeig el nostre camp de visió. A més, el projecte qüestiona la proliferació de la publicitat a Internet dins l'òptica de la relació entre la propietat tecnològica i el discurs consumista que hi predomina. Les ressonàncies marxistes del projecte en fan el vestigi vague dels eslògans polítics que proliferaven en els règims comunistes. Per altra banda, està clar que els artistes no han volgut aquí combatre una coerció per reemplaçar-la per una altra. Les frases de diferents colors sobre un fons negre se'ns presenten com a dades que es disgreguen. Es superposen unes amb les altres, puguen i rellisquen sobre la superfície negra, es desplacen com les ones. El leitmotiv "*who owns them controls them*" ("qui les posseeix les controla") és alhora una afirmació i una qüestió. Un so ambient retrunyidor serveix per atenuar l'aspecte categòric de les frases. L'ambigüitat està amplificada per la composició visual, els mots de diferents colors s'acumulen i s'entremesclen a mesura dels seus desplaçaments verticals ascendents i descendents. El frasejat de la trama sonora es compon de dos elements: un ascendent, agut i estrident, l'altre un brunzit més greu, com un rumor descendent. L'obra es recolza doncs en un model de paral·lelismes velats entre el que es veu i el que s'escolta. L'internauta es troba amb una pàgina única, sense enllaços. Li sembla impossible de navegar, i es té la impressió de no tenir cap control sobre la informació que desfila per la pantalla. Tanmateix, a l'entrada de la seu, l'internauta veu mots en blanc aparèixer centrats a la part baixa de la pantalla, una lletra a la vegada, com si fos ell o ella qui teclegés. A mesura que apareixen, les lletres queden gravades en el fons negre i donen al conjunt un aire improvisat. S'hi pot llegir "*You can access this in many ways*" ("podeu accedir-hi de diferents maneres"). Després com un missatge secret escrit a la sorra, onades de nous mots rompen, cobreixen les precedents i les escombren. La peça està composta com una música barrejant els elements visuals, els sons i els mots. A la dreta de la pantalla les dades són aglutinades en una banda immòbil de la que se'n destaquen uns elements en fileres horitzontals i verticals a la pantalla. A l'esquerra, la inscripció "*You can access this in many ways*" reapareix en lletres roses, després en contrapès "*themselves*" ("ells mateixos") apareix en gris a la pantalla a cada moviment del cursor, interrompent de cop la trama sonora. Aquí l'internauta és interpellat, els seus moviments deixen rastre i serveixen d'intermediaris entre els pols de control basat en la propietat tecnològica i les altres possibilitats d'accés. Responent a un qüestionari de *Soundtoys*¹¹⁴, Kate Southworth i Patrick

¹¹⁴ Response to questionnaire for Soundtoys, <http://www.soundtoys.net/a/journal/texts/interview/south.html>

Simons afirmen: “A un altre nivell, com en el conjunt dels nostres treballs, aquest projecte s’interessa pels canvis constants que tenen lloc en el nostre món. Sempre hi ha moviments d’una cosa cap a una altra, però si aquests canvis es produeixen molt lentament sovint els ignorem. L’obra canvia sense parar a mesura que els elements que la componen interactuen. Si de vegades sembla que l’activitat sigui monolítica, també tenen lloc canvis monumentals més perceptibles”. L’experiència de *Who_Owns_Them_Controls* passa per la codificació i la descodificació. La seva constant regeneració palesa l’absurditat de la propietat de la informació i del desig de poder enfront de la comunicació. A l’ombra impenetrable del buit (el rerafons negre) hi proliferen el caos, les trampes i les nombroses possibilitats d’experiència.

6. Tipologies d’activisme a la xarxa

Situem-nos en el 1998. El col·lectiu Electronic Disturbance Theater, des de la xarxa, va lluitar pel desenvolupament d’una nova experimentació amb accions de desobediència civil electrònica adreçades contra el govern mexicà; amb el seu software FloodNet va invitar a un grup d’artistes i activistes polítics a fer un gest simbòlic a favor dels zapatistes mexicans. Al mateix any, un jove hacker britànic, conegut com “JF” entrava a unes 300 seues web, canviant i afegint codi HTML, introduint-hi imatges i textos amb missatges antinuclears. Desobediència civil electrònica i hacktivisme s’instal·laven a la xarxa com a manifestacions artivistes (activisme artístic) en contra de la política tradicional. La primera pàgina del New York Times se’n va fer ressò¹¹⁵.

Seguint a Stefan Wray¹¹⁶, mirem de sintetitzar com a Internet s’està produint aquesta confluència d’activisme, art i mitjans informàtics.

6.1. Activisme informatitzat

En els seus orígens hi trobem la primera versió de PeaceNet –aparegut a començament del 1986– que va permetre als activistes polítics comunicar-se els uns

¹¹⁵ Amy Harmon, “‘Hacktivists’ of All Persuasions Take Their Struggle to the Web”, *New York Times*, 31 d’octubre de 1998, sec. A1; també a Carmin Karasic Scrapbook, <http://custwww.xensei.com/users/carmin/scrapbook/nyt103198/31hack.html>

¹¹⁶ Stefan Wray, La desobediència electrònica civil y la world wide web del hacktivismo: la política extraparlamentaria de acción directa en la red. *Aleph*. <http://aleph-arts.org/pens/wray.html>

amb els altres amb rapidesa i facilitat¹¹⁷. L'entorn cibernètic d'aquests primers activistes en línia estava caracteritzat pels serveis de grups d'interès (com PeaceNet), els Bulletin Board Systems, les llistes de correu i els gophers. El text hi és, doncs, l'element predominant. Tot i la introducció de les Interfícies Gràfiques d'Usuari (GUI), el correu electrònic segueix essent l'eina bàsica en el manteniment de xarxes internacionals de solidaritat¹¹⁸.

Entre els estudis que s'han fet sobre la "democràcia electrònica" i la comunicació a través d'ordinadors¹¹⁹, destaca el de Downing, "*Computers for Political Change*"¹²⁰, on es posa de manifest el paper del correu electrònic en la creació i manteniment de xarxes internacionals de solidaritat. A començament dels noranta es podia ja palesar la importància de la comunicació per correu electrònic tant en les lluites predemocràtiques dels estudiants xinesos com en els moviments que propiciaren la dissolució de la Unió Soviètica [no ens ha d'estranyar, doncs, que una de les primeres formes d'art d'Internet sigui, precisament, l'e-mail-art]. Amb l'eclosió d'Internet i l'arribada dels navegadors gràfics, molts són els grups que constitueixen l'activisme informatitzat (és a dir, el que fa servir Internet com a mitjà de comunicació entre activistes), que es caracteritza per defensar el diàleg, el debat i l'accés lliure i gratuït a la xarxa.

6.2. Infoguerra de base

Hi ha un activisme, però, que considera Internet no només com un mitjà o entorn de comunicació, sinó un objecte o entorn d'acció. La infoguerra de base n'és un primer model. El terme infoguerra es refereix a una guerra verbal, una guerra de propaganda, i la infoguerra de base és el primer moviment que vol superar el concepte d'Internet com a àmbit de comunicació i transformar-lo en àmbit d'acció. Aquests activistes són conscients que es troben en un escenari mundial, telepresent més enllà de les fronteres i en molts llocs simultàniament, cosa que produeix una sensació d'immediatesa i d'interconnectivitat a nivell mundial i un desig de passar de les paraules a l'acció.

¹¹⁷ John D.H. Downing, "Computers for Political change: PeaceNet and Public Data Access", *Journal of Communication* 39, n° 3 (estiu 1998), pàgs. 154-162

¹¹⁸ Harry Cleaver, "The Zapatistas and the International Circulation of Struggle: Lessons Suggested and Problems Raised", a Harry Cleaver <http://www.eco.utexas.edu/faculty/Cleaver/lessons.html>

¹¹⁹ Linda M. Harasim (ed.) (1993), *Global Networks: Computers and International Communication*. Cambridge, Mass. MIT Press; Kenneth L. Hacker, "Missing links in the evolution of electronic democratization", *Media, Culture & Society* 18 (1996), pàgs. 213-232; Lewis A. Friedland, "Electronic democracy and the new citizenship", *Media, Culture & Society* 18 (1996), pàgs.185-212; John Street, "Remote Control? Politics, Technology and 'Electronic Democracy'", *European Journal of Communication* 12, n° 1 (1997), pàgs. 27-42

¹²⁰ John D.H. Downing: The INDYMEDIA phenomenon: space-place-democracy and the new Independent Media Centers, <http://www.er.uqam.ca/nobel/gricis/actes/bogues/Downing.pdf>

S'entén per guerra informàtica¹²¹ un fenomen que es basa en l'aprofitament de l'eina informàtica, amb l'objectiu d'afectar, d'alguna manera, els sistemes d'informació de l'oponent per a destorbar o destruir la seva capacitat operativa. Abastaria, segons Widnall i Foglemann, "qualsevol acció per a negar, explotar, corrompre o destruir la informació de l'enemic, protegint-nos de les seves accions i explotant les nostres pròpies funcions d'informació militar".¹²² Per tant, s'ocupa de totes aquelles accions encaminades a obtenir la superioritat en informació sobre un adversari, tant atacant els sistemes físics de transferència i procés d'informació (*Information Systems Warfare*, ISW), com el seu contingut simbòlic i informatiu (*Information Dominance Warfare*, IDW). La guerra informàtica va ser definida com "un conflicte electrònic en el qual la informació és un actiu estratègic vàlid de conquerir o destruir. Els ordinadors i altres sistemes de comunicacions i informació es transformen en dianes atractives per a atacs inicials".¹²³ Segons el Departament de Defensa dels Estats Units, la infoguerra és el conjunt d'accions encaminades a assolir la superioritat d'informació, i afecta la informació, els processos basats en informació, els sistemes d'informació i les xarxes de l'adversari. Així, si la definició de Schwartau es concentra en els mitjans, la del Pentàgon ho estén a les finalitats. La Rand Corporation, centre d'investigació del govern nordamericà pel que fa a la ciberconfrontació, va elaborar un informe el 1996, *Strategic Information Warfare: a New Face of War*¹²⁴, en el que s'identifiquen un conjunt de característiques distintives d'aquest fenomen, que són: el baix cost, ja que l'armament utilitzat consisteix en ordinadors, software i sistemes de comunicació com Internet; límits difosos, atès que en el ciberespai es dilueixen els tradicionals límits entre sectors i/o interessos públics i privats, interns i externs; difícil detecció, ja que les agressions d'infoguerra poden ser fàcilment confoses amb altres activitats (com espionatge), amb errors del hardware o del software, o passar inadvertides; nous sistemes i anàlisis d'informació, atès que els mètodes tradicionals no serveixen per a reconèixer els agressors i els seus modes d'operació; ampli ventall de dianes, atès que poden ser susceptibles d'atacs tots els sistemes connectats informàticament amb l'exterior. A aquestes característiques se n'hi poden afegir tres més: operació remota, ja que una agressió informàtica pot ser executada des de qualsevol lloc, cosa que redueix les possibilitats de detecció dels seus responsables; flexibilitat, perquè pot ser programada per tal que tingui lloc en un dia i hora determinats, o sota determinades

¹²¹ Infowar, http://www.twurled-world.com/Infowar/Update3/Vocabularies_for_iw/_infowar/_infowar.htm

¹²² Widnall, Sheila.E. i Fogleman, Ronald.R., "*Cornestones of Information Warfare*", Washington, Dep. Of the Air Force, 1955 <http://www.af.mil:80/lib/corner.html>

¹²³ Definició de Winn Schwartau, a Paul Taylor, "West faces prospect of hacker warfare", *Financial Times Review on Information Technology*, 2 abril 1997, pàg. 2. citat a Infowar <http://www.ba.ucla.edu/ar/isco/doc/ln2.htm>

¹²⁴ Strategic Information Warfare, <http://www.rand.org/publications/MR/MR661/MR661.pdf>

condicions; multiplicitat de blancs, ja que pot assolir milers d'ordinadors simultàniament i bases de dades interconnectades de tot el planeta.

No hi ha acord sobre les diverses tipologies d'infoguerra. John Arquilla i David Ronfeldt, analistes de la Rand, diferencien guerra de xarxes (netwar) i guerra cibernètica (cyberwar)¹²⁵. La netwar es refereix a "conflictes que tenen lloc entre estats, o a l'interior de societats i que es desenvolupen a través de nodes interconnectats de comunicació, pels quals circula la informació". Bàsicament consisteix a bloquejar o malmetre el que una "població-blanc" coneix, o creu conèixer, sobre ella mateixa i el món que l'envolta; es tracta, doncs, de malmetre la informació que utilitza la "població-blanc". La principal tàctica és l'atac d'informació, que mira de corrompre la informació de l'adversari de manera directa. L'objectiu de la netwar és el pensament i el comportament humà i que la primera i fonamental expressió és la propaganda dels mitjans de comunicació. La principal diferència entre la netwar i la cyberwar és que aquesta es circumscriu al camp militar, és a dir, es tracta d'operacions militars que persegueixen la intercepció o destrucció de sistemes d'informació i comunicacions i l'obtenció de la informació de l'enemic. La cyberwar, com a forma de combat, si bé fa servir tecnologia informàtica vinculada al comandament i control, a obtenció i processament de dades, a les comunicacions i a l'ús de les armes intel·ligents (*smart weapons*), es refereix a la seva utilització per a dur a terme operacions militars típiques. Un exemple paradigmàtic és la Guerra el Golf.

Si prenem com a base un dels treballs més famosos sobre infoguerra, irònicament titulat "*Terrorisme informàtic: pots confiar en la teva torradora?*"¹²⁶, Rathmell¹²⁷ elabora una tipologia basada en la combinació entre les activitats desenvolupades per l'agressor i les tècniques que fa servir. Identifica tres categories on el terrorisme informàtic pot ser un blanc o una eina. La categoria I seria l'aplicació de noves tècniques d'infoguerra a activitats no noves, com ara l'obtenció i processament d'informació, les comunicacions, la propaganda, el blanqueig de diner. La novetat radica en la tècnica utilitzada, com els virus informàtics. La categoria II és l'aplicació de tècniques velles a activitats noves, per exemple sabotatges a centrals i línies de comunicacions, arxius informàtics i bases de dades. La categoria III és l'aplicació de noves tècniques a noves activitats.

¹²⁵ John J. Arquilla and David F. Ronfeldt, "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict" <http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html>

¹²⁶ Matthew G. Devost, Brian K. Houghton and Neal A. Pollard, *Information Terrorism: Can You Trust Your Toaster?* <http://www.crime-research.org/eng/library/Terrorism.htm>

¹²⁷ Andrew Rathmell, "Cyber-terrorism: The Shape of Future Conflict?" *Royal United Service Institute Journal*, October 1997, pp. 40-46.

Després de la Guerra “intel·ligent” del Golf i de la dissolució de la Unió Soviètica va desaparèixer la retòrica de la Guerra Freda com a fonament racional de la intervenció militar en altres països i es va haver de crear una nova doctrina militar; va sorgir, d'aquesta manera, la idea de l'“eix del mal” i l'amenaça de l'infoterrorisme. Un primer model que fonamenta la guerra de la informació el trobem a *Cyberwar is Coming!*¹²⁸, de Ronfeldt i Arquilla, publicat el 1993, i on s'estableix la diferència entre la guerra de la xarxa (netwar), que es refereix a la guerra de propaganda que es dona dins la xarxa, i la ciberguerra (cyberwar) que es refereix a la guerra cibernètica, que depèn d'ordinadors i sistemes de telecomunicació, a la guerra del C4I –Comandament, Control, Comunicació, Computadors i Informació¹²⁹.

Un cas paradigmàtic de guerra a la xarxa és el dels zapatistes mexicans, que ha obligat a replantejar-se els primers models teòrics de netwar, com ho ha fet Harry Cleaver, una de les persones clau del projecte Chiapas95, un servei de distribució de notícies i informació per correu electrònic¹³⁰. L'experiència de les xarxes de solidaritat i la resistència prozapatista en els darrers cinc anys mostra que es tracta d'una guerra de paraules en contraposició a un conflicte armat prolongat. No neguem la presència militar a l'estat de Chiapas, però des del 12 de gener de 1994 es manté l'alto el foc i s'han donat nombrosos intents de negociació¹³¹. Tothom està d'acord en què els zapatistes deuen la seva supervivència en gran art a aquesta guerra de paraules.

El conflicte bèl·lic de la província sèrbia de Kosovo que va tenir lloc el 1999 és citat, sovint, com la primera guerra que es va desenvolupar, en paral·lel, sobre el territori i sobre Internet. Actors governamentals o no, varen fer servir la xarxa per a disseminar informació, difondre propaganda, demonitzar als oponents i sol·licitar suport per a les seves posicions. Internautes d'arreu feien servir Internet per a debatre sobre el tema i intercanviar text, imatges i vidoeclips que no estaven disponibles a través d'altres mitjans. Els hackers es feren notar interferint serveis en ordinadors governamentals i bloquejant les seves seues. A l'abril de 1999, el diari *Los Angeles Times* afirmava que el conflicte de Kosovo estava transformant el ciberespai en “una zona etèria de combat

¹²⁸ John Arquilla and David Ronfeldt: *Cyberwar is Coming!*, <http://www.well.com:70/0/Military/cyberwar> i també <http://www.rand.org/publications/MR/MR880/MR880.ch2.pdf>

¹²⁹ John Arquilla i David Ronfeldt, “Cyberwar is Coming!”, *Comparative Strategy* 12 (abril-juny 1993), pàgs. 141-165, <http://gopher.well.sf.ca.us:70/0/Military/cyberwar>

¹³⁰ Cleaver, Harry (1995), “*The Zapatistas and The Electronic Fabric of Struggle*”, a <http://www.eco.utexas.edu/faculty/Cleaver/zaps.html>

¹³¹ Stefan Wray, “*The Drug War and Information Warfare in Mexico*”. Tesi pel grau de màster per la Universitat de Texas a Austin, Electronic Civil Disobedience Archive 1997, a <http://www.nyu.edu/projects/wray/masters.html>; del mateix autor: “*Towards Bottom-Up Information Warfare: Theory and Practice. Version 1.0*”, Electronic Civil Disobedience Archive 1998, a <http://www.nyu.edu/projects/wray/BottomUp.html>

on la batalla per les ments i els cors és lluitada a través de l'ús d'imatges, llistes de discussió i atacs de hackers".¹³² Anthony Pratkanis, professor de psicologia a la Universitat de Califòrnia, assenyalava: "El que estem veient ara és només el primer round del que serà una important i altament sofisticada eina en les tècniques de la propaganda de guerra (...) els estrategs militars haurien d'estar preocupats".¹³³ Cal remarcar que l'OTAN va intentar silenciar els mitjans de comunicació que difonien la propaganda del govern serbi de Milosevic, però no va bombardejar els proveïdors de serveis d'Internet, ni va clausurar els canals via satèl·lit que duïen Internet a Iugoslàvia. La política era la de mantenir Internet oberta. James P. Rubin, portaveu del Departament d'Estat, deia: "L'accés ple i obert a Internet contribuirà al fet que els serbis coneguin l'espantosa veritat sobre els crims de lesa humanitat perpetrats a Kosovo pel règim de Milosevic".¹³⁴ Durant tot el desenvolupament del conflicte, els serbis tingueren ple accés a Internet. El *Washington Post* informava que, segons fonts oficials d'Estats Units i Anglaterra, el govern de Milosevic va permetre que els quatre proveïdors d'accés a Internet de Iugoslàvia romanguessin oberts, per tal de contribuir a difondre informació falsa i propaganda. Segons aquest diari, Belgrad, amb una població d'un milió i mig d'habitants, tenia unes 100.000 persones connectades a Internet a l'abril de 1999.¹³⁵ Internautes dels dos bàndols enviaren "bombes d'e-mail" (enviament massiu de missatges) contra seus governamentals. El portaveu de l'OTAN, Jamie Shea, va comentar que el seu servidor havia estat saturat cap a finals de març per un individu que els enviava un 2.000 missatges diaris. *Fox News* va informar que quan Richard Clarke, un resident de Califòrnia, va sentir que la seu de l'OTAN havia estat atacada per hackers de Belgrad, va replicar enviant bombes d'e-mail a la seu del govern iugoslau. El *Boston Globe* informava que un grup de hackers nordamericans, anomenat *Team Spl0it*, va entrar a seus governamentals sèrbies penjant-hi textos com "Diguin al seu govern que pari la guerra". El *Kosovo Hackers Group*, una coalició de hackers europeus, va entrar a cinc seus posant-hi anuncis negres i vermells que deien *Free Kosovo*. Per la seva banda, l'agència sèrbia de notícies SRNA afirmava que el grup de hackers serbis *Black Hand* va esborrar totes les dades d'un servidor de la marina americana. Els membres dels grups *Black Hand* i *Serbian Angel* planejaren

¹³² Ashley Dunn, "Crisis in Yugoslavia: Battle Spilling Over the Internet". *Los Angeles Times*, 3 d'abril de 1999. Veure Myriam A. Dunn, *The cyberspace dimension in armed conflict: approaching a complex issue with assistance of the morphological method*, *Information & Security*. Volum 7, 2001, pags. 145-158. http://www.isn.ethz.ch/onlinepubli/publihouse/infosecurity/volume_7/c2/C2_index.htm

¹³³ Dorothy E. Denning, *Activism, hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, <http://www.nautilus.org/info-policy/workshop/papers/denning.html>

¹³⁴ David Briscoe, *Kosovo-Propaganda War*. Notícia de l'agència Associated Press, 17 de maig de 1999, citat per Dorothy E. Denning, *op. cit.* <http://www.ehj-navarre.org/aehj/denning2.html>

¹³⁵ Michael Dobbs, "The War on the Airwaves". *The Washington Post*, 9 d'abril de 1999.

accions diàries destinades a bloquejar i a interferir els ordinadors militars utilitzats pels països de l'OTAN.¹³⁶

Després que l'OTAN bombardegés accidentalment l'ambaixada de Xina a Belgrad, un grup de hackers xinesos foren acusats de penetrar en diverses seus governamentals americanes. L'eslògan "*Down with barbarians*" (Avall amb els bàrbars) va ser penjat a la pàgina de l'ambaixada dels Estats Units a Pequín. Segons el *Washington Post*, el portaveu del Departament d'Interior, va confirmar que els seus experts havien rastrejat els hackers xinesos.¹³⁷

L'1 d'abril del 2001, un avió nordamericà de reconeixement va haver de realitzar un aterratge d'emergència a l'illa xinesa de Hainan després de topat amb un caça xinès que havia sortit a interceptar-lo. La col·lisió i els 11 dies de detenció de la tripulació varen provocar la pitjor tensió entre Beijing i Washington des del bombardeig accidental de l'ambaixada xinesa a Belgrad. El conflicte va acabar el 3 de juliol, quan les darreres peces de l'avió espia foren transportades a les Filipines. Durant el conflicte va tenir lloc un important conflicte virtual entre hackers xinesos i nordamericans. Segons un article publicat a *Wired* el 18 d'abril del 2001, el grup de hackers dels Estats Units *PoisonBOX* va atacar pel cap baix un centenar de seus xineses des del 4 d'abril¹³⁸. Segons la mateixa font, un hacker conegut com *PrOphet* (que figura a la llista d'Attrition.org¹³⁹ com a responsable del hacking de dues seus xineses) va instar els hackers dels Estats Units a desencadenar l'infern sobre els servidors xinesos. Al seu torn, la *Hackers Union of China*¹⁴⁰ es va autoadjudicar diferents atacs a empreses de comerç electrònic, i en alguna web van aparèixer missatges del tipus *China have atom bombs too*¹⁴¹. A través d'un article difós en un grup de notícies sobre seguretat informàtica, Brian Martin, de l'Attrition.org, va treure credibilitat a la informació periodística que es publicava sobre aquest tema: "Si un observa tant la trajectòria de prOphet com la de poisonb0x, queda clar que cap dels dos té una agenda política. Varen passar 10 dies entre l'incident de l'avió espia i la publicació del primer article a *Wired*. Durant aquest lapsus de temps, cap grup va fer cap referència política. Fou només després dels

¹³⁶ Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* http://www.carta.org/campagne/scienza_tecnologia/hacker/Activism.htm

¹³⁷ Stephen Barr, *Anti-NATO Hackers Sabotage 3 Web Sites*. *Washington Post*, 12 de maig de 1999 <http://www.wired.com/news/politics/0,1283,43134,00.html>

¹³⁸ Michelle Delio, "Crackers Expand Private War". *Wired News*, 18 d'abril 2001

<http://www.wired.com/news/politics/0,1283,42982,00.html>

¹³⁹ La seu d'Attrition.org, <http://www.attrition.org>, actualitza una llista amb les seus hackejades de tot el món, i és considerada la font més fiable d'informació i estadístiques sobre el tema.

¹⁴⁰ Veure a CNN.com *Feds warn of May Day attacks on U.S. Web sites*

<http://www.cnn.com/2001/TECH/internet/04/26/hacker.warning/>

¹⁴¹ Ariana Eunjung Cha. Chinese Suspected of Hacking U.S. sites. *Washington Post* Staff Writer, 13 d'abril 2001 <http://cert.uni-stuttgart.de/archive/isn/2001/04/msg00083.html>

articles de Wired que un seguit d'actes de hacking foren interpretats en aquest sentit. Clarament Wired va agafar una història sense substància i va crear notícies del no res (...) la veritat és que no es pot verificar si realment els atacs foren fets per hackers xinesos o per qualsevol altra persona que vulgui inflamar la situació".¹⁴²

La guerra de la informació¹⁴³ ha arribat a la comunitat d'art digital, ja que fou el tema principal del festival anual Ars Electronica de Linz, Àustria. A diferència de l'activisme informatitzat, la infoguerra de base té un caràcter més intens, s'apercep als qui hi participen com una força comuna, i manifesta el desig d'incitar a l'acció a escala mundial.

6.3. Desobediència civil electrònica

Aquesta expressió, "Desobediència Civil Electrònica" fou encunyada per un grup d'artistes anomenat Critical Art Ensemble, que publicaren, el 1994, el primer llibre sobre el tema, *The Electronic Disturbance*, i el 1996 *Electronic Civil Disobedience and Other Unpopular Ideas*¹⁴⁴. Ambdues obres estan dedicades a un estudi teòric de com traslladar les protestes del carrer a Internet. Una estratègia clàssica de desobediència civil ha estat la de bloquejar l'accés, amb el cos dels propis manifestants, a les oficines o edificis, o bé ocupar les instal·lacions o el carrer amb segudes. Doncs bé, la DCE¹⁴⁵, com una forma d'acció massiva directa, electrònica i descentralitzada, utilitza el bloqueig i les segudes virtuals, a les quals s'hi pot participar de casa estant, o des del treball o de qualsevol punt de la xarxa.

L'activisme on line es mostra en el col·lectiu @Tmark¹⁴⁶, que proposa un seguit d'accions de sabotatge creatiu contra les multinacionals i els polítics, parodiant en *mirrors* les pàgines oficials de polítics i corporacions, i sobretot amb el grup Critical Art Ensemble¹⁴⁷ que amb *Diseases of Consciousness*¹⁴⁸, produït per al museu Walter Phillips Gallery, ens parla de les malalties de l'ànima, típiques de finals del segle XX, amb humor negre. L'ús d'imatges mediàtiques suggereix que les malalties de la consciència humana provenen dels personatges artificials creats pels mitjans que

¹⁴² Brian Martin, *Cyberwar with China: Self-fulfilling Prophecy* <http://www.attrition.org/security/commentary/cn-us-war.html>

¹⁴³ Gerfried Stocker i Christine Schopf (eds.) (1998), *InfoWar*. Viena. Springer. Ars Electronica Festival 1998 a <http://www.aec.at/infowar>

¹⁴⁴ cfr. la pàgina principal del Critical Art Ensemble a <http://www.critical-art.net/>

¹⁴⁵ Stefan Wray, "On Electronic Civil Disobedience", *Peace Review* 11, nº 1, (1999); Electronic Civil Disobedience archive 1998, a <http://nyu.edu/projects/wray/oecd.html>

¹⁴⁶ Seu de @TMark, <http://rtmark.com/>

¹⁴⁷ Seu de Critical Art Ensemble, <http://www.critical-art.net/>

¹⁴⁸ Critical Art Ensemble: *Diseases of Consciousness*, <http://www.t0.or.at/cae/doc/doc.htm>

influencien i alteren la identitat dels espectadors, mentre que ells es contempen a través dels prismes d'aquestes noves imatges culturals. A través dels seus projectes, el col·lectiu Critical Art Ensemble ha desenvolupat una mirada crítica sobre les noves tecnologies i el seu impacte en la consciència individual i social. *Flesh Machine*¹⁴⁹ (1997) es centra en les relacions entre les tecnologies de reproducció i les seves conseqüències a nivell polític i social. Un seguit d'imatges i d'afirmacions revelen allò que s'amaga darrere l'ideal de perfecció corporal: un mercat d'òrgans humans, el control sobre el codi genètic dels individus, la invasió de la vida privada. El col·lectiu posa en evidència com el sistema capitalista també ha posat preu al cos dels individus i al seu desig de perfecció.

Després de la massacre d'Acteal, a Chiapas, a finals de 1997, en la que 45 indígenes foren assassinats, la DCE va deixar de ser una mera teorització hipotètica per a concretar-se en una concepció d'Internet com a mitjà de comunicació i com a àmbit d'acció directa, com a via per a una política oberta a les tàctiques extraparlamentàries. I a començament de 1998, el petit col·lectiu autodenominat Electronic Disturbance Theater¹⁵⁰, va crear un software anomenat FloodNet, que és un aplet de Java que contínuament envia comandament de *reload*: d'aquesta manera, quan un nombre prou alt d'internautes apunten simultàniament la URL de FloodNet¹⁵¹ contra la seu d'un oponent, una massa crítica de missatges bloqueja el seu servidor. El 9 de setembre de 1998 l'EDT va presentar el seu projecte SWARM¹⁵² a l'Ars Electronica Festival dedicat a la guerra de la informació, i es va llençar un atac a les seus web de la presidència mexicana, la borsa de Frankfurt i el Pentàgon, per a donar testimoni del suport internacional als zapatistes, contra el govern mexicà, contra l'exèrcit dels EE.UU. i contra un símbol del capitalisme internacional. Unes 20.000 persones d'arreu es varen connectar al navegador FloodNet entre el 9 i el 10 de setembre¹⁵³ i van atacar les seus del president Zedillo, el Pentàgon i la borsa de Frankfurt, enviant 600.000 hits per minut a cadascuna d'elles. En relació amb l'impacte dels atacs, Ricardo Domínguez afirmava: "El zapatisme digital és i ha estat un dels usos d'Internet políticament més efectius que coneixem. Ha creat una xarxa de distribució d'informació amb 100 o més nodes autònoms de suport. Això ha permès a l'Exèrcit Zapatista d'Alliberament Nacional parlar al món sense haver de passar pel filtre dels mitjans dominants. Els

¹⁴⁹ Critical Art Ensemble: *Flesh Machine*, <http://www.critical-art.net/biotech/biocom/index.html>

¹⁵⁰ Electronic Civil Disobedience, <http://www.thing.net/~rdom/ecd/ecd.html>

¹⁵¹ Brett Stalbaum, "The Zapatista Tactical FloodNet", a Electronic Civil Disobedience Web Page 1998, <http://www.nyu.edu/projects/wray/ZapTactFlood.html>

¹⁵² Ricardo Domínguez, "SWARM: An ECD Project for Ars Electronica Festival '98", a <http://www.thing.net/~rdom> i Electronic Disturbance Theater, "Chronology of SWARM", <http://www.nyu.edu/projects/wray/CHRON.html>

¹⁵³ Veure la crida de l'Electronic Disturbance Theater per a la Desobediència Civil Electrònica el 22 de novembre de 1998 a <http://www.thing.net/~rdom/ecd/November22.html>

zapatistes foren elegits per la revista Wired com un dels 25 grups online més importants el 1998".¹⁵⁴ Tot va començar pel gener de 1998, quan un grup activista italià anomenat Anonymous Digital Coalition va fer circular la proposta de dur a terme un bloqueig virtual sobre cinc seus d'entitats financeres mexicanes. Sugerien que si molts internautes premien el "reload" del seu navegador diverses vegades seguides, les seues web podrien ser efectivament bloquejades. Basant-se en aquesta teoria d'acció simultània, col·lectiva i descentralitzada sobre una seu determinada, Brett Stalbaum, de l'EDT, va dissenyar el FloodNet, que automatitzava la tasca de recarregar les seues escollides.¹⁵⁵ Segons Stalbaum, el Pentàgon fou escollit perquè es creu que l'exèrcit dels Estats Units va entrenar els soldats que dugueren a terme diversos abusos contra els drets humans a Llatinoamèrica. Per la mateixa raó va ser elegida l'Escola de les Amèriques. La borsa de Frankfurt va ser escollida "perquè representa el rol del capitalisme en la globalització utilitzant les tècniques del genocidi i la neteja ètnica, que està a la rel dels problemes de Chiapas. La gent de Chiapas hauria de tenir un rol preponderant cara a determinar el seu destí, en lloc de ser forçada a una reubicació a punta de pistola, fet que és actualment finançat pel capital occidental."¹⁵⁶ Els integrants de l'EDT varen distribuir el nou software a través d'Internet; tot el que els interessats a participar en aquestes accions havien de fer era visitar una de les seues de FloodNet, i en fer-ho, el seu programa de navegació es baixava el software (un applet de Java), que accediria a la seu elegida com a objectiu diverses vegades per minut. A més, el software permetia als manifestants deixar les seues proclames a l'*error log* del servidor de la seu agredida. Per exemple, en apuntar els seus navegadors envers un arxiu no existent com ara human-rights en el servidor atacat, aquest enviava, i emmagatzemava, el missatge *human-rights not found on this server* (drets humans no trobats en aquest servidor). Quan els servidors del Pentàgon detectaren la "invasió", varen llençar una contraofensiva contra els navegadors dels usuaris, redireccionant-los a una pàgina amb un applet anomenat HostileApplet, que es descarregava als seus navegadors i els feia recargar un mateix document sense parar fins que l'usuari apagava l'ordinador. La borsa de Frankfurt no es va veure afectada ja que, habitualment, reben uns sis milions de visites al dia, amb el que aquesta càrrega addicional no els va generar inconvenients. Tampoc va reaccionar la seu del president Zedillo, però en un nou atac el juny de 1999 va contraatacar amb un software que provocava que els navegadors dels internautes obrissin finestres de manera consecutiva fins que obligava a apagar l'ordinador. Ricardo Domínguez, en un

¹⁵⁴ Entrevista publicada a la seu de l'EDT <http://www.thing.net/~rdom/ecd/ecd.html>

¹⁵⁵ Stephan Wray, *The Electronic Disturbance Theater and Electronic Civil Disobedience*, 17 de juny de 1998, <http://www.thing.net/~rdom/ecd/EDTECD.html>

¹⁵⁶ Dorothy E. Denning: *Hactivism: An Emerging Threat to Diplomacy*. Article publicat a la seu de l'American Foreign Service Association, <http://www.afsa.org/fsj/sept00/Denning.cfm>

missatge enviat a un fòrum d'activistes, cita una frase que explica el vincle entre artistes i activistes: "Els historiadors de l'art saben que els grans i famosos genis del renaixement no només crearen pintures i edificis, sinó que a més dissenyaren fortalezes i construïren màquines de guerra. Si el fantasma de la guerra informàtica es fes realitat, els hackers farien el paper dels històrics artistes-enginyers."¹⁵⁷

6.4. Hacktivisme

S'anomena hacktivisme la convergència del hacking amb l'activisme social o polític. Els seus orígens es remunten a mitjan anys vuitanta, amb la primera versió de PeaceNet, una xarxa electrònica mundial dedicada a la pau, la justícia social i econòmica, els drets humans i la lluita contra del racisme, que va aparèixer el 1986 i que va permetre als activistes polítics comunicar-se els uns amb els altres amb relativa rapidesa i facilitat. A més de les accions de DCE a la via d'accés de la seu web, durant 1998 també es van dur a terme cops hacker contra la seu web del govern mexicà, introduint-hi missatges polítics¹⁵⁸. Es tracta d'una tàctica específica per accedir i alterar les seus web de la xarxa, tal com ho va exemplificar el hacker britànic "JF" i com recull l'edició d'octubre de l'*Ottawa Citizen* i el *New York Times*.¹⁵⁹

Una distinció bàsica entre les activitats hacker polititzades i les de la DCE, és que els agents d'aquesta darrera no amaguen els noms i operen lliurement; en canvi, els hackers desitgen romandre en l'anonimat (ja que els riscos són més alts, atès que algunes accions són, sens dubte, il·legals) i, segurament, les seves accions són fetes per individus de forma aïllada. La naturalesa secreta, privada, poc publicitada i anònima de les accions hacker polititzades, ens fan pensar que no es tracta d'una política de mobilització, ni d'una política que requereixi la participació de la massa. Amb tot, el hacktivisme sembla involucrat en accions obertament polítiques i en una actitud de liberalitzar la informació. No hi ha consens, però, sobre el hacktivisme i la seva possible evolució; és possible parlar de codis ètics hacker¹⁶⁰, com la prioritat a l'accés gratuït i lliure per a tothom, però no hi ha una perspectiva hacker monolítica (alguns hackers han criticat el projecte FloodNet al·legant que bloqueja l'amplada de banda).

¹⁵⁷ La frase citada per Domínguez, el 26 de maig de 1998, pertany a un jove activista alemany anomenat Frederich Kittler. Veure <http://www.aec.at/infowar/NETSYMPOSIUM/ARCH-EN/msg00138.html>

¹⁵⁸ "Mexico rebel supporters hack government home page", *Reuters*, 4 febrer de 1998. També a <http://www.nyu.edu/projects/wray/real.html>

¹⁵⁹ Bob Paquin, "E-Guerrillas in the mist", *The Ottawa Citizen*, 26 d'octubre de 1998. <http://www.ottawacitizen.com/hightech/981026/1964496.html>

¹⁶⁰ Pekka Himanen (2003), *L'ètica del hacker i l'esperit de l'era de la informació*. Barcelona. Ed. UOC i Pòrtic.

La tasca dels hackers consisteix a infiltrar-se a les xarxes del poder per a obtenir informació, inocular falsa informació o destruir la que troben; ja no es tracta de descentralitzar la informació, sinó de capturar-la, anul·lar-la o subvertir-la. Per això Laura Baigorri¹⁶¹ els compara amb l'esperit estratègic del filòsof-guerrer Sun Tzu (segle V ane), el qual a l'*Art de la Guerra*¹⁶² exposa, en forma de dos principis, que la màxima eficiència és fer que el conflicte esdevingui innecessari: l'art de la guerra es basa en l'engany i el suprem art de la guerra consisteix a sotmetre l'enemic sense lluitar. I per aconseguir-ho proposa infiltrar-se en els secrets de l'enemic i canviar-lo des de dins. La supervivència del hacker es troba en la seva creativitat (l'ús que fa de la xarxa per assolir els seus objectius subversius), en la seva habilitat per desaparèixer sense deixar rastre i en la seva capacitat per a reorganitzar un nou atac. Estem parlant, òbviament, de les Zones Temporalment Autònomes (TAZ): "El TAZ és com una revolta que no s'enganxa amb l'Estat, una operació guerrillera que allibera una àrea i s'autodissolt per a reconstruir-se en qualsevol altre lloc o temps, abans que l'Estat la pugui aixafar (...) La seva força resideix en la seva invisibilitat. Tan aviat com un TAZ és nomenat –representat i mediatitzat– ha de desaparèixer, desapareix de fet, deixant rere seu un buit, ressorgint novament en un altre lloc, i invisible de nou en tant que indefinible per als termes de l'Espectacle. (...) El TAZ és un campament de guerrillers ontològics: colpegen i corren".¹⁶³

Tot un seguit d'obres de Net.art es podrien integrar dins l'apartat de hacktivistes, en el sentit de l'actitud i el compromís polític envers la creació artística, o per l'anàlisi crítica que fan de la pròpia xarxa. Anem a comentar algunes de les més significatives que, de retruc, ens mostraran els principals aspectes de l'estètica artista.

Cal començar per Heath Bunting¹⁶⁴ que, juntament amb Vuk Cosic, és el hacker i activista per excel·lència d'Internet. Les seves activitats abasten des de graffiti, ràdio pirata, performances, intervencions públiques... És el responsable d'irational.org i de cibercafe, una BBS per a l'art i el hacking. Al llarg de la seva trajectòria es veu una clara actitud contra els multimèdia, rebuig als plug-ins i a l'alta tecnologia. El seu projecte *Visitor's Guide to London*¹⁶⁵, presentada a la Documenta de Kassel, tot i estar feta amb un potent ordinador sembla que s'hagi utilitzat baixa tecnologia:

¹⁶¹ Laura Baigorri: *El futuro ya no es lo que era*, a <http://www.aleph-arts.org/pens/baigorri.html>

¹⁶² Sun Tzu: *El arte de la guerra*, <http://www.gorinkai.com/textos/suntzu.htm>

¹⁶³ Hakim Bey (1996), *TAZ. Zona Temporalmente Autónoma*. Madrid. Ediciones Talasa També a *Acción Paralela* n.3, Valencia, 1998. Originalment TAZ. The Temporary Autonomous Zone, Antological Anarchy, Poetic Terrorism, a *Autonomedia*. URL: http://www.hermetic.com/bey/taz_cont.html

¹⁶⁴ Heath Bunting, <http://www.irational.org/cgi-bin/cv/cv.pl?member=heath>

¹⁶⁵ *Visitor's Guide to London*, <http://www.irational.org/london/front.html>. Veure també <http://www.irational.org/heath/london/>

originàriament va ser creat per a ser emmagatzemat en un disquet. Defineix aquesta guia com a "*the official irrationalists guide to London*". L'obra està feta a partir de mapes d'imatge, totes elles bitmaps, que mostren llocs no turístics de la ciutat de Londres. Bunting recicla símbols i llenguatge de la societat electrònica a la recerca del seu propi llenguatge visual de navegació. A més, aquesta preferència per la baixa tecnologia l'ha dut a recollir i reciclar hardware real obsolet com mòdems i ordinadors dels contenidors. Explora, críticament, el concepte de la realitat urbana, en una exploració virtual amb diferents punts de vista, en una aproximació distanciada de la realitat. L'obra presenta vistes de la ciutat de Londres, en una estètica que tracta de reproduir la fotografia en blanc i negre sense massa detall. S'obre a l'internauta a través d'un portal amb una vista convencional de Londres, la vista del Parlament des de l'altra banda del riu. Hi ha a més algunes icones: un esquema amb els punts cardinals, com el que surt als mapes, una línia en forma de ziga-zaga, una figura humana. En accedir al símbol de l'orientació, apareix una estranya massa de claus angleses i alguns números. El simbolisme de la representació no és clar, ja que és evident que tot i que sembla mantenir el format que podríem pensar en una guia urbana penjada a Internet conté elements discordants. Fent clic sobre l'esquema amb la icona dels punts cardinals apareix una vista; també una sèrie de lletres que són les inicials de certs punts cardinals. D'aquesta manera cada vegada que fem clic en alguna de les lletres apareix una nova vista, com si ens traslladéssim per la ciutat. Les vistes són arquitectòniques, en general sense persones, encara que hi ha alguna excepció. La impressió que sembla voler transmetre és el passeig per una ciutat, de la mateixa forma que ho podríem fer en un autobús, fent fotografies a l'atzar. Però ja hem dit que per altra banda, hi ha elements estranys, intel·ligibles o desconcertants. Per exemple, accedint a la icona de la figura humana, apareix en la mateixa estètica de blanc i negre símbols, uns ulls, una mà...; o fent clic sobre la silueta humana apareixen lletres que formen un missatge sense sentit, acompanyades de fletxes direccionals que no porten la navegació enlloc. L'estructura de l'obra però és senzilla; quan es progressa en una determinada direcció, després d'un cert nombre de fotografies, s'arriba a un final; cal escollir una nova direcció per seguir. Aquesta obra centra molt les preocupacions de Bunting; i la forma de treballar a la xarxa. No hi ha realment cooperació de l'internauta en la construcció de l'obra, ni aplica tecnologia o explora la ciberpercepció. De fet l'estructura és relativament simple, i els mitjans modestos. En canvi és important la connectivitat. Bunting pretén fer participar l'usuari d'una exploració virtual per la ciutat, a l'atzar, de la mateixa manera que podria ser a la vida real, però amb la irrupció d'elements irracionals, que suggereixin una sensació d'estranyesa.

El 1996, amb motiu d'una exposició a Hamburg, Daniel García Andújar comença a desenvolupar el projecte *Technologies to the People*¹⁶⁶ que, fins ara, s'ha presentat en diversos suports (la xarxa, cederom i instal·lacions), i on, amb ironia i amb l'ús d'estratègies de presentació de les noves tecnologies de la comunicació, qüestiona les promeses democràtiques i igualitàries d'aquests mitjans i critica la voluntat de control que amaguen rere la seva aparent transparència. Partint de la constatació que les noves tecnologies de la comunicació estan transformant la nostra experiència quotidiana, Daniel García Andújar crea una ficció amb la finalitat de conscienciar-nos de la realitat que ens envolta i de l'engany d'unes promeses de lliure elecció que esdevenen, irremissiblement, noves formes de control i desigualtat. *Technologies to the People* ® és un *work in progress*, una metàfora sobre la utilització de les tecnologies, a més d'una provocació pública. "Estic creant una companyia virtual que només existeix com a projecte artístic, operant, en realitat, per a la resta de la societat. *Technologies to the People* ® treballa amb la infraestructura mediàtica de les grans empreses i, com a part de la seva política de representació, patrocina esdeveniments artístics. Està adreçada a les persones de l'anomenat tercer món, així com als "sense llar", els orfes, expatriats o els aturats, als grups marginals, als fugitius, als immigrants, als alcohòlics, als drogodependents, a la gent amb trastorns psíquics i a qualsevol que respongui a la descripció d'"indesitjable", a tots aquells deslligats de la societat i incapaçs de trobar un lloc segur on viure, a tots els que demanen almoina per a subsistir. Està adreçada a les persones a les que es nega l'accés a la nova societat de la informació i a les noves tecnologies, a tots els que viuen constrenyits pels límits que marquen noves i estranyes barreres. TTTT vol facilitar el teu accés a la societat de la informació. TTTT vol que més persones formin part de la xarxa. TTTT ha dissenyat i creat *Street Access Machine* ® específicament per als grups minoritaris abans citats. La màquina està a la seva disposició les 24 hores del dia i es pot utilitzar amb qualsevol tarja de crèdit (ciberefectiu) [...] Amb només instal·lar el teu *Street Access Machine* ® s'acabaran per sempre tots els problemes de la mendicitat. Les persones que vulguin donar diners només necessiten tenir una tarja de crèdit i especificar la quantitat de diner de la que estan disposats a prescindir. L'indigent pot llavors treure diners d'un caixer fent servir la seva *Recovery Card* ® amb una contrasenya. Fàcil d'utilitzar i sense interessos. Un servei global de targes de crèdit per a tothom sense excepció".¹⁶⁷ La navegació per l'obra ens pot dur a *WE ARE WATCHING YOU*¹⁶⁸, on, després d'un petit ensurt, ens adonem que l'agressió no és real, o bé ens podem

¹⁶⁶ Seu de la Technologies to the People Foundation, <http://www.irational.org/ttp/primera.html>

¹⁶⁷ Daniel García Andújar: TTTT, <http://aleph-arts.org/condicion.net/proyectos/proy01.html>

¹⁶⁸ Sorry, we are watching your computer, <http://www.irational.org/ttp/watch/index.html>

trobar amb missatges com *Et veiem*, on sembla palès que no és l'usuari qui actua sobre les interfícies, sinó elles sobre l'usuari. També accedirem a portals d'*entertainment* i consum perquè no oblidem la base propagandística consumista del sistema que amenaça amb l'apropiació de qualsevol moviment artístic. No oblidem que el projecte es planteja com una reflexió en meitat d'un mar mort de deixalles consumistes. Els mots i les situacions esdevenen quasi bé sempre trampes que provoquen una certa frustració. Per exemple en el metrònom, la *manipulator interfície machine*¹⁶⁹: la frustració és el fet inicial d'omplir qüestionaris amb dades avorrides¹⁷⁰ que et demana, l'efecte plaent és el del disseny gràfic final que has fet segons les dades introduïdes en el manipulador. Esdevé una crítica a tot un sistema de comunicació, l'excés del qual és caòtic. La màquina és un desencís, volem jugar amb alguna cosa, i no, el joc és omplir qüestionaris de qualsevol manera, això és jugar. El joc esdevé un joc identitari que aborda tota aquesta problemàtica a través d'inventar-se un mateix a través de dades estúpides. Mai sabem què ens espera a la pantalla següent. Amb tot, hi ha sorpreses divertides, sempre crítiques. Quan entrem a la pàgina *Language (translation)*¹⁷¹ apareix una finestra que ens pregunta: *no parlem el mateix llenguatge?* Quan cliquem damunt de qualsevol de les banderetes d'idiomes diferents, un altre avis ens diu: *LANGUAGE BARRIER...Only English translation free*, els altres idiomes han de pagar per avançat!. A la fi, si cliquem sobre un llaç blau ens envia a una pàgina anglesa de viatges organitzats a l'estranger. A la pàgina *LANGUAGE (property)*¹⁷², se'ns avisa que anem en compte ja que moltes frases que emprem normalment són *Trade Marcs* que pertanyen a qui les ha enregistrat al seu nom. Des la pàgina *VIDEO COLLECTION*¹⁷³ es poden enviar i veure treballs de vídeo, i a *PHOTO COLLECTION*¹⁷⁴, de fotografies. La pàgina *Blue Ribbon Campanign*¹⁷⁵ versa sobre la llibertat d'expressió a la xarxa, i ens remet a altres crítiques com la que cita els efectes de l'antiterrorisme, *Chilling Effects of Anti-Terrorism*¹⁷⁶ on surten totes les pàgines eliminades pel govern o amb continguts prohibits.

Dedicada al moviment zapatista mexicà, i actualitzada després de les protestes contra la reunió del G8 a Gènova (20 de juliol del 2001), que desembocaren en l'assassinat d'un jove manifestant (l'activista antiglobalització Carlo Giuliani) a mans de la policia. trobem l'obra *Los días y las noches de los muertos*¹⁷⁷ (1998) de Francesca da Rimini i Michael Grimm. La seva bandera és la denúncia de suposades violacions dels drets

¹⁶⁹ Do you want to manipulate my exhibition in metronom?, <http://www.irational.org/ttpp/metronom/index.html>

¹⁷⁰ Com a *Preliminary Basic Application*: <http://www.irational.org/ttpp/Application.html>

¹⁷¹ To The People Translation Service, <http://www.irational.org/ttpp/banderas/transla.html#>

¹⁷² "Remember, language is not freeTM", <http://www.irational.org/ttpp/TM/trademark.html>

¹⁷³ Video collection, <http://www.irational.org/video/>

¹⁷⁴ TTTP, Photo Collection, <http://www.irational.org/ttpp/collection/Collection.html>

¹⁷⁵ Seu de Blue Ribbon Site, Help Us Protect Free Speech Online!, <http://www.eff.org/br/index.html>

¹⁷⁶ Chilling Effects of Anti-Terrorism, http://www.eff.org/Censorship/Terrorism_militias/antiterrorism_chill.html

¹⁷⁷ *Los días y las noches de los muertos*, <http://dollyoko.thing.net/LOSDIAS/INDEX.HTML>

humans i civils, en el marc de les anomenades nacions civilitzades, i concretament del G8. Les consignes antisistema, provocadores, reivindicatives i apolítiques de l'obra, en fan un fetitxe dins del ciberart per als grups llibertaris i antiG8. Es centra en el principi de l'explotació capitalista i la repressió policial amb els seus exemples corresponents; denuncia l'arbitrarietat de la guerra de l'Iraq i contraposa als governs servils al capitals i explotadors dels pobles, als manifestants que defensen un model alternatiu de món. La repressió policial gira al voltant de l'assassinat de Carlo Giuliani i el presenta com l'intent de silenciar un moviment que denuncia les corrupcions del model actual.

La primera gran acció del grup 0100101110101101.org a Internet va ser el projecte anomenat *Vaticano.org*.¹⁷⁸ que, en la línia activista que els defineix, va consistir a reservar i utilitzar, el desembre de 1998 –comprant-la–, la seu web del Vaticà, simulant l'espai de l'estat del Vaticà, amb una estètica idèntica. Durant unes 24 hores varen copiar els textos de la seu web oficial del Vaticà, els varen modificar lleugerament introduint-hi alguns missatges i els varen tornar a penjar al web¹⁷⁹. Es convertia, d'aquesta manera en la major “protesta civil a la xarxa”.¹⁸⁰ Així, a través de la suposada web oficial, enviaven missatges als lectors que no feien més que provocar confusió entre els religiosos que consultaven la falsa web. Un cop descobert el “mal ús”, l'organisme oficial responsable dels dominis va anul·lar el dret a tornar a reservar-lo el domini, un cop que l'església catòlica va protestar i va reclamar per a ella la url¹⁸¹. Amb aquestes accions, el grup tornava a la polèmica sobre l'ús i les llicències a Internet.

L'obra de Rachel Baker que té per títol *Art of Work*¹⁸² (1999) es basa en un joc de paraules. El fet que no sigui traduïble al català no té importància: cadascú comprendrà el sentit d'aquest joc que és un joc sobre el “sentit” dels mots, on la desviació del sentit dona lloc a una desviació dels mots en l'expressió *Work of Art* (“obra d'art”), que esdevé *Art of Work*. Allò que il·lustra literalment és el que vol dir: una crida a una inversió, a una convulsió del món del treball, a la seva invasió i inversió per l'art. Trobem, en aquesta obra de Baker, els mateixos aspectes que hom pot reconèixer com a típics dels *artistes del net art*: alhora lúdica, irònica, crítica i utòpica, aquesta

¹⁷⁸ *Vaticano.org*, <http://0100101110101101.org/home/vaticano.org/index.html>

¹⁷⁹ *Vaticano.org*, <http://0100101110101101.org/home/vaticano.org/spoof/index.html>

¹⁸⁰ José Luis Brea: *Entre museización y radicalización. La guerra de los dominios*. http://www.rtve.es/tve/program/metropolis/net_art/presentacion2.html

¹⁸¹ ROMA - La imaginación de los piratas en Internet no tiene confines. Así lo demostró durante meses la página web <http://www.vaticano.org> que obviamente pretendía ser una copia descarada de la página oficial de la Santa Sede (<http://www.vatican.va>). La confusión se hacía particularmente astuta por el hecho de que el formato era también una copia del sitio vaticano. Entre mensajes, encíclicas y actividades del Papa, sin embargo, introducían textos paganos o irreverentes de manera camuflada.

¹⁸² *Art of Work*, http://www.irational.org/tm/art_of_work/

obra és més que un simple jocs de paraules, ja que s'hi pot retrobar un ressò d'aquell lema de "la imaginació al poder" del maig del 68. Visualment AOW adopta la forma d'un formulari en diferents seccions per a la constitució d'una base de dades. El seu *look* seriós i professional, amb un color verd-blau clínic de laboratori, fa dubtar: deu ser seriós? Fins i tot si ens hi fixem hi ha un toc irònic present a dalt i a l'esquerra de totes les pàgines: una il·lustració a l'estil del disseny comercial dels anys cinquanta que representa una noia que repeteix "*business needs art*". A mesura que avancem en el qüestionari, les intencions pertorbadores de l'obra s'obren camí: fixem-nos en el test d'ortografia, en què la tria de les paraules (*agitació, burocràcia, sabotatge, surrealitat, proletariat, irracional...*) no és pas innocent. D'aquesta manera, AOW constitueix una altra obra de *net art* que insisteix en la vocació de comunicació i de col·laboració del web, en què el text és la dada primària, atès que les imatges només estimulen el consum passiu. Davant aquesta obra ens podem preguntar: és que el web pot tenir realment el potencial que alguns pensadors (Natalie Bookchin, Alexei Shulgin, Pierre Lévy) li atribueixen de "refer el món"? Pel cap baix, podem afirmar que amb el *net art* com a arma, i amb obres com AOW, Internet té el poder, seriosament o lúdicament, de qüestionar-lo.

Durant aquests darrers anys la càmera web s'ha consolidat com un dels emblemes de la Xarxa; en la mesura en què és una arma perillosa com a eina de vigilància pública i col·lectiva, no ha de semblar estrany que les seves potencialitats contradictòries atreguin l'atenció dels *net artistes*. Tenim, per exemple, els *Surveillance Camera Players*¹⁸³ (2001), que amb les seves accions volen reforçar el dret a la intimitat i afavorir el debat sobre el seu ús generalitzat en una societat democràtica: el 7 de setembre els SCP van celebrar el primer dia internacional contra la videovigilància¹⁸⁴. *The Surveillance Camera Players* és un espai cedit a un grup d'activistes polítics que desconfien de qualsevol tipus de Govern; consideren que l'ús de càmeres de vigilància per part de la policia és una flagrant violació de la quarta esmena de la Constitució americana i es manifesten en contra del seu ús. Els seus components fan actuacions davant les càmeres de vigilància enfilant-s'hi i posant cartells davant els seus objectius, atès que les càmeres no graven el so. A la seva web s'hi poden consultar tot tipus de documents legals i articles sobre l'ús i l'abús de les càmeres de vigilància, cosa que s'ha agreujat especialment després de l'11 de setembre. El 2 de desembre del 2001, el grup 01.Org va piratejar, de manera temporal, la seva web de l'Ars Festival de Korea. La finalitat del hackeig era la de manifestar i mostrar

¹⁸³ Seu de Not bored!, <http://www.notbored.org/>

¹⁸⁴ International Day of Protest Against Video Surveillance, <http://www.notbored.org/7sept01.html>

els camuflaments que la xarxa amaga. Aprofitant l'accés que tenien a la seu web del certamen, atès que hi estaven inscrits com a participants, es van introduir al sistema i intercanviaren –permutaren– noms dels artistes en els directoris, i van anomenar aquesta acció *FR-permutations*¹⁸⁵. L'objectiu consistia a subratllar que l'art ha de ser lliure i d'accés universal i no és vàlid que un grup d'interessos econòmics particulars reunixin per a uns pocs el plaer de la visió.

La presència de tecnologia wireless, és a dir, sense cables de connexió, en medis artístics ja s'havia intensificat en el 2002 amb nombrosos projectes, més o menys directament inspirats en els sistemes de vigilància personal utilitzats habitualment als Estats Units amb nens, vells, vigilats policials... Típic exemple d'aquest corrent va ser *Vopos*, darrera part d'un projecte sobre l'artista i la seva relació amb la xarxa, de la parella d'italians que s'anomenen 0100101110101101.ORG, que havia de permetre a l'usuari seguir les passes dels artistes a través de la seva pàgina web.

*Vopos*¹⁸⁶ (2002) és la segona fase de *Glasnost*, un projecte més ampli iniciat el 2000, i que consisteix en el seguiment i publicació, en temps real, de la major quantitat de dades sobre un individu en la vida real. A la primera fase, *Life-sharing*, 0100101110101101.ORG va començar donant accés al seu ordinador, 24 hores al dia i 7 dies a la setmana, a tots els usuaris d'Internet: tots els seus programes, sistemes, arxius, eines, projectes en curs i fins i tot el correu privat es van fer públics. *Glasnost* suposava un repte radical al concepte de propietat intel·lectual i explorava les contradiccions de la privacitat a l'era de les tecnologies de la informació. 0100101110101101.ORG intenta explicar com grans quantitats d'informació privada cauen a mans de les grans empreses, que poden desenvolupar-la i convertir-la en perfils electrònics de grups i individus, potencialment molt més detallats i intrusius que els arxius creats en el passat per les agències policials. 0100101110101101.ORG mostra com els ciutadans normals estan perdent el control de la informació sobre ells mateixos, i que aquesta informació està disponible per a qualsevol que pugui pagar-la. El telèfon, els satèl·lits i Internet: *Vopos* explota i fusiona aquests tres tipus de xarxes. Els dos membres de 0100101110101101.ORG constitueixen la cèl·lula que s'està controlant. Porten un transmissor GPS (El GPS -Global Position System- està format per un seguit de satèl·lits propietat del govern dels Estats Units; els receptors GPS que es troben a la superfície de la Terra reben la informació procedent d'entre 3 i 12

¹⁸⁵ Bosco i Caldena: El colectivo 01.ORG 'piratea' el sitio del Web Art Festival de Corea. Article del diari "El País". 20/12/01.

- *FP Permutations*, <http://www.0100101110101101.org/home/ftpermutations/indexx.html>

¹⁸⁶ *Vopos*, <http://www.0100101110101101.org/home/vopos/index.html>

satèl·lits, cosa que permet determinar la seva posició exacta, així com la rapidesa i direcció dels seus moviments) que envia les seves coordenades a una seu web a través d'un telèfon mòbil. Un programa informàtic calcula la posició exacta en la que es troba en un mapa digital, creant un itinerari que segueix tots els seus moviments. *Vopos* és un projecte específic de la xarxa però, al mateix temps, també de l'espai urbà, que constitueix un espai ontològic. *Vopos*, que es presentà a Sónar 2002 de Barcelona, es mostra de tres maneres diferents, cadascuna de les quals complementa les altres: la presència en xarxa a Sónar On Line i una instal·lació i presentació pública en el Centre d'Art Santa Mònica. Durant els tres dies del festival Sónar, un software especialment desenvolupat per a l'ocasió va fer el seguiment i va mostrar les coordenades geogràfiques dels dos membres de 0100101110101101.ORG. Les projeccions de les coordenades en un mapa va permetre que tots els assistents al festival poguessin seguir els seus itineraris en un temps real amb una precisió a nivell de carrer.

6.5. Resistència a una guerra futura

La Guerra del Golf de 1990-1991 és considerada com la primera guerra d'informació per la gran dependència de l'exèrcit respecte la informació i les telecomunicacions, i on es va posar a prova el sofisticat armament dissenyat i fabricat durant la presidència de Reagan i Bush (pare). El funcionament de les armes depenia d'una important infraestructura de telecomunicacions amb satèl·lits, radars, ràdios i telèfons. Les bombes intel·ligents foren només l'aspecte més abastament difós per la CNN del sofisticat sistema armamentístic.

Però va existir un altre ús de les tecnologies de la comunicació i la informació: la censura d'imatges, la manipulació d'episodis, la reposició d'imatges gravades anteriorment i emeses com si fossin del moment i, sobretot, l'intent de crear un consens favorable a l'atac i l'ocultació dels moviments de protesta cara a desmobilitzar als qui hi estaven en contra. Als EE.UU. i a la resta del món, existia una considerable corrent d'opinió que s'oposava a la Guerra; a San Francisco es parla dels tres primers dies de la guerra com dels Tres Dies d'Ira: els manifestants abarrotaren, ocuparen i controlaren els carrers, ponts i autopistes de la perifèria de la badia de San Francisco. Les tecnologies de la informació i la comunicació, fonamentals per a les noves armes i per al control de la informació des del poder, també varen exercir un paper important en la resistència a la guerra: el correu electrònic, els taulers d'anuncis i els grups de

notícies varen contribuir a la comunicació entre els grups i col·lectius que s'hi oposaven. Tanmateix, el paper d'Internet va ser limitat a l'hora de propagar notícies i mobilitzar a la gent. Els qui s'oposaven a la guerra veien, també, la CNN. Era la fase pre-web i la Guerra del Golf s'emmarca dins l'etapa prèvia del boom d'Internet als EE.UU. Alguns es pregunten què s'hagués esdevingut si la Guerra del Golf hagués tingut lloc ara?, o bé quina forma adoptaria el hacktivisme en un entorn de resistència més generalitzada? Respondre aquesta qüestió passa per analitzar quina ha estat la mobilització hacker davant la guerra d'Afganistà o davant la guerra contra l'Iraq, ara de la mà de Bush (fill).

Com lluitar, des d'Internet, contra les més que segures guerres futures? Fins ara els episodis de hacktivitat han estat esporàdics i inconnexos, aïllats i no relacionats. Deixarà el hacktivisme d'estar integrat per incidents aïllats i esdevindrà una convergència de forces aliades? Quines podrien ser les conseqüències si els individus poguessin involucrar-se en moviments de resistència ciberespacial més enllà de les fronteres geopolítiques tradicionals? "El món electrònic no està, ni molt menys, totalment establert; cal aprofitar la seva fluïdesa i ser inventius ara, abans que només ens quedi com a arma la crítica."¹⁸⁷

Un dels artistes que es revolta contra el poder institucional i critica l'hegemonia del negoci al món de l'art és Andy Cox. El treball d'aquest artista americà s'inscriu en una voluntat activista que engloba diversos aspectes formals de l'art web. *Anti-capitalist Operating System*¹⁸⁸ (2000) és un extens projecte politicoartístic que denuncia les pràctiques i els excessos procapitalistes de la nostra societat. La Xarxa era, per a ell, lògicament un mitjà ideal per a fer-ho, per dues raons: d'entrada perquè el seu missatge i la seva lluita (*Together We Can Defeat Capitalism* és el nom del col·lectiu d'artistes que ha fundat) necessiten una agrupació i una col·laboració important, i la xarxa li permet arribar a un gran públic. En segon lloc, perquè Internet és la gallina dels ous d'or dels inversors, de les empreses i dels seus accionistes, i esdevé, per tant, un símbol del capitalisme.

Cox ataca un altre símbol del poder financer apropiant-se de la interfície de Windows. Tocarà el torn després de "*Who wants to be a millionaire*", la versió original americana de la cèlebre emissió "Qui vol guanyar milions", corresponent a la publicitat del Citibank. Les figures emblemàtiques de la seva lluita són Che Guevara, Arnold

¹⁸⁷ Critical Art Ensemble, <http://www.critical-art.net/>

¹⁸⁸ Anti-capitalist operating system (acos) v2.0, <http://www.twcdc.com/>

Schwarzenegger en el paper de Terminator, i també Batman i Robin, nous "revolucionaris socialistes".

Andy Cox fa servir nombrosos mitjans, vídeo, imatge fixa o animada, text i so per a transmetre el seu missatge, però el seu treball no es limita a Internet. El col·lectiu TWDC i ell porten a terme nombroses accions polítiques subversives que s'assimilen a accions artístiques, en què fan servir taulers lluminosos per a penjar-hi missatges i capgiren els continguts informatius de les pantalles públiques de comunicació. Les imatges d'aquestes accions són enregistrades i visibles a la seu web. Com a exemple, podem esmentar el missatge "*The spectre of anticapitalism is haunting America*" penjat davant la seu de Nike, o bé "*No over-taking of art by big business*" davant el MOMA de San Francisco.

A mitjan 1997, un grup d'artistes liderats pel britànic establert a Califòrnia Andy Cox van començar una companyia anomenada "sticking up for art". Es tractava d'omplir les rodalies del MOMA de San Francisco d'enganxines amb el lema "*Together we can defeat Capitalism*". La mateixa acció fou reproduïda en el marc del Documenta X de Kassel. Un article al San Francisco Weekly, juntament amb la retirada de les enganxines, substituïdes per diversos rètols amb el lema "No enganxeu cartells", foren tota resposta. Prèviament, el mateix any 1997, amb motiu de la campanya publicitària de la pel·lícula Batman, Andy Cox havia fet circular ja una versió alternativa dels herois del còmic amb un disseny en el qual aquests apareixien com a revolucionaris socialistes. Per la mateixa època, jugant amb l'anunci de Citibank "*In your dreams*", el Citibank Project de Cox va consistir a empaperar els carrers de San Francisco amb rèpliques revolucionàries del missatge publicitari del banc. No existeix, certament, un discurs sòlidament construït al voltant del per què d'aquesta proposta anti-capitalista. El mateix Cox empra arguments aparentment extrets d'aportacions dels mateixos internautes per combatre (però també per justificar!) la continuïtat del nostre model econòmic capitalista. Abans que res, la lluita de TWDC (*Together We Can Defeat Capitalism*) és una pulsio anarquista contra un sistema immoral i pervers. Altres accions del grup a partir de 1998 foren la compra d'espai publicitari en les andanes del metro de San Francisco per emetre missatges anti-capitalistes¹⁸⁹ del tipus "*Capitalism stops at nothing*". La creació d'una falsa web de Citibank que fou retirada a instàncies de la gran corporació¹⁹⁰, l'acció *bed-in for peace*¹⁹¹, on dos artistes de Nova Zelanda

¹⁸⁹ Vegeu un comentari de premsa d'aquestes accions a <http://www.rtmk.com/more/twcdc.html>

¹⁹⁰ Vegeu el comentari del *New York Times* del 17 d'abril de 2001 a http://www.twcdc.com/documents/new_york_times_04_07_01.htm

¹⁹¹ *Bed-in for peace*, <http://www.bed-in-for-peace.net/>

es quedaren 48 hores al llit, connectats a altres artistes de tot el món, per tal de protestar a favor de la pau en el món. L'ús de falsos missatges d'alerta en els carrers i carreteres locals amb frases subversives. La pintada de carrils bus afegint una H a la "Bus Stop". L'acció de protesta de Cox davant del Banc d'Anglaterra oferint-se a treballar "per vèncer el capitalisme"¹⁹². Cox ens explica el per què de la necessitat de crear l'ACOS (*Anti-Capitalist Operating System*¹⁹³): "Desenvolupant els nostres propis sistemes d'explotació, podem desenvolupar els nostres propis objectius al marge de l'impàs actual del sistema capitalista"¹⁹⁴. Per a d'altres, Cox és bàsicament un enginyer de formació que vol "emprenyar" les grans corporacions¹⁹⁵. En les seves mateixes paraules¹⁹⁶: "El meu treball és un intent desesperat de sobreviure en un món que gira al voltant del món financer, on el poder mediàtic es concentra a les mans d'un pocs i on la fam i la SIDA es passegen per l'Àfrica mentre nosaltres ens preocupem pel preu de les nostres accions. Aquest és un treball que neix de la irritació i la confusió barrejat amb l'humor. Per tirar endavant aquest projecte he fundat el col·lectiu d'artistes TWCDC".

"Pràcticament totes les imatges que veiem pel carrer contenen la mateixa ideologia consumista: la salvació mitjançant el consum, Internet i el mercat borsari (Déu Pare, Fill i Esperit Sant). Quan veiem alternatives que qüestionin aquesta ideologia? (...) La meva feina al TWCDC té per objectiu injectar un mica de (in)sanitat en aquest espectacle esborronador".

A la revista *Artbyte* del juliol de 2001 Cox admet que se sent més proper a l'artivisme que no pas a l'art tradicional¹⁹⁷: "Actuar com a hacker implica no caure en els paradigmes empresarials i comercials. Es tracta de recuperar el poder (...) D'alguna manera em sento vinculat a les forces que estan fent la història. Quan era un nen sempre em preguntava què feia que les coses canviessin. Encara ara estic tractant de respondre aquesta pregunta".

A la negativa del SFMOMA a considerar l'obra de Cox i del TWCDC com a dignes de poder entrar en la institució, el seu responsable justifica el seu criteri en la necessitat del museu d'establir estàndards de qualitat estètica, en la impossibilitat d'abstracte's del comú interès de la institució i els seus benefactors (empreses i individus

¹⁹² Per al conjunt de la obra satírico-artística de Cox, abans i després de la constitució de TWCDC, vegeu: http://www.twcdc.com/web_resume.htm

¹⁹³ Anti-capitalist operating system (acos) v2.0, <http://www.twcdc.com/>

¹⁹⁴ Fred Rapinel: *Projects de media activism*, <http://www.arpla.univ-paris8.fr/~canal10/rapinel/>

¹⁹⁵ Announcements 16 setembre 2001, <http://amsterdam.nettime.org/Lists-Archives/nettime-l-0109/msg00143.html>

¹⁹⁶ Cox a http://www.0100101110101101.org/home/glasnost/stasi/andy_cox/program.htm

¹⁹⁷ *Web of Lies*, http://www.twcdc.com/documents/artbyte_07_01.htm

acabats), però, finalment, accepta l'interès de la seva reflexió al voltant de la funció de l'art en la contemporaneïtat. En molts punts la resposta del SFMOMA a Cox ens recorda al debat al voltant de l'obra de Hans Haacke, *MOMA-Poll*, de 1970 i, sens dubte, en la difícil relació entre institucions museístiques, obra artística i poder econòmic.

El fet cabdal del 2001 es va produir l'11 de setembre, quan les torres bessones del World Trade Center de Nova York varen ser destruïdes per un atac terrorista suïcida. La reacció de la comunitat hacker va ser molt ràpida. La primera acció difosa pels mitjans massius va tenir lloc el dia 12 de setembre: un hacker rus anomenat Ryden va atacar la seu *taleban.com*, que correspon a la denominada "Missió Afgana de Taliban". La pàgina principal fou alterada i s'hi va penjar una fotografia d'Osama Bin Laden, amb un text acusant-lo per l'atemptat. Pocs dies després es va anunciar la creació del grup The Dispatchers, creat per 100 hackers de diferents països decidits a pertorbar, a través d'Internet, les nacions i organitzacions que donen suport al terrorisme islàmic. Un dels principals integrants del grup era un hacker canadenc que va decidir organitzar el grup en constatar que entre les víctimes dels atemptats hi figuraven amics i familiars seus. El grup es va atribuir l'haver posat fora de servei algunes seus palestines i iranianes. Una altra iniciativa fou duta a terme per Kim Schmitz, un hacker alemany transformat en consultor de seguretat, que va obrir una seu a Internet per a reclutar hackers amb l'objectiu de rastrejar fluxos de fons i altres evidències que vincuessin Bin Laden amb els atemptats de l'11 de setembre. El grup de Schmitz, anomenat YIHAT (Young Intelligent Hackers Against Terror) estava format per 34 persones de 10 països, amb tres traductors de l'àrab, i sembla ser que varen entrar en un banc sudanès, obtenint informació sobre comptes vinculats amb Bin Laden, però el National Infrastructure Protection Center, del FBI, va condemnar aquestes accions, com a il·legals i punibles amb cinc anys de presó. Tanmateix, no tots els hackers es varen adherir a aquest tipus de postures. El Chaos Computer Club va manifestar la seva oposició categòrica a atacar seus islàmiques a través d'Internet: "Precisament ara, els mitjans de comunicació electrònics com Internet poden contribuir de forma important a la comprensió entre els pobles. Amb la tensió actual, no podem bloquejar els mitjans de comunicació i obrir així un terreny encara més ampli a la incomprensió".

Davant l'aparent unanimitat de les anàlisis i dels comentaris, els *net.artistes* també varen reaccionar. Rhizome recorda l'artista jamaicà Michael Richards¹⁹⁸ que estava treballant aquell dia al pis 92 d'una de les torres i ha activat una pàgina, *911-The*

¹⁹⁸ Remembering Michael Richards, <http://www.studiomuseuminharlem.org/richards.html>

tema de la guerra, *The>Wartime<Project* és un intent de trencar la cortina de silenci que a partir de la primera Guerra del Golf, fa deu anys, envolta tots els conflictes", afirma Forbes. L'obra és un exemple ben clar d'activisme artístic, ja que es basa en una visió de l'art com a intercanvi comunicatiu, on es defensa el dret a participar i a ser testimoni de la més gran diversitat possible de formes d'expressió. En aquesta obra l'expressió personal de cada participant és un requisit previ per a l'autoafirmació del conjunt de l'obra, i és el conjunt d'aquestes expressions que són un element indispensable més per a la cultura. Tots els participants en aquest projecte mostren clarament la seva oposició a la guerra. Tal i com ho demostren les paraules del col·lectiu que aglutina els diferents artistes que han intervingut en el projecte: "esperem que la riquesa i diversitat en l'apropament, materials, sentiments i localització de les parts components del nostre projecte pugui demostrar i reflectir l'abast i escala d'aquesta oposició a la guerra. No serem arrossegats a la guerra de forma col·lectiva sense reacció, sense qüestionaments, i mantenim el desig i la capacitat de desafiar les fronteres i barreres que els faedors de guerres aixequen entre les persones".

És una iniciativa conjunta del grup d'artistes digitals offline²⁰⁷ i l'associació d'esdeveniments artístics digitals de South London open²⁰⁸ digital, encapçalats per Andrew Forbes, pare del projecte. L'obra es proposa reunir les reflexions creatives dels net artistes sobre el tema de la guerra, precisament quan la política dels Estats Units es fa cada dia més agressiva. Malgrat que molts participants del projecte han centrat les seves obres al voltant dels atacs dels Estats Units contra l'Iraq, el projecte segons paraules del mateix Forbes "no va estar realitzat específicament per anar contra la guerra a l'Iraq", l'objectiu del programa és "aconseguir que la gent jove que no ha experimentat cap guerra reflexioni sobre els seus poders destructius".

Partint de la idea que la funció de l'art no consisteix a reflectir l'estat del món, sinó a treure el món del seu estat, *The>Wartime<Project* es desenvolupa a partir d'una interfície concebuda com una representació del món en el qual estan entrellaçats tots els projectes dels artistes participants en correspondència amb la seva ciutat d'origen. Per a accedir a les obres, l'internauta ha de desencadenar petits bombardeigs virtuals: l'obra triada esdevé el blanc, el mapa del món es va ampliant com en la simulació d'un atac aeri i, quan la bomba arriba al seu objectiu, el projecte es desplega sota la mirada de l'usuari.

²⁰⁷ Offline route map, <http://offline.area3.net/>

²⁰⁸ Open_digi_Party, <http://club.net-art.ws/>

El projecte està allotjat al servidor del col·lectiu barceloní Area3²⁰⁹ i es desenvolupa a partir d'una representació del món dissenyada pel mateix Forbes, on l'internauta pot escollir entre la bidimensionalitat o la tridimensionalitat. La qualitat i complexitat de les obres que s'hi poden trobar navegant és diversa, hi ha des d'escenes interactives simples, animacions petites o vídeos curts. En aquest mapamundi els projectes dels diferents artistes participants es troben en correspondència amb la seva ciutat d'origen. Per accedir a les obres cal bombardejar-les virtualment: la ciutat d'origen de l'artista és el blanc, el mapa del món es va ampliant com en una simulació d'atac aeri i, quan la bomba arriba al seu destí l'obra esclata davant la mirada de l'espectador.

La diversitat de treballs que s'hi poden trobar van des d'una imatge, una frase o una petita animació en *flash*, fins a treball força complexos, com *Stop the War*, de l'anglesa Ruth Catlow²¹⁰, una anàlisi introspectiva dels moviments contra la guerra a partir de les darreres manifestacions que han tingut lloc al Regne Unit. L'obra d'Entropy8Zuper sembla un joc: quan l'internauta, convertit en un executiu de Wall Street, mira de disparar contra unes figures vestides amb la característica *kefia* palestina, immediatament apareix l'expressió "*game over*". Erik Salvaggio, amb l'obra *Flight*, respon a la pregunta "què poden fer els homes amb ales?" amb crues imatges fetes amb caràcters ASCII, i el londinenc Stanza hi contribueix amb un mapa de Nova York que es va destruint, acompanyat de la llista dels països bombardejats pels Estats Units des de la Segona Guerra Mundial. L'artista cubà Antonio Mendoza, que viu a Los Angeles, hi participa amb dues obres que barregen l'estètica psicodèlica dels anys setanta, la cultura dels còmics i les noies del *manga* per a adults. *Axis of evil tour 2003*²¹¹ i *South Beach Disco* agredeixen l'usuari amb un bombardeig visual i sonor en el qual se succeeixen de forma caòtica les imatges del conflicte a l'Afganistà²¹². L'artista holandès, Eluot de Kok, també fa una obra singular. A la pantalla es pinta dinàmicament el seu retrat, a base d'una xarxa de quadradets blancs, negres i grisos, seguint el moviment del cursor de l'espectador. Tot i que sembla clar que no és una opció gaire encertada per un projecte sobre la guerra, es veu que el software que genera el retrat havia estat programat perquè cada quadrat que configura la silueta lluiti per concretar el color, ja sigui blanc, negre o gris.

²⁰⁹ Area 3, <http://offline.area3.net/>

²¹⁰ Ruth Catlow, http://www.furtherfield.org/displayartist.php?artist_id=12

²¹¹ *Axis of evil tour 2003*, <http://www.csmonitor.com/2003/0221/p13s01-alm.html>

²¹² *South Beach Disco*, <http://offline.area3.net/wartime/press.php?show=2>

Filla de la cultura del realisme socialista i d'una guerra especialment cruel, la poètica de l'artista iugoslau Andrey Tisma²¹³ combina la referència a l'alta cultura amb la crítica més ferotge i descarnada. A *American Art School*²¹⁴ (2003), fa servir les imatges dels soldats dels Estats Units destruint les estàtues i pintures de Saddam, per a una insòlita lliçó sobre la història de l'art americà del segle XX. Aquest autor ja s'havia posicionat clarament davant dels atemptats de l'11 de setembre, com ho reflecteix en l'obra *Remember Crime*²¹⁵.

“A través d'Internet és possible desemascarar l'engany que envolta aquesta i totes les guerres” afirma l'artista novaiorquès Andy Deck que, amb l'objectiu d'ampliar la visibilitat i la repercussió de l'activisme pacifista creatiu, proposa *Anti-War Web Ring*²¹⁶ (2003), una estructura que enllaça pàgines web contra la guerra, amb un directori amb la descripció de cada web i d'un cercador que facilita la navegació de l'usuari.

7. La guerra de dominis: etoy contra eToys

Segons els mites que s'han generat, el ciberespai seria un territori virtual, lliure i infinit. D'aquesta manera, els informàtics americans recuperaven la metàfora del Far West per a il·lustrar l'esperança d'un espai obert a tothom, una nova frontera on hi haurien de regnar el “*free speech*” (la llibertat de paraula), noves regles democràtiques i econòmiques, i on cadascú tindria el dret d'expressar-se i de comerciar lliurement²¹⁷. Però com ho ha mostrat Michel Foucault²¹⁸ el discurs pot ser un principi d'exclusió i d'asserviment social. A Internet, l'autoritat s'exerceix igualment pel control d'una estructura textual, basada en els noms de domini i les seves adreces URL (*Uniform Resource Locator*, Localitzador Uniforme de Recursos)²¹⁹. A la xarxa, el territori és el nom de domini²²⁰ (l'adreça), i sota el pretext de civilitzar-se i pacificar-se, l'Oest salvatge virtual es va comercialitzar i les “zones autònomes temporals”²²¹ van anar desapareixent per a garantir la seguretat del comerç. Les formes anàrquiques com el

²¹³ Andrey Tisma, <http://members.tripod.com/~aaart/>

²¹⁴ Culture the American Way, <http://www.webheaven.co.yu/usa/artschool.htm>

²¹⁵ <http://www.webheaven.co.yu/usa/remember.htm>

²¹⁶ Andrey Tisma: *Remember the Crime*, <http://artcontext.org/antiWar>

²¹⁷ Gundolf Freyermuth (1996), *Cyberland*. Berlin. Rowohlt. Veure

<http://www.ucs.mun.ca/~lemelin/AGONIQUE.html#foucault>

²¹⁸ Michel Foucault (1971), *L'Ordre du discours*, Paris. Gallimard.

²¹⁹ Cfr. Luther Blissett/Sonja Brünzels (1998), *Handbook of Communication Guerilla* <http://www.contrast.org/KG/>

²²⁰ DNS: domain name system. Servei essencial d'Internet que assegura la conversió dels noms de domini (ex: www.uoc.edu) en adreces IP (ex: 123.45.67.89). Una adreça IP és un grup de quatre números, que corresponen a quatre octets, separats per punts. Fins al començament de l'any 2000, els noms de dominis eren administrats per una societat privada americana, Net Solution.

²²¹ T.A.Z., http://www.hermetic.com/bey/taz_cont.html i també <http://aredje.net/taz.htm>

cybersquatting²²², el hacking, l'infowar²²³ han estat perseguides i amenaçades de prohibició. La història d'etoy²²⁴ contra eToys²²⁵ és un exemple de la batalla entre l'Internet mercantil i l'Internet artístic no comercial que va tenir lloc en el moment de l'eufòria de les empreses .com. Gràcies a la mobilització mundial d'internautes, d'artistes, de col·lectius com Rtmark i de la pràctica del hactivisme, els artistes d'etoy obtingueren la victòria davant de la casa de joguines en línia americana eToys.

El grup etoy va ser fundat a Munic el 1994, per uns quants artistes europeus alternatius, que provenien d'Itàlia, Anglaterra i Suïssa, i el 1996 va guanyar el premi més prestigiós del net.art, el Golden Nica de l'Ars Electronica Festival de Linz a Àustria, pel seu projecte *Digital Hijack*²²⁶, mitjançant el qual va aconseguir redirigir a la seva pàgina web a uns 600.000 internautes en tres mesos, fent servir un seguit de paraules reconegudes pels més grans motors de cerca, com Altavista o Infoseek. "Volíem demostrar que un grupat de companyies controlen el destí de milions d'internautes i que la majoria de la gent no en té ni idea de com funcionen els motors de cerca" va dir Zai portaveu d'etoy. La seva activitat es centrava en la venda de falses accions sobre el temps, per a finançar una càpsula temporal estrambòtica; en definitiva, una burla als valors conjugats del capitalisme i de la hipercomunicació. A l'octubre de 1995, el grup va registrar el seu domini a Internet com etoy.com (el fet de posar-se ".com" és una mena de pam-i-pipa als ".org" dels alternatius i un intent de sortir del marc habitual del gueto artístic) dos anys abans que, pel novembre de 1997, l'empresa de joguines eToys (fundada el 1996) enregistrés el seu.

eToys és un poderós grup de comerç en línia. Va néixer el 1996 de la mà del directiu de la Disney Toby Lenk i del fundador d'Idealab²²⁷ Bill Gross. Va rebre el suport moral i financer de la Disney (propietària d'un 20 % de la companyia) i d'altres empreses de capital risc com Highland Capital Partners. Durant el 1999 el seu creixement semblava imparable: amb més de 500 treballadors, va obrir una versió anglesa, va sortir a la borsa el 20 de maig, va comprar Baby Center i va acabar l'any fiscal amb unes vendes que superaven els 30 milions de dòlars (el 1998 havien estat de 0,7 milions). El Nadal de 1999 prometia beneficis molt alts: 25 milions de compradors varen fer les seves compres per Internet i es varen gastar uns 7.000 milions de dòlars en les tendes en

²²² Cybersquatting, <http://www.webopedia.com/TERM/C/cybersquatting.html> i també

<http://www.tipz.net/cybersquatting.htm>

²²³ Infowar.com, <http://www.infowar.com/>

²²⁴ etoy.Corporation, <http://www.etoy.com/>

²²⁵ eToys.com, <http://www.etoys.com/etoys/index.html>

²²⁶ etoy: *Digital hijack*, <http://www.hijack.org/>

²²⁷ Idealab, <http://www.idealab.com/>

línia, segons les dades de Jupiter Communications²²⁸. eToys fou la seu més visitada segons Mediametrix i va exhaurir moltes de les seves existències, tot i la competència d'Amazon.com, que també ven joguines, i la divisió en línia de Toys'R'US. Tanmateix, els bons resultats del Nadal no varen compensar la gran quantitat de milions que es va gastar en la campanya de publicitat i marketing. El fet que el col·lectiu d'artistes etoy fos el propietari del domini etoy.com li desagradava molt, ja que creia que aquest nom molt proper al seu, etoys.com, feia que els seus clients es confonguessin. Fou per això que va iniciar un procés judicial per a obtenir el tancament de la seu etoy.com. El plet vas durar fins a finals de 1999 i després d'una espectacular mobilització digital, anomenada Toywar²²⁹, etoy va guanyar el recurs definitiu i va poder conservar el seu nom²³⁰. Esdevingué un símbol de la lluita per la llibertat d'expressió i el dret a la identitat en el ciberespai.

Birgit Richard²³¹ explica els fets i fa l'anàlisi de Toywar (la guerra de les joguines), posant en evidència el fet que l'aspecte corporatiu del treball del col·lectiu etoy s'assemblava molt a les estratègies desenvolupades per les corporacions mercantils, és a dir, la manera de fer del grup d'artistes era molt similar a la manera de fer de les empreses comercials. I aquesta similitud no era tolerada per aquest entorn dels negocis, ja que segons ells els artistes usurpaven un terreny que no era el seu propi i, per tant, s'interferien amb el terreny dels negocis. La falsa imatge corporativa del col·lectiu etoy (fins i tot amb el seu domini .com) creava una confusió inacceptable per aquells que se sentien imitats massa de prop. El grup etoy semblava ocupar, d'aquesta manera, un territori comercial que no era el seu i obria l'espai de l'art a altres zones que li estaven vedades; no acontentant-se amb el nínxol reservat a l'art, el col·lectiu eToy havia introduït noves estratègies en l'art. El problema de fons no era, doncs, tant un conflicte de dominis, com l'intent de reubicar l'expressió artística en el seu vedat habitual.

Per tal de veure aquestes noves estratègies, aquesta confrontació d'espais, és interessant de reconstruir els aspectes centrals d'aquest enfrontament. El 1999, un comunicat adreçat als internautes anunciava que el consorci de comerciants de

²²⁸ Troy Wolverton and Greg Sandoval: *Online retail sales reach \$7 billion this holiday*. 13 gener 2000 <http://news.com.com/2100-1017-235631.html?legacy=cnet>

²²⁹ Toywar, <http://toywar.etoy.com/>

²³⁰ Tensions al si del grup o la necessitat d'emprendre camins diferents, van provocar la fractura del grup. Gino Esposto va fundar Micromusic i Hans Ubermorgen es va involucrar en un seguit d'accions de tecno-avantguarda, que difuminen els límits conceptuals entre art, economia i comunicació. El que resta del nucli històric, Gramazio, Kubli i Zai, continua la seva trajectòria ampliant el radi de les seves intervencions públiques amb l'etoy.DAY-CARE, un projecte basat en un contenidor dotat de totes les tecnologies de la comunicació, on realitzen tallers amb nens de 6 a 12 anys, convertits per unes hores en agents subversius encarregats d'un projecte col·lectiu top secret.

²³¹ Birgit Richard: « etoy contre eToys », a Annick Bureaud i Nathalie Magnan (2002), *Art, réseaux, média*. París. Ensba, pàgs. 91-114.

joguines americana eToys iniciava un procés a Califòrnia el 8 de novembre de 1999 contra el grup de net artistes etoy. Des del 1998, eToys intentava comprar a etoy (que s'anomena d'aquesta manera des del 1994 i que es va enregistrar com a nom de domini internacional el 13 d'octubre de 1995) el nom de domini etoy.com. Les ofertes de compra del domini, que havien començat amb alguns centenars de dòlars, arribaven als 524.000 dòlars poc abans de la vista judicial, que va interrompre momentàniament la presència dels artistes a la xarxa. Etoys acusava etoy d'ocupar abusivament el seu nom de domini i va intentar, amb l'ajut dels seus advocats, eliminar els artistes criminalitzant-los i aclaparant-los amb despeses judicials. L'objectiu dels comerciants de joguines era el d'excloure al col·lectiu d'artistes de la categoria del domini més important “.com”, de treure'ls el seu caràcter global i internacional, i de reenviar-lo al signe nacional suís “.ch” (el món de l'art no té un domini propi). Una ordre provisional feia que el nom del competidor artístic fos inaccessible als internautes.

El fet era, doncs, que una empresa comercial reivindicava el dret d'ocupar un domini artístic; etoy era descrit davant la justícia com a il·legal i perjudicial pels infants, i els seus membres eren tractats de criminals, hackers, pornògrafs i terroristes. Quan un nen es perdia navegant amb el seu avi per la seu d'etoy, i es queixava després a la firma eToys, aquesta ho aprofitava per atacar els seus competidors; etoy era estigmatitzada com “econòmicament altre”, perill públic que calia posar sota tutela judicial. La denúncia arribava fins a la violació del nom enregistrarat. Els artistes es mostraven, en principi, optimistes, ja que tenien al seu favor alguns elements com ara la diferència de noms (l'absència de la “s”) i l'enregistrament molt anterior al del seu adversari. Però el 29 de novembre, el domini etoy.com era condemnat per un judici provisional a una pena de 10.000 dòlars de multa per dia de seguir a la xarxa segons els termes següents: “... a l'espera del judici definitiu d'aquest procés, l'associació que defensa etoy d/b/a/ (“etoy”) i tota persona actuant en nom d'etoy estan sota l'efecte del present decret en els casos següents:

1. en explotar una seu web sota el nom de domini www.etoy.com
2. en utilitzar, presentar o explotar de qualsevol manera, el nom de domini www.etoy.com en connexió amb el “digital hijack”²³²
3. en vendre, en proposar vendre, en sol·licitar ofertes de compra d'accions no enregistrades de l'“etoy.STOCK” a tota persona resident als Estats Units o a Califòrnia.

²³² Desviament digital que porta els internautes a la seu d'etoy i els reté a desgrat. Veure el projecte a <http://www.hijack.org/>

Signat, el 29 de novembre de 1999: John P. Shook, jutge, Tribunal del comtat de Los Angeles”.

Aquesta sentència no feia més que reduir la possibilitat d'un ús no reglamentat d'Internet. L'economia no suportava ser trastornada per un projecte artístic que, sortint del seu gueto, es comportava en la xarxa com un somni d'esperança. Etoy transgredia efectivament tan bé els valors del comerç que no era pensable que es tractés d'una paròdia o d'una exageració; i se'n reia massa bé de les regles d'un cert sistema de valors econòmics per a pensar que podia ser integrat a aquest sistema. Observem, si no, com presentava etoy la venda de les seves “falses” accions: “Comunicat: etoy.SHARE és un producte artístic il·legal als Estats Units des del 28 de novembre de 1999. No intenteu comprar les etoy.SHARES si viviu a Amèrica o si sou ciutadà americà. Gràcies pel vostre ajut per un futur millor, sense associacions que comprometin la llibertat a Internet”. Les shares²³³ –que etoy no venia només simbòlicament– desvetllaven els mecanismes borsaris de l'especulació i de la plusvàlua. Mostraven el comportament irracional dels mercats, que han esdevinguts virtuals abans de l'emergència dels nous mercats i de l'adveniment del NASDAQ, i ens recordaven que són els rumors, les expectatives, els mites els que determinen el guany o la pèrdua de bilions de dòlars. Fou aquesta crítica, des de l'estètica activista, al sistema econòmic capitalista, la que va conduir a etoy a la seva primera desfeta. Amb aquesta decisió judicial etoy semblava vençut; però va agafar l'adreça IP disponible <http://146.228.204.72:8080>, i es va crear la seu web www.toywar.com²³⁴ des d'on es va fer una crida als activistes simpatitzants com RTMark²³⁵, The Thing Nova York, ninfomaina, detritus.net²³⁶, [illegal art](http://illegalart.net)²³⁷, plagiarist.org²³⁸, namespace, negativeland, evolution control committee, styro2000, boombox.net, per a constituir una plataforma de resistència, dedicada a la llibertat de l'art a Internet i a la igualtat dels drets de l'art amb els del comerç. La seva finalitat era la d'impedir la venda del territori digital (la URL) a les empreses i establir un entorn pacífic a la xarxa. Tanmateix, des de les primeres accions de resistència, i encara que això no formés part de la sentència, Network Solutions (l'encarregada de gestionar els dominis d'Internet) va sotmetre la inscripció DNS d'etoy a les pressions econòmiques. “Estem en una situació crítica. Per començar, Network Solutions ha tallat els nostres accessos DNS. Hem migrat a comptes d'e-mail temporals. Ara algú ha tallat el segon compte e-mail del que

²³³ Les etoy.shares són parts de la societat etoy posades a la venda seguint els models de les accions borsàries

²³⁴ Toywar, <http://toywar.etoy.com/>

²³⁵ Seu de ®TMark, <http://www.rtmk.com/>

²³⁶ Detritus.net, dedicated to recycled cultura, <http://detritus.net/>

²³⁷ Illegal art, <http://detritus.net/illegalart/>

²³⁸ Plagiarist.org, <http://plagiarist.org/>

ens servíem per a seguir en contacte amb els periodistes. Una nova adreça email, e07@toybomb.com, ha estat activada. Guerra total... totes les nostres plataformes estan sota el control permanent d'aquests porcs hipòcrites...”.

Quedava clar que les relacions de força i poder del “món real” també s'havien estès al WWW. Conforme al nou ordre mundial, Internet només posava a disposició dels artistes espais lliures estrictament definits, com en la realitat tangible en la qual el sistema només els concedeix terrenys de joc ben circumscrits (galeries, museus...). L'exemple d'etoy mostrava que tots els camps socials no podien ja coexistir a la xarxa, com ho feien al principi d'Internet, i que no existia una igualtat de drets pel que fa a l'adquisició dels noms de domini.

La lluita d'etoy és un clar exemple d'estratègia en xarxa. L'elaboració de diferents nivells intermediaris és característica de totes les accions veritablement eficaces dels net activistes. Així, a través de toywar, els artistes podien actuar des d'una plataforma jurídicament irreprotxable, i en passar pel registre d'adreces de rhizome.org i amb la col·laboració dels activistes de RTMark, la resistència es concentrava en formes polítiques efectives i aconseguia assegurar el lligam entre el Web, la premsa, la televisió i la realitat del carrer. Noves xarxes d'insubmissió es posaren aleshores en pràctica. Per una banda trobem el “*Campaign Information Center*”, dirigit pels teòrics Barlow i Rushkoff, on es reunien totes les informacions abans de ser enviades a la premsa; per una altra, els militants organitzaven conferències de premsa al MOMA de Nova York i manifestacions davant la seu d'eToys. La plataforma The Thing, sobre la que opera l'Electronic Disturbance Theatre, assumia les funcions infraestructurals i aconseguia sotmetre eToys a la prova d'un atac Floodnet²³⁹, neutralitzant ràpidament el servidor: el programa feia el procés de compra d'una joguina, parava abans de pagar i tornava a començar. Quants més programes s'unien a la protesta, el sistema d'eToys.com anava més lent i les seves accions, a la borsa, van acabar caient. Es recorda com “la guerra de les joguines”.²⁴⁰ RTMark presentava el 12 de desembre de 1999 un conjunt d'accions com una mena de joc en xarxa amb la consigna “ajudeu a destruir eToys.com!”. “Aquest joc és més excitant que qualsevol altre joc d'ordinador, perquè heu de lluitar contra un mala pell del món real” deia el portaveu d'RTMark Lucha. “eToys acusa etoy.com d'obstaculitzar les seves vendes desviant els seus clients cap a la seva seu web. Però ja que el domini eToys pertorba també els qui cerquen art a Internet i que van a parar a eToys, per què no qüestionar l'existència

²³⁹ ®TMark: *FloodNet*, <http://www.rtmark.com/zapflood.html>

²⁴⁰ Mercè Molist: *Entrevista a Ricardo Domínguez*. <http://www.quands.info/articles/html/rdominguez.html>

mateixa d'eToys? Per què el poder financer hauria de tenir força de llei? Si volen jugar segons regles bàrbares, respondrem de la mateixa manera.” “Ja que eToys troba divertit sacrificar l'art en benefici propi, no hi ha cap raó per a no divertir-se destruint eToys en benefici de l'art” declarava Lucha a rhizome.org²⁴¹.

RTMark era la punta de llança d'un moviment contestatari la lluita del qual contra les grans companyies i les seves reivindicacions de poder s'estenien més enllà de la xarxa. Aquest col·lectiu va organitzar per a etoy un dels seus fons mutus subversius. Els projectes del “fons etoy”²⁴² tenien per objectiu reduir al no res el valor de l'acció borsària d'eToys. Per això es posaren en funcionament les aplicacions DoS Attack Floodnet que obstaculitzaven el servidor de la firma durant el període de les compres de Nadal, mentre que una important campanya d'informació duta a terme amb el suport d'Electronic Disturbance Theatre desacreditava eToys als ulls de la seva clientela, dels seus col·laboradors i dels seus inversors. La seu web d'eToys fou envaïda de protestes. El 16 de desembre el sit-in virtual fou un èxit; va provocar una gran confusió i va falsificar les dades estadístiques. Els atacs no duraven més d'un quart d'hora, sobrecarregant el servidor d'eToys, aclaparant-lo amb innumbrables operacions, que provenien de set o vuit seus “mirrors” sobre els que fluïen cinc scripts diferents. Una altra tàctica s'afegia a l'atac Floodnet: aconseguir que el càlcul de l'avaluació financera de la seu fos impossible i devaluar-ne les estadístiques. Amb aquesta finalitat, l'script no lineal “killertoy.html” emmagatzemava compres sense parar en els cistells de la compra, naturalment sense comprar. El servidor es veia així obligat, per cada diguem-ne compra, a refer la llista global de les existències i del cistell de compra. Les seus mirrors produïen quotidianament més de cent mil respostes i el temps necessari pel càlcul de la llista esdevenia cada cop més llarg. Als scripts s'hi afegien eines que els usuaris podien instal·lar-se en el seus ordinadors i enviaments d'emails, com els mailbombs, que els serveis comercials havien de tractar un a un sense programes automàtics. Fou aquesta agressió simbòlica de gran envergadura, aquesta protesta a través de la xarxa, la que va fer possible el triomf d'eToy: conservar el seu domini.²⁴³

8. Ciberguerrilla

²⁴¹ Lucha, <http://www.rhizome.org/print.rhiz?1607>

²⁴² ®TMark: *Le fonds etoy*, <http://rtmark.com/etoyfr.html>

²⁴³ *Cool business: etoy's toy wars* per Birgit Richard
<http://www.nettime.org/lists-archives/nettime-l-0012/msg00025.html>

http://www.isea2000.com/actes_doc/09_richard.rf

<http://www.uni-frankfurt.de/fb09/kunstpaed/indexweb/frankfurt/etoy31.htm>

El 1996, la comissió internacional de les Forces Armades Revolucionàries de Colòmbia (FARC) va recomanar crear una pàgina interactiva per a poder comunicar-se amb tot el món des dels fronts de combat. “Una forma de medir la intensidad del conflicto colombiano, tal vez la más rápida para quienes viven fuera de este país, es ingresar a las páginas de Internet de los actores armados: la guerrilla, los paramilitares de ultraderecha y el ejército nacional. Allí, en la autopista de la información, se libra una de las batallas más intensas y menos conocidas, aunque se trata de un enfrentamiento virtual no tan cruento como el que se vive a diario en las selvas y cordilleras colombianas desde hace cuatro décadas. Las primeras incursiones armadas a la Web las hizo la guerrilla hace cinco años, con el principal grupo rebelde del país, las Fuerzas Armadas Revolucionarias de Colombia (<http://www.farcep.org/>). (...) Las FARC estuvieron casi medio año fuera de Internet hasta que lograron acceder a un servidor en Canadá, conectado a la Universidad de California. Cuando en Estados Unidos se enteraron de la situación volvieron a sacarlos de la red acusados de promover ataques contra terceros y de violar las normas informáticas norteamericanas. Desde hace dos años consiguieron en forma clandestina otro servidor con el que funcionan actualmente en seis idiomas: español, inglés, francés, italiano, alemán y portugués. ‘Pelear sólo a través de Internet sería como disparar balas de caucho. No utilizar Internet sería seguir peleando contra el ejército con una escopeta’, dijo Calarcá al reconocer la importancia estratégica de este servicio. En su página se pueden leer desde los partes de guerra a partir de 1997 hasta poemas escritos por guerrilleros. Hay una página universitaria, porque buena parte de los mensajes están dirigidos a captar la atención de los jóvenes, para ellos potenciales nuevos militantes. (...) Por esta vía “paras” y rebeldes tienen acceso a información sobre el mercado internacional de armas y consultan manuales de manejo y mantenimiento de fusiles, explosivos, misiles y helicópteros. Ante esta avalancha electrónica al gobierno no le quedó otra opción que entrar a la batalla virtual con páginas como la del Ejército (www.ejercito.mil.co) donde funciona una agencia de noticias que registra los resultados contra la guerrilla, los paramilitares y el narcotráfico, el negocio clandestino que financia la guerra. (...) El paso siguiente que dieron todos fue la formación de hackers capaces de penetrar las páginas de su enemigo y bloquearlas. La guerrilla ha logrado bloquear mensajes militares y viceversa. Cuando se conoció de la renuncia de Castaño lo primero que se dijo fue que era obra de ‘hackers de la guerrilla’.”²⁴⁴ La construcció de la primera seu web es va fer a través de delegats internacionals com Marcos León Calarcá, que des de la

²⁴⁴ Nelson Padilla: “Internet, otro campo de batalla donde se libra la guerra colombiana. Guerrilleros, paramilitares y ejército tienen sus páginas en la Web · Y desde allí “pelean” en una guerra virtual”. *Diario Clarín*, 7 de juliol 2001 <http://old.clarin.com.ar/diario/2001/07/07/i-04601.htm>

ciutat de Mèxic va coordinar la implementació de la seu en un servidor de l'empresa mexicana Teesnet. Aquesta seu va funcionar fins el setembre de 1996, quan l'empresa va cancel·lar el compte per les implicacions polítiques internacionals. Pel gener de 1997, els rebels van penjar el seu web d'un servidor canadenc vinculat al campus de la Universitat de Califòrnia a San Diego; però la seva presència violava les normes del servei virtual d'aquesta universitat, que prohibeixen les pàgines web que promouen danys o perjudicis contra qualsevol grup o individu. Les FARC varen estar quasi mig any fora d'Internet, fins que varen trobar un servidor al Canadà, però els Estats Units els tornaren a treure de la xarxa acusant-los de promoure atacs contra tercers i de violar les normes informàtiques nordamericanes. El 1999 aconseguiren, de forma clandestina, un altre servidor on hi està allotjada la seva seu web actual²⁴⁵. Un membre de les FARC, amb base a la ciutat de Mèxic, és el responsable del disseny, i el contingut és subministrat pels comandants i els combatents. S'hi poden llegir des dels "partes" de guerra a partir de 1997 fins a poemes escrits per guerrillers. També s'hi edita una revista en línia i un programa de ràdio. També hi ha una pàgina universitària, ja que bona part dels missatges estan adreçats a captar l'atenció dels joves colombians²⁴⁶. Quan el president Andrés Pastrana es va internar a la selva per entrevistar-se amb el comandant suprem de les FARC, Manuel Marulanda Vélez "Tirofijo" el juliol de 1998, per a iniciar les converses de pau, els preparatius van ser realitzats minut a minut a través d'Internet. Marulanda, que té més de 70 anys, amb el seu portàtil connectat per telèfon via satèl·lit, enviava per correu electrònic a un intermediari indicacions exactes sobre el seu parador. Els missatges eren retransmesos a Pastrana mentre volava en un avió de la Creu Roja al lloc de reunió²⁴⁷. "Con el advenimiento del "Plan Colombia", financiado por Estados Unidos para combatir el comercio de heroína y cocaína en el sur de Colombia, los jefes de las FARC súbitamente han encontrado nuevos motivos para navegar. 'Esta información nos va a resultar muy útil', dijo el comandante guerrillero, mientras buscaba puntos débiles en el diagrama del helicóptero Blackhawk de trece millones de dólares, 20 de los cuales le fueron donados a Colombia por Washington."²⁴⁸ Internet no és l'únic mitjà d'informació que fan servir els guerrillers de les FARC; a través d'antenes parabòliques penjades dels arbres, alguns d'aquests combatents tenen accés a més de 100 canals d'esports i entreteniment. "David Beckham es mi héroe. Lo veo en Sky cada vez que me lo permiten mis comandantes", le dijo recientemente un joven combatiente de las

²⁴⁵ FarcEp.org, Fuerzas armadas revolucionarias de Colombia, <http://www.farcep.org/>

²⁴⁶ Veure Julia Scheeres, "Blacklisted Groups Visible on Web". *Wired New*, sense data, <http://www.wired.com/news/politics/0,1283,47616,00.html>

²⁴⁷ Karl Penhaul, "Novedad en el frente". *Revista Poder* <http://www.revistapoder.com/NR/exeres/12BEF2DE-2EA0-4CA7-83A9-E8CD15021975.htm>

²⁴⁸ Ibid.

FARC llamado Andrés a un periodista extranjero, refiriéndose al jugador estrella del equipo inglés de fútbol Manchester United.”²⁴⁹

L'ús d'Internet per part de l'organització ETA no passarà a la història per la seva originalitat i intensitat, però sí pels atacs que va rebre de nombrosos internautes espanyols. El 1997 la revista *iWorld* va publicar: “La comunitat espanyola d'internautes ha plantat cara en la xarxa al grup terrorista ETA i al seu entorn, com a reacció al segrest i posterior assassinat del regidor del partit Popular d'Ermua (Biscaia), Miguel Ángel Blanco Garrido. Al crit unànime de ¡Basta ya!, els internautes espanyols han reproduït en els diferents serveis de la xarxa les massives mobilitzacions que s'han repetit per tot el país des que es va conèixer la notícia, unint-se a la indignació general i a la repulsa pel brutal assassinat.”²⁵⁰ Un mes després de l'assassinat de Miguel Ángel Blanco es va produir un bombardeig de missatges que pretenia saturar el proveïdor de serveis d'Internet IGC (Institute for Global Communication) de San Francisco, amb l'objectiu de desallotjar l'*Euskal Herria Journal*, una publicació pro-ETA editada per un grup de simpatitzants des de Nova York. Els atacants al·legaven que IGC fomentava el terrorisme.²⁵¹ Com a resultat de l'acció, el servidor d'e-mail d'IGC es va col·lapsar i la línia telefònica d'ajuda també. Els atacants també enviaren “spams” als clients i treballadors d'IGC i penjaren a les seves webs ordres de compra amb números de tarja de crèdit erronis. IGC va tancar la seu de l'*Euskal Herria Journal* el 18 de juliol de 1997, però pocs dies després va reparèixer en tres servidors. Chris Ellison, portaveu de la Campanya per la Llibertat a Internet –grup anglès que va hostatjar una d'aquestes seus– va manifestar que “la xarxa ha de generar l'oportunitat de llegir i debatre les idees controvertides”²⁵². Un mes després que IGC tanqués els seus servidors a la publicació basca, la brigada antiterrorista de Scotland Yard va tancar el servidor en el Regne Unit del grup Campanya per la Llibertat a Internet, pel fet d'haver allotjat aquesta publicació. Alguns quadres d'ETA²⁵³ van decidir contraatacar virtualment i varen rastrejar l'origen de milers de missatges que reclamaven acabar amb la violència i bloquejaren les pàgines d'alguns dels manifestants virtuals. El cas més notori de hacktivisme pro etarra va tenir lloc a l'abril del 2000, quan un grup d'activistes modificaren la pàgina oficial del Museu Guggenheim de Bilbao, i l'ompliren amb eslògans separatistes i fotografies de membres empresonats d'ETA. Amb tot, l'ús

²⁴⁹ Ibid.

²⁵⁰ Miguel Angel Ferreira, Los internautas españoles se unen contra ETA. *Revista iWorld*, 1997. Veure el portal d'ehj Navarre http://www.ehj-navarre.org/aejh/aejh_ehj_press.html

²⁵¹ Bombardeo al servidor de *Euskal Herria Journal* <http://www.rojuser.net/ciberpol/ciberpol/spa/terror/eta.htm> i també Gordon Thomas, EEUU ya espía a ETA http://www.rojuser.net/ciberpol/ciberpol/spa/terror/usa_espia_eta.htm

²⁵² Dorothy E. Denning, *Activism, hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, <http://www.nautilus.org/info-policy/workshop/papers/denning.html>

²⁵³ Veure l'article d'Al Goodman: *ETA en la Red*. CNN en espanyol <http://cnnespanol.com/especial/2001/mundo.interactivo/stories/societies/eta/>

d'Internet per part de militants d'ETA no ha posat en evidència una concepció veritablement estratègica sobre els usos potencials de la xarxa.

També l'ús que l'Exèrcit Republicà irlandès (IRA) feia d'Internet era discret i evitava qualsevol crida a la lluita directa o a la violència. La seva estratègia d'imatge mirava d'evitar qualsevol associació amb el terrorisme. No es troben seus ni publicacions oficials de l'IRA a Internet. La seva presència virtual es dóna de forma indirecta, bàsicament a través del seu braç polític, el Sinn Féin²⁵⁴, a la web del qual hi ha un enllaç a la versió en línia d'*An Phoblacht/Republican news*, una publicació setmanal que lluita des de fa més de 25 anys pel final del domini britànic a Irlanda del Nord, i que representa l'ideari polític de l'IRA. El perfil moderat de les seues vinculades a l'IRA no ha provocat casos de censura governamental. L'excepció és el tancament de la seu IRARadio.com pel FBI, a Nova York, acusada de donar suport al Real IRA (una facció dissident de l'IRA), a l'octubre del 2001. L'explicació oficial del govern americà va ser la següent: "El president Bush recentment va signar una nova llei que permet al FBI i a la CIA confiscar actius sense previ avís davant la presència d'evidències raonables que qualsevol persona o empresa assisteixi, recolzi o faci alguna cosa que pugui ser qualificada com a terrorisme, o mantingui connexions amb terroristes de qualsevol mena"²⁵⁵. Així mateix, es prohibeix al Real IRA recaptar fons en els Estats Units i rebre el suport d'algú. També explica que, en revisar el codi font de la seu, s'havia trobat en els meta tags (lloc on s'escriuen les paraules que seran detectades pels cercadors d'Internet) expressions com "bombs", "blowing up british", "down with the brits", "freedom". També ens trobem amb censura exercida per servidors o universitats, que esborren fitxers que feien referència a l'exèrcit republicà. Aquest és un fenomen que sovinteja a Internet: quan s'intenta accedir a seues vinculades amb grups guerrillers o terroristes, es pot comprovar que alguns enllaços no funcionen, posant en evidència que els servidors on estan hostatjades aquestes seues escanegen periòdicament els fitxers emmagatzemats i eliminen la informació "compromesa".

També els grups extremistes musulmans han trobat en Internet un mètode per a difondre les seues idees i transmetre missatges als seus seguidors. El febrer de 1998, Dale Watson, cap de la secció de terrorisme internacional del FBI, va informar a un comitè del senat dels Estats Units que els principals grups terroristes islàmics utilitzaven Internet per a difondre propaganda i reclutar nous membres. A partir dels atemptats de l'11 de setembre, les seues que fan crides a la Jihad han estat sotmeses a

²⁵⁴ Seu del Sinn Féin, <http://sinnfein.org/>

²⁵⁵ James Middleton, FBI shuts down 'IRA' website, article publicat a *vnunet.com* el 12 d'octubre del 2001 <http://www.pcw.co.uk/News/1126099>

una intensa vigilància i, en molts casos, han estat clausurades. "Obtenir informació sobre com recaptar fons per a una croada antioccidental, construir una bomba o fer que els creients musulmans s'incorporin als camps guerrillers d'entrenament ha estat fins ara tan senzill com anar a Yahoo o a qualsevol altre portal d'Internet" afirmava Stephanie Gruner²⁵⁶. Un dels casos amb més ressò fou el d'Azzam.com, seu a càrrec d'Azzam Publications. Aquesta pàgina fou víctima d'un seguit de violacions fetes a Alemanya el setembre del 2001. Azzam.com ofereix continguts del tipus "Com em puc entrenar per a la Guerra Santa", i la quantitat de visites es va multiplicar per deu després dels atemptats. Diverses persones i institucions varen protestar davant les empreses d'Internet que l'hostatjaven, entre elles el FBI, i la seu va ser clausurada; el seu portaveu no entenia com en nom de la llibertat es podien clausurar les seves seus web.

9. L'artivisme, entre l'ètica i l'eficàcia

No hi ha consens sobre les accions de desobediència civil electrònica, o sobre les accions hacker amb finalitats polítiques o, en general, sobre la política extraparlamentària d'acció directa a la xarxa. Una part de les crítiques tenen a veure amb l'efectivitat de les protestes: són efectius aquests mètodes d'activisme informatitzat? Si es tracta de cridar l'atenció sobre qüestions concretes fent servir accions poc comunes que tinguin un cert ressò mediàtic, aleshores es pot dir que el nivell d'efectivitat és alt. Si el que es pretén és mobilitzar molta gent per assolir objectius de canvi polític, aleshores probablement aquestes tècniques no són massa efectives. Sembla, doncs, que el hacktivisme pot funcionar com a complement dels esforços organitzatius que ja existeixen.

La difusió és, doncs, un aspecte clau de l'activisme artístic. Ja el vídeo art activista havia tingut problemes de difusió, ja que les cadenes públiques de TV no el difonien (bàsicament s'emetia per cadenes locals). L'opció més habitual era la d'optar per distribuïdores independents amb el consegüent àmbit reduït de difusió. Si a això hi afegim que les obres de vídeo art només solen interessar als vídeo artistes, l'eficàcia de les propostes de l'activisme videoartístic s'havien de mesurar pel seu impacte i el seu potencial comunicador (quantitat d'individus susceptibles de ser afectats i implicats). Pel seu caràcter minoritari i amb un radi d'acció tant reduït hom té la

²⁵⁶ Stephanie Gruner, "Extremist web sites under scrutiny". *The Wall Street Journal*, 8 d'octubre de 2001 <http://www.indymedia.org.uk/en/2001/10/13461.html>

sensació d'estar davant d'una interacció només entre vídeoartistes. Per tot plegat, és lògic que l'activisme artístic hagi vist en Internet la possibilitat de trencar aquesta endogàmia, democratitzar l'art i ampliar la fins ara difusió selectiva. A partir de la xarxa les obres i els artistes podien prescindir de les institucions oficials del món de l'art (museus, galeries, curadors...). Ha superat, tanmateix, l'art activista les barreres imposades pels espais institucionals? La resposta és afirmativa si pensem en els espais físics, però negativa si tenim present que la majoria de seus web es troben en URL progressivament institucionalitzades. Per altra banda, les institucions incorporen i assimilen iniciatives que, a simple vista, atempten contra les seves pròpies estructures de poder: els artistes segueixen sense independitzar-se de la mediació institucional.

En els 70 era fàcil reconèixer l'enemic: s'hostatjava on hi havia la censura, el conservadorisme i l'explotació. Són d'aquesta dècada la negativa del MOMA a participar en la distribució de la fotografia de Ronald Haerberle *Q. And Babies? A. And babies*²⁵⁷, o bé la censura del Guggenheim de Nova York a una exposició de Haacke després de la instal·lació *MOMA-Poll* que aquest havia organitzat al MOMA. Actualment, es fa més difícil destriar els elements de control i censura culturals, atesa una certa i aparent permissivitat i actitud conciliadora del pensament únic neo-liberal que amaga, tanmateix, noves i més poderoses formes de control sota una aparença de neutralitat. Per això Internet s'ha volgut veure com "un nou espai de llibertat", oblidant el que diu Bourdieu: "la llibertat no és una cosa donada, sinó una conquesta, i col·lectiva"²⁵⁸.

Però també Internet és utilitzat de forma selectiva (només entren a les seus web d'art els interessats en art). Qui i quants han entrat a la seu web del Critical Art Ensemble i s'ha descarregat els Book Projects²⁵⁹ que ofereix en línia? A quants internautes se'ls ha penjat l'ordinador navegant per l'obra de JODI²⁶⁰? Certament, Internet permet una gran accessibilitat, però com crear l'interès per accedir a la seu web del grup The Cult of the Dead Cow²⁶¹ la finalitat del qual és la de bloquejar o sabotejar els fluxos d'informació de les corporacions i institucions tradicionals? Un dels problemes, doncs, de les noves formes d'art i, en particular, de l'activisme informàtic, és el d'atreure i implicar a més població, captar més interactors. També des del punt de vista tècnic en tot el referent a codis informàtics, hi ha una certa tendència a valorar l'amplada de

²⁵⁷ Ronald Haerberle *Q. And Babies? A. And babies*.

http://lists.village.virginia.edu/sixties/HTML_docs/Exhibits/Track16/And_babies.html

²⁵⁸ Bourdieu, P. (1988), *Cosas dichas*. Barcelona. Gedisa

²⁵⁹ Critical Art Ensemble: Books Projects, <http://www.critical-art.net/books/index.html>

²⁶⁰ Seu de JODI, <http://www.jodi.org>

²⁶¹ Seu de Cult of the Dead Cow, <http://www.cultdeadcow.com>

banda i tota acció que l'obstrueixi es considera negativa. I no cal dir que molts consideren inadequades aquestes tàctiques pel seu caràcter il·legal.

Mentre existeixi Nablus²⁶², per a què necessitem l'art? Quina funció social compleix l'art i l'artista? Pot l'art aportar alguna cosa a la societat? Tenen algun sentit l'art i els artistes? Podem partir d'una constatació: la cultura té un poder per a determinar com la gent apercip el món que l'envolta; i l'art –un tipus d'art, si més no– pot, a partir de la subversió i la mobilització, modificar, transformar, reconfigurar i desconstruir la “cultura oficial”, la cultura del pensament únic neoliberal, la “cultura” del capital. Com? L'activisme artístic s'enfronta i critica l'homogeneïtat de la cultura dominant, que només beneficia uns quants però que ens afecta a tots. Aquesta cultura pretén que tothom ha de saber i fer el mateix en el mateix moment i de la mateixa manera. Nega, doncs, la llibertat de creació i defensa, només, la llibertat de consum. L'art activista pot reflectir l'experiència vital de la diferència. L'activisme artístic defensa el dret a participar i a ser testimoni de la més gran diversitat possible de formes d'expressió, ja que es basa en una visió de l'art com a intercanvi comunicatiu. L'expressió personal és un requisit previ per a l'autoafirmació i aquesta és un element indispensable per a la cultura; això no vol dir que tothom hagi de fer art, de la mateixa manera que crear un poble políticament conscient no significa que tothom hagi d'esdevenir un polític professional. La creació artística no està lligada, doncs, tant a la producció d'objectes com a la definició d'identitats. L'art activista no està circumscrit a cap estil particular, no es limita als mitjans artístics tradicionals i abasta moltes diferents activitats: cartells, performances, instal·lacions, vídeo, xarxes... Es tracta de diversificar les formes d'expressió i no de limitar les alternatives possibles. Els artistes activistes veuen l'art com un diàleg, una interacció entre autor i receptors, i no com una lliçó especialitzada sobre bellesa o ideologia que s'imparteix de dalt a baix. Per això l'art activista està orientat al procés: tant important com el resultat final (si és que n'hi ha) la veritable obra inclou el procés creatiu i interactiu. L'activisme artístic és contestatari i crític: s'enfronta als valors de la classe dominant, a les institucions artístiques (museus, galeries...), a la semantització androcèntrica i etnocèntrica, i a qualsevol procés de deshumanització, subministrant imatges alternatives, informació, metàfores concebudes a base d'ironia i provocació, amb l'objectiu de fer audibles i visibles les veus i les cares fins fa poc invisibles i impotents (l'art fa visible l'invisible, com deia Paul Klee).

²⁶² Nablus during the invasion, <http://www.nablus.org/invasion/during.html>

Els artistes per sí sols no poden canviar el món: cap persona pot fer-ho mentre romanguí sola. Però el paradigma de la complexitat ens ha mostrat el poder de la impotència, el poder del gest aparentment inútil (quan pesa un floc de neu? Quasi bé res. Però quan una infinitud de flocs s'acumulen damunt d'una branca d'arbre, la poden trencar per gruixuda que sigui; però cal que caigui el darrer floc...) I com és el poder de l'art? És un poder subversiu, transgressor, i no pas autoritari; no imposa, suggereix; no dicta, sinó que invita a la lectura; no ensenya, sinó que estimula l'aprenentatge. I on rau aquest poder? Radica en com connecta la capacitat de fer amb la capacitat de veure, i a fer que altres vegin que ells també poden fer alguna cosa amb el que veuen. Perquè el que sí que podem fer, encara, és elegir i formar part del món que està canviant.

10. L'ètica hacker

El filòsof finlandès Pekka Himanen²⁶³ fa un plantejament original contraposant l'ètica protestant, que representaria l'esperit del capitalisme, a l'ètica hacker que podria esdevenir la matriu cultural de l'era de la informació. No es vol pas dir que els creadors de la societat de la informació han de ser hackers, de la mateixa manera que els protagonistes del capitalisme no eren tots protestants. El que mira d'argumentar Himanen és que tot canvi tecnoeconòmic i tota apropiació social d'una determinada tecnologia es produeix des d'un determinat sistema de valors en interacció amb aquesta tecnologia. En el cas del capitalisme, i segons el conegut estudi de Max Weber²⁶⁴, el desenvolupament del capitalisme va anar de la mà de l'ètica del treball i de l'acumulació de capital a l'empresa com a forma de salvació personal (cosa que, paradoxalment, no està en contradicció amb l'explotació dels altres, sigui dels assalariats, dels esclaus o dels nens).

Segons Manuel Castells "en l'era de la informació, la matriu de tot desenvolupament (tecnològic, econòmic, social) rau en la innovació, en el valor suprem de la innovació que, potenciada per la revolució tecnològica informacional, incrementa exponencialment la capacitat de generació de riquesa i d'acumulació de poder. Però innovar no és un valor obvi. Ha d'anar associat a una satisfacció personal, del tipus que sigui, lligada a l'acte de la innovació. Això és la cultura *hacker*, segons Himanen.

²⁶³ www.hackerethic.org. Per a aquest apartat s'han seguit les seves argumentacions i tesis presentades en el llibre Pekka Himanen (2003), *L'ètica del hacker i l'esperit de l'era de la informació*. Barcelona. Pòrtic i Editorial UOC, de lectura imprescindible, tot i el seu caràcter de vegades massa ingenu i utòpic.

²⁶⁴ Weber, Max (1994), *L'ètica protestant i l'esperit del capitalisme*. Barcelona. Ed. 62. Col. Clàssics del pensament modern.

El plaer de crear per crear. I això mou el món, sobretot el món en el qual la creació cultural, tecnològica, científica i també empresarial, en l'aspecte no crematístic, es converteix en força productiva directa per la nova relació tecnològica entre coneixement i producció de béns i serveis. Es podria argumentar que, segons aquesta definició, hi ha *hackers* pertot arreu i no solament en la informàtica. I aquest és, en realitat, l'argument de Himanen: que tothom pot ser *hacker* pel que fa i que qualsevol que es mogui per la passió de crear en la seva activitat està motivat per una força superior a la dels guanys econòmics o la satisfacció dels seus instints. El que passa és que la innovació tecnològica informàtica té el pinyó directe sobre la roda del canvi en l'era de la informació; d'aquí ve que la cultura *hacker* es manifesti de manera particularment espectacular en les tecnologies d'informació i a Internet.”²⁶⁵

El hacker programa perquè troba que la programació és intrínsecament interessant, emocionant i divertida; els reptes que li planteja la programació l'estimulen i fa que tingui ganes d'aprendre'n més. Així ho descriu la hacker irlandesa Sarah Flannery: “M'apassionava... Treballava sense parar durant dies i dies perquè era molt emocionant. De vegades no volia parar.”²⁶⁶ Tot i desenvolupant la tecnologia del xifratge, comenta que “sempre que programava alguna cosa acabava jugant durant hores en comptes de tornar al paper a fer la feina més dura i pesada”²⁶⁷. Linus Torvalds ha descrit, en missatges a la xarxa, com Linux es va començar a expandir a partir de petits experiments amb l'ordinador que acabava de comprar, i afirma que la seva motivació és que “era divertit”. La idea de joc és molt present en la creació i desenvolupament de programari. Per la seva banda, Tim Berners-Lee, el creador del WWW, descriu que va començar amb experiments que comunicaven el que ell anomenava programes de joc; Wozniak explica que moltes característiques de l'ordinador Apple “provenen d'un joc, i les característiques divertides que s'hi van incorporar eren només per a fer un projecte curiós, que era programar (...) [un joc anomenat] Breakout i mostrar-lo al club”²⁶⁸. Per a resumir l'esperit de l'activitat hacker i l'ètica del treball, Eric Raymond fa servir mots com passió, jugar, importar, explicar: “Per a seguir la filosofia de Unix bé, has de ser lleial a l'excel·lència. Has de creure que el programari és un art que es mereix tota la intel·ligència i la passió que tinguis (...) El disseny i la implantació de programari hauria de ser un art alegre, i una mena de joc d'alt nivell. Si aquesta actitud et sembla absurda o vagament violenta, pensa-t'hi; has oblidat res? Per què dissenyes programes en comptes de fer una altra cosa per

²⁶⁵ Manuel Castells *Hackers, crackers, llibertat i seguretat*. Lliçó inaugural del curs acadèmic 2001-2002 de la UOC <http://www.uoc.edu/web/cat/launiversitat/inaugural01/hackers.html>

²⁶⁶ Sarah Flannery i David Flannery (2000), *In Code: a mathematical journey*. Londres. Profile Books, pàg. 182

²⁶⁷ *ibid.* Pàg. 182

²⁶⁸ Connick. “...And Then There Was Apple”, Call-APPLE, octubre 1986, pàg. 24

aconseguir diners o passar l'estona? Algun cop deus haver pensat que el programari era digne de les teves passions (...) Per a fer la filosofia Unix bé, has de tenir (o recuperar) aquesta actitud. T'ha d'importar. Has de jugar. Has d'estar disposat a explorar.”²⁶⁹ [Retrobem, aquí, una nova convergència de les metanarratives del joc amb l'actitud hacker sobre la programació com a joc].

Aquesta relació apassionada amb el treball és una actitud de la majoria de hackers informàtics, però també es pot estendre a totes les altres professions. Ja a la primera conferència de hackers a San Francisco, el 1984, Burrell Smith, el hacker que hi ha al darrere l'ordinador Macintosh d'Apple, va definir el terme d'aquesta manera: “Els hackers poden fer pràcticament qualsevol cosa i ser un hacker. Pots ser un fuster hacker. No ha de ser necessàriament alguna cosa relacionada amb l'alta tecnologia, sinó que es tracta d'un treball artesà, de tenir cura pel que es fa”.²⁷⁰ Raymond destaca en la seva guia *How to Become Hacker* que “hi ha gent que aplica l'actitud hacker a altres coses [que no són programació], com l'electrònica i la música; de fet, es pot trobar als nivells més elevats de qualsevol ciència o art”.²⁷¹ L'actitud hacker pot considerar-se com un exemple excel·lent d'una ètica del treball oposada a l'ètica del treball protestant, base de l'esperit del capitalisme segons l'estudi de Max Weber²⁷²: “La idea tan peculiar –i tant corrent avui en dia, però tan poc evident en ella mateixa– del deure professional, és a dir, d'una obligació que l'individu ha de sentir i de fet sent davant el contingut de la seva activitat ‘professional’, sigui la que sigui i independentment que la senti com una pura utilització de la seva força de treball o de la simple utilització d'uns béns que hom posseeix (‘capital’), és la idea més característica de tota l'‘ètica social’ de la civilització capitalista, per a la qual posseeix en cert sentit una significació constitutiva. (...) [és necessari] a més d'un sentiment força desenvolupat de la pròpia responsabilitat, una mentalitat que a l'hora de la feina sàpiga prescindir de la vella qüestió de combinar el guany habitual amb un màxim de comoditat i un mínim d'esforç, per a practicar al contrari el treball com a finalitat absoluta en ella mateixa, com a veritable ‘professió’, o àdhuc ‘vocació’”.²⁷³

Vet aquí com el predicador protestant Richard Baxter expressa aquesta ètica del treball: “És per a l'acció que Déu ens manté, nosaltres i les nostres activitats: el treball és la fi, tant moral com natural, de tot el poder” i dir “el que jo vull és pregar i meditar,

²⁶⁹ Eric Raymond (2000), *The Art of Unix Programming*, cap. 1 <http://www.catb.org/~esr/writings/taoup/html/>

²⁷⁰ Steven Levy (1994), *Hackers: Heroes of the Computer Revolution*. Nova York. Delta, pàg. 434

²⁷¹ Eric Steven Raymond (1999), *How to Become a Hacker*, pàg. 232 <http://www.catb.org/~esr/faqs/hacker-howto.html>

²⁷² Weber, Max (1994), *L'ètica protestant i l'esperit del capitalisme*. Barcelona. Ed. 62. col. Classics del pensament modern.

²⁷³ Idem, Pàgs.. 76 i 85

fóra com si el teu servent es negués a fer la feina principal i es dediqués a coses menys importants i més senzilles²⁷⁴. A Déu no li agrada de veure gent que es limita a meditar i a pregar, sinó que vol que treballin. Baxter enumera les tres actituds centrals de l'ètica del treball protestant: la feina s'ha de considerar com un fi en si mateix, s'ha de fer tan bé com sigui possible i s'ha de considerar un deure, que s'ha de fer perquè s'ha de fer.

Abans de la Reforma, el treball no formava part dels ideals més elevats de l'Església: al cel no s'havia de treballar. El paradís era positiu, el treball negatiu. Segons sant Agustí al cel trobarem un diumenge perenne. El treball és un càstig, per això a l'infern hi ha una tortura encara més cruel que la tortura física: el treball fatigant perenne. A la *Divina Comèdia*, Dant ens presenta els pecadors que han dedicat la vida als diners, tant els pròdigs com els avars, condemnats a empènyer enormes pedres en un cercle etern²⁷⁵. I tot plegat es remunta a la mitologia grega, que ens explica com Sísif va ser condemnat a empènyer eternament una gran roca i fer-la arribar al cim de la muntanya només per veure com, tan bon punt arribava al cim, la pedra tornava a caure inexorablement muntanya avall.²⁷⁶

L'ètica protestant va posar el treball al centre de la vida, i el descans a la perifèria. El treball va esdevenir un fi en ell mateix i *Robinson Crusoe* (1719) de Daniel Defoe l'exemple a seguir. L'actitud dels hackers s'assembla més a l'ètica precapitalista que a la protestant. No es tracta de no treballar ni de reproduir l'ideal platònic segons el qual en la millor societat possible només les classes més baixes i els esclaus treballarien²⁷⁷, sinó de treballar apassionadament encara que no sempre això sigui un joc divertit. Per això Linus Torvalds descriu el seu treball a Linux com una combinació de diversió i treball seriós. Raymond diu a la seva guia: "Ser un hacker és molt divertit, però és una classe de diversió que implica molt d'esforç"²⁷⁸. L'activitat hacker és apassionada i creativa, però també implica un dur treball, i si cal també s'ha d'estar disposat a fer les parts menys interessants però necessàries per a la creació del conjunt.

Entre els consells que Benjamin Franklin donava a un jove comerciant el 1748²⁷⁹ s'hi pot llegir: "Recorda que el temps és or. Aquella persona que pot guanyar deu xílings al dia amb el seu treball, i marxa fora o seu sense cap ocupació, mig dia, encara que

²⁷⁴ Citat a Weber, *L'Ètica protestant*, pàg. 223, n.13 i pàg. 225, n. 19

²⁷⁵ Dant, *Divina comèdia*, Infern 7.25-35

²⁷⁶ Homer, *L'Odissea*, XI, 593-600

²⁷⁷ Plató, *República*, 371 d-e, 347 b, 370 b-c

²⁷⁸ Eric S. Raymond: *How to Become a Hacker*, <http://www.sindominio.net/biblioweb/telematica/hacker-como.html>. En català, *Com convertir-te en un hacker*, a http://dilvert.com/andreu/hacker_howto.html

²⁷⁹ Benjamin Franklin, *Advice to a Young Tradesman*, 1748, <http://www.angelfire.com/biz3/eserve/ayt.html>

només dediqui sis penics a la seva diversió o ociositat, no hauria de pensar que aquesta ha estat l'única despesa, sinó que realment ha gastat, o, més aviat, ha dilapidat, cinc xílings més". Vet aquí l'expressió més pura de la concepció del temps segons l'esperit capitalista. "No tinc temps" és una de les frases més repetides a les societats occidentals industrialitzades. "Vaig de bòlit" és la manera de definir que el temps passa encara més intensament per a nosaltres. L'economia informacional ha comprimit el temps, l'ha intensificat, accelerat, optimitzat, creant una cultura de la rapidesa construïda a base de dates de lliurament, de menjars preparats amb el microones, de trucades perdudes de mòbil.

La llei de Gordon Moore segons la qual l'eficiència dels microprocessadors es duplica cada divuit mesos, la llei d'acceleració contínua de Jim Clark sobre el ritme de creació de nous productes tecnològics, les lleis de Michael Dell sobre l'externalització de les operacions que no són claus per a l'empresa, semblen anar en la mateixa direcció d'estimular el capital a moure's més de pressa que mai: el capital ha d'estar preparat per a una inversió ràpida en innovació tecnològica o en objectius en canvi constant en els mercats financers. La compressió del temps ha arribat a un punt en què la competició tecnològica i econòmica consisteix a prometre que el futur arribarà més de pressa al consumidor amb la nostra empresa que amb la competència. El futur ja és aquí, ens diuen; el present, doncs, ja ha quedat obsolet.

L'ètica protestant ja ho deia que no hi havia temps per a jugar al treball. A l'era de la informació aquest ideal d'optimització del temps afecta ara tots els àmbits de la vida d'una persona, totes les seves activitats. Ara, per exemple, ja no juguem, entrenem: en el gimnàs es treballen els músculs; ja no ens relaxem, sinó que anem a classes de tècniques de relaxació; no juguem a tennis, sinó que practiquem el revés. No podem ser només aficionats a les nostres aficions: hem de treballar-les. Fins i tot el poc temps lliure del que disposem ha d'optimitzar-se, ha de ser un temps de qualitat, programat i planificat com el temps de treball. El nou símbol d'estatus és 'estar ocupat'. A la llar s'han eliminat les converses perquè és més fàcil prémer el comandament a distància i veure comèdies en què surten pares i fills que parlen entre ells.

L'ètica protestant va introduir la idea del temps de treball regular com a centre de la vida. El treball repetit regularment organitza tota la resta d'usos del temps: "El treball regular o eventual que el jornalero ordinari es veu obligat a agafar representa una situació transitòria, sovint inevitable i en qualsevol cas indesitjable. A la vida de l'home

'sense professió' li mancarà sempre aquell caràcter sistemàtic i metòdic que exigeix (...) l'ascetisme intramundà"²⁸⁰.

Tot i que les tecnologies de la informació redueixen el temps i el fan més flexible, el desseqüencien, i que amb la xarxa i el telèfon mòbil es pot treballar on i quan es vulgui, el treball en l'economia informacional és reforçat com a centre de la vida: els professionals de la informació fan servir la flexibilitat per a fer que el temps lliure estigui més disponible per a breus intervals de treball i no a l'inrevés. Si en el passat una persona formava part de l'elit quan no havia de córrer d'un lloc a l'altre, avui l'elit està formada per gent que sempre està en moviment, que sempre està pendent d'alguna data límit. Si la reducció de la jornada laboral va ampliar el temps lliure del diumenge a divendres tarda, l'optimització i la flexibilitat del temps estan aconseguint que el diumenge i el dissabte s'assemblin més al divendres.

Els hackers, per contra, optimitzen el treball per a tenir més espai per al joc, per a fer experiments que no tinguin objectius immediats. El treball no és sempre el centre de la seva activitat; utilitzar màquines per a l'optimització i flexibilitat del temps hauria de conduir els éssers humans a una vida que fos menys semblant a les màquines, menys rutinària.

En l'economia de la informació la font de productivitat més important és la creativitat, i no es poden crear coses interessants amb presses o de forma regulada de nou a cinc. Cal, doncs, permetre la diversió, estimular l'estil individual de creativitat i no establir calendaris de projectes massa a curt termini. Supervisar i controlar el temps de treball és fruit d'una cultura que considera els adults massa immadurs per a ser responsables de la seva vida, significa que només una elit té prou maduresa per a responsabilitzar-se d'ells mateixos i que la majoria ha d'estar sotmesa a un grup d'autoritat reduït. Els hackers sempre han estat en contra de l'autoritarisme: "S'ha de lluitar en contra de l'actitud autoritària sempre que es trobi, per a evitar que t'ofegui a tu i a altres hackers" afirma Raymond. L'ètica hacker ens recorda que el treball és només una part de la nostra vida, en la qual també hi ha d'haver lloc per a altres passions. Descentrar el treball és una forma de respectar els éssers humans com a éssers humans. Els hackers no estan d'acord amb al frase 'el temps és or', i opten per a viure una vida plena i no una versió beta o una simple 'demo'.

²⁸⁰ Max Weber, *L'ètica protestant*, op. cit, pàg. 232

Els set valors dominants de l'ètica protestant, segons Weber, són els diners, el treball, l'optimització, la flexibilitat, l'estabilitat, la determinació i la comptabilització dels resultats. Però el bé més gran és "guanyar més i més diners". Si fins ara el treball havia estat considerat com el valor més elevat, actualment ho són els diners, de manera que el treball ha esdevingut un mer mitjà per a obtenir diners. En l'economia informacional les empreses duen a terme el seu objectiu de fer diners mirant de ser propietàries de la màxima informació, a través de patents, marques registrades i copyrights. En contrast amb aquesta ètica dels diners, els hackers emfasitzen l'obertura. Segons el *Jargon File*²⁸¹ la seva ètica parteix del principi que "compartir informació és un bé positiu i poderós, i que és un deure ètic dels hackers compartir la seva expertesa creant programari gratuït". En aquesta línia, molts hackers distribueixen els resultats de la seva creativitat de manera oberta perquè altres persones els utilitzin, els provin i els desenvolupin més. És el cas de Linux, creat per un grup de hackers que feien servir el seu temps lliure per a treballar plegats; els motivava el reconeixement dels iguals, la diversió i la vida social. "No fas res a la vida si no és per felicitat (...) Aquest és el meu teorema de la vida (...) Una fórmula simple, realment: $H = F^3$. La felicitat és igual a menjar, diversió i amics".²⁸²

En la nostra societat el treball és, en realitat, una font d'acceptació social. Ja a la societat ideal de Saint-Simon només les persones que treballaven eren ciutadans, a l'inrevés precisament de les societats ideals antigues en les quals només els homes que no havien de treballar es consideraven mereixedors de la ciutadania²⁸³. En una vida centrada en el treball i governada per l'ètica protestant, la gent gairebé no té amics que no siguin de la feina i és el lloc principal on trobar parella; en aquest estil de vida, l'activitat fora de la feina sovint no proporciona el sentiment de pertinença social, reconeixement o afecte que s'experimenta tradicionalment a casa o durant el temps lliure i, en conseqüència, la feina esdevé fàcilment en substitut de la casa. A la feina es cerca ara el que tradicionalment es trobava en el lleure.

No és fàcil entendre per quina raó hi ha hackers que dediquen el seu temps lliure a desenvolupar programes que donen obertament als altres. Eric Raymond²⁸⁴ diu que estan motivats per la força del reconeixement dels seus iguals. Per als hackers, el reconeixement dintre una comunitat que comparteix la seva passió és més important i dóna una satisfacció més profunda que els diners, com passa també en àmbits

²⁸¹ The Jargon File, <http://catb.org/~esr/jargon/html/>

²⁸² Discurs de Wozniak en el seu acte de graduació a la Universitat de Berkeley el 1986, a Rebecca Gold (1994), *Steve Wozniak a Wizard called woz*. Minneapolis. Lerner Publications, pàg. 10

²⁸³ Veure Aristòtil, *Política* 1277b-78a

²⁸⁴ Eric S. Raymond (1998), *Homesteading the Noosphere*, a http://www.firstmonday.dk/issues/issue3_10/raymond/

científics, de recerca o acadèmics. Per als hackers és important que el reconeixement dels iguals no sigui un substitut de la passió, sinó que ha de ser el resultat de l'acció apassionada, de la creació d'alguna cosa valuosa des del punt de vista social. En canvi, seguint l'ètica protestant, el treball esdevé un doble substitut, per la manca de vida social fora de la feina i per la manca d'un element de passió en la feina mateixa. La unió de vida social i de passió és el que fa que el model hacker sigui tan poderós. I és obvi preguntar-se per què, malgrat tots els avenços tecnològics, dediquem la major part del dia a allò que sol anomenar-se "guanyar-se la vida". Sembla que el progrés consisteixi no a fer la vida més fàcil sinó a fer que guanyar-se la vida sigui contínuament més difícil. "El perill és que ens civilitzem massa i que arribem a un punt (...) en què el treball d'aconseguir menjar sigui tan extenuant que en el procés d'aconseguir-lo, perdem la gana".²⁸⁵

Per als hackers, el factor organitzatiu bàsic en la vida no és el treball ni els diners, sinó la passió i el desig de crear alguna cosa socialment valuosa; però els hackers saben que en la societat capitalista és realment molt difícil ser totalment lliure si la persona no té prou capital individual. Quan es treballa per compte d'altri, la persona no pot ser lliure per a centrar el seu treball en la passió personal i perd el dret a determinar els ritmes de la seva vida. L'emergència de la societat de la informació ha permès a alguns hackers triar l'acumulació capitalista. Uns ho fan temporalment, fins que aconseguen la seva independència financera gràcies a accions o *stock options* adquirides treballant en una empresa. És el cas de Wozniak: quan es va retirar d'Apple, amb 29 anys, era propietari d'accions valorades en uns cent milions de dòlars. La independència financera multiplica per molt les possibilitats d'acció. Paradigma de hacker integrat al sistema és Bill Gates. Quan va fundar la companyia el 1975 només era un hacker com Bill Joy (un dels fundadors de SUN Microsystems), Wozniak o Torvalds, i es va guanyar el respecte dels hackers programant el primer intèrpret del llenguatge de programació BASIC sense accés a l'ordinador per al qual anava destinat, i va funcionar. Amb Paul Allen, va fundar Microsoft amb la intenció inicial de crear llenguatges de programació per a ordinadors personals, un punt de partida hackerista atès que només els hackers feien servir aquests ordinadors per a programar. En maximitzar el guany es minimitza la passió, i el reconeixement ve determinat pel poder i no per la creativitat o riquesa personal.

Un grup de hackers, fidel al seu esperit inicial, han obert noves direccions per oposar-se a la fagocitació capitalista. És l'economia basada en l'empresa de font oberta (*open*

²⁸⁵ Lin Yutang: *The importance of living*. Stocolm. Zephyr Books, pàg. 158. L'original és de 1937.

source) que desenvolupa programari en model obert. És el cas del desenvolupador de Linux, Red Hat. El Linux és un *kernel*, és a dir, la part del sistema operatiu que s'encarrega que els programes que utilitzem funcionin en el nostre ordinador; concebut per Linus Torvalds cap a l'any 1990, és multiplataforma, multiusuari i *open source*. Per multiplataforma s'entén el fet que és capaç de funcionar amb molts tipus diferents de processadors²⁸⁶; per multiusuari s'entén el fet que molts usuaris puguin treballar alhora amb el mateix ordinador. El sistema operatiu mostrarà l'ordinador a cadascun dels usuaris com si fos un ordinador per a ell tot sol, quan en realitat hi pot haver molta gent treballant amb el mateix ordinador; i per *open source* cal entendre que podem llegir, modificar el "codi font" i distribuir les modificacions que hi fem, és a dir, que podem veure com han fet el Linux, i si no ens agrada el podem modificar per tal que s'adapti a les nostres necessitats. Estem, però, obligats a publicar totes les modificacions o afegits que fem en el Linux, si és que en fem alguna.

El teòric i líder de l'open source²⁸⁷ o font oberta és el radical Richard Stallman, per a qui la paraula "free" de l'expressió "free software"²⁸⁸ no vol dir necessàriament "gratuït", sinó lliure; la seva ètica no s'oposa a guanyar diners, sinó a guanyar diners negant l'accés a informació a altres persones. El problema amb què es troben les empreses en la nova economia de la informació és que l'èxit capitalista i l'obtenció de guanys només és possible mentre la majoria d'investigadors continuï compartint la informació: rebre la informació produïda pels altres mentre es guarda tota la informació que produeix un mateix presenta, pel cap baix, un dilema ètic.

11. Ciberterrorisme, control i negoci

El 1986, un llibre que duia per títol *Softwar* afirmava que els països del pacte de Varsòvia podien incapacitar el món occidental llençant atacs contra els ordinadors militars i financers dels Estats Units i de l'OTAN²⁸⁹. El 1989 es va donar per acabada

²⁸⁶ De fet, el Linux és capaç de funcionar amb les següents processadors: els Intel x86 (386 en endavant, AMD, Cyrix, etc.), Alpha AXP, Sun SPARC, Motorola 680xx (Atari ST, Amiga, Macintosh), Digital StrongARM, MIPS, SuperH, Hewlett-Packard PA-RISC, IA-64 (Itanium, els nous processadors d'Intel), els CRUSOE de Transmeta (entre ells el TM-3120 el primer processador dissenyat expressament per funcionar amb Linux), etc.

²⁸⁷ Cfr. What is Free Software? (1996), a <http://www.gnu.org/philosophy/free-sw.html>, The GNU Manifesto (1985) a <http://www.gnu.org/gnu/manifesto.html>, i The GNU Operating System and the Free Software Movement (1999) a <http://www.gnu.org/gnu/thegnuproject>

²⁸⁸ Els dos models principals de catalogació del software són el propietari i el lliure. En Anglès, la paraula 'free' tant vol dir lliure com gratuït, però cal remarcar que el Software és lliure per la seva manca de restriccions, no per ser gratuït. Per tal que un software sigui lliure cal que sigui de lliure ús, de lliure codi i de lliure distribució. Mentre que el software propietari no deixa obrir arxius generats amb altres programes o impedeix l'ús d'un programa per a fer doses diferents per a les que ha estat dissenyat.

²⁸⁹ Veure el pròleg del llibre *Cybercrime... Cyberterrorism... Cyberwarfare...*, document desenvolupat pel Center for Strategic and International Studies (CSIS), novembre de 1998. <http://www.csis.org/pubs/cyberfor.html>

l'etapa de la guerra freda, però el perill d'un atac electrònic ja estava incorporat als discursos oficials: si ja no existia un enemic que pogués inutilitzar les instal·lacions militars, calia crear un nou motiu d'inseguretat i es va trobar en els possibles atacs contra la infraestructura civil del país. I la primera acció preventiva fou la creació, per part del govern dels Estats Units, de *The Critical Technologies Institute* (1991), organisme que va elaborar un seguit de recomanacions dividides en accions immediates, accions a curt termini i accions a mitjà termini, entre les quals hi figurava la creació de mecanismes d'alerta i d'un organisme de coordinació, i el 1996, l'ex director d'Intel·ligència Central John Deutch, en el seu testimoni davant d'un comitè del Congrés, afirmava: "Hackers criminals varen estar venent els seus serveis a estats-delinquents (*rogue states*) (...) estan utilitzant diversos esquemes per agredir els interessos vitals dels Estats Units a través d'intrusions il·legals en els ordinadors".²⁹⁰ Pel juliol del mateix any, Clinton anunciava la formació de la *Comissió Presidencial per a la Protecció de la Infraestructura Crítica*, coneguda amb les sigles PCCIP, amb l'objectiu d'estudiar les infraestructures que constitueixen el suport de la vida quotidiana dels Estats Units, determinar les seves vulnerabilitats davant d'una àmplia gamma d'amenaques i proposar una estratègia per a protegir-les en el futur. Foren identificades vuit tipus d'infraestructures: telecomunicacions, bancs i finances, energia elèctrica, emmagatzematge i distribució de gas i petroli, proveïment d'aigua potable, transports, serveis d'emergència i serveis governamentals. L'informe elaborat arribava a la conclusió que les amenaces eren reals i que les àrees analitzades eren vulnerables en diferents aspectes. "L'explotació intencional d'aquestes vulnerabilitats podria tenir serioses conseqüències per a la nostra economia, la nostra seguretat i el nostre estil de vida (...) Però quasi tots els grups consultats varen parlar amb preocupació de les noves amenaces cibernètiques, i posaren l'èmfasi en la importància de desenvolupar enfocaments que ens serveixin per a protegir la nostra infraestructura contra elles abans que es materialitzin i ens produeixin un dany més gran en els sistemes".²⁹¹ La PCCIP indicava que la possibilitat d'un atac cibernètic implicava un canvi qualitatiu en relació a tots els conceptes coneguts de seguretat. "En el passat hem estat protegits d'atacs hostils contra la nostra infraestructura per grans oceans i veïns amics. Però en el ciberespai, les fronteres nacionals ja no són rellevants. Els electrons no es paren a ensenyar el passaport. Ciberatacs potencialment seriosos podrien ser concebuts i planejats sense una preparació logística detectable. A més, podrien assajar-se de manera invisible i muntats en qüestió de minuts o fins i tot de segons sense revelar la

²⁹⁰ Citat a David Scassa, *Paper on Cyberterrorism*, 2000.

²⁹¹ Citat a Denning, Dorothy E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. <http://www.nautilus.org/info-policy/workshop/papers/denning.html>

identitat ni la ubicació de l'atacant"²⁹². La comissió va afirmar que diversos operadors qualificats d'ordinadors varen demostrar la seva habilitat per a penetrar en xarxes sense autorització. "Sigui quina sigui la seva motivació, el seu grau d'èxit a ingressar a les xarxes per alterar dades, extreure'n informació financera propietària o introduir-hi virus, demostra que (...) en el futur, algun grup interessat a provocar seriosos danys als Estats Units podria fer-ho utilitzant aquests mateixos mitjans."²⁹³

El febrer de 1998, com a resposta al citat informe de la PCCIP, el Departament de Justícia i el FBI varen crear el *Centre Nacional de Protecció d'Infrastructures* (NIPC)²⁹⁴ per a coordinar les ciberdefenses nacionals, i Clinton va emetre la *Presidential Decision Directive –PDD– 63*²⁹⁵ mitjançant la qual s'adoptaren un seguit de mesures, com la creació del càrrec de *Coordinador Nacional de Seguretat, Protecció de la Infraestructura i Contraterrorisme*, que va recaure en Richard Clarke²⁹⁶, o la creació de la *Critical Infrastructure Assurance Office*, CIAO, amb Jeffrey Hunker²⁹⁷ com a director, o el *National Infrastructure Assurance Council*, NIAC, encarregat de coordinar i intercanviar dades sobre vulnerabilitats, ciberatacs i penetracions a sistemes. Paral·lelament, el Departament de Defensa va crear la seva pròpia xarxa de seguretat, la *Joint Task Force-Computers Network Defense*. També el 1998, Clinton va començar a plantejar el tema dels ordinadors davant del canvi del mil·lenni i va fixar el març de 1999 per a què els organismes federals solucionessin el problema. El que es va anomenar *The Millenium Bug* era el problema derivat del fet que la majoria d'ordinadors no podien enregistrar dates de quatre dígits (els anys només duïen les darreres dues xifres) i això va fer témer la paralització o mal funcionament d'empreses, serveis bàsics i hospitals en començar l'any 2000. El cap del NIPC, Michael Vatis, va advertir sobre una eventual presència d'"estrangers infiltrats" entre els tècnics que serien necessaris per a solucionar el *Millenium Bug*, de possibles terroristes cibernètics que podrien introduir virus i codis en els sistemes computacionals, de manera que la infraestructura dels Estats Units podia estar en perill.²⁹⁸

Seguint amb el tema de la prevenció dels atacs cibernètics, pel gener del 1999 Clinton va proposar el pla *Cyber Corps*²⁹⁹, que contemplava iniciatives específiques com ara la

²⁹² Ibid.

²⁹³ *Cybercrime... Cyberterrorism... Cyberwarfare...*, document citat. <http://www.csis.org/pubs/cyberfor.html>

²⁹⁴ A la pàgina principal del National Infrastructure Protection Center, <http://www.nipc.gov/>, s'hi pot trobar la història d'aquest organisme.

²⁹⁵ *Presidential Decision Directive –PDD– 63*, <http://www.fedcirc.gov/library/legislation/presDecDirective63.html>

²⁹⁶ Richard Clarke, http://abcnews.go.com/sections/politics/DailyNews/bush_advisors_clarke.html

²⁹⁷ Jeffrey Hunker, http://abcnews.go.com/sections/tech/DailyNews/terror990203_chaf.html

²⁹⁸ Eric Ginoerio, *Hunting Phantoms*, 31 de juliol 2000 <http://www.landfield.com/isn/mail-archive/2000/Jul/0105.html>

²⁹⁹ <http://www.cis.utulsa.edu/CyberCorps/>. Veure també Janet Kornblum : *Cyber Corps tackles terrorism* <http://www.usatoday.com/tech/news/2001/09/18/cyber-corps.htm>, i també Join the Cyber Corps

creació de xarxes de detecció amb l'objectiu d'alertar el personal adequat davant la invasió d'un sistema computacional crític, la creació de centres d'informació en el sector privat per a treballar conjuntament amb el govern davant les ciberamenaces, i el finançament per a millorar la formació dels especialistes capaços de prevenir i respondre als problemes generats pels ordinadors. El gener del 2000, la CIAO va posar en funcionament el *National Plan for Information Systems Protection* amb l'objectiu de coordinar les diferents agències per abordar les qüestions vinculades amb la infraestructura crítica del govern federal.

Tot aquest discurs sobre les ciberamenaces i el ciberterrorisme, està fonamentat? Són tan vulnerables els sistemes informàtics?³⁰⁰ Barry Collin, investigador de l'*Institute for Security and Intelligence*, va elaborar un seguit d'hipòtesis sobre possibles actes ciberterroristes, que foren i són àmpliament utilitzades pels periodistes, els polítics i els funcionaris dels organismes de seguretat, i que han acabat configurant un determinat imaginari col·lectiu entre la població dels Estats Units sobre les possibles conseqüències d'un atemptat terrorista informàtic. Segons Barry Collin un ciberterrorista podria accedir als sistemes de control de processament d'una planta elaboradora de cereals, canviar els nivells de suplementació de ferro i provocar malalties entre els nens americans; també podria interferir les transaccions financeres de diners i els centres borsaris, amb el que els ciutadans perdrien la confiança en el sistema econòmic. "Gosaria un ciberterrorista intentar ingressar físicament en l'edifici de la Reserva Federal, o un altre de similar? Difícilment, ja que seria immediatament arrestat. És més, un camió gran aparcat prop de l'edifici seria detectat automàticament. Tanmateix, en el cas d'un ciberterrorista, l'individu podria estar assegut en un altre continent mentre que els sistemes econòmics de la nació es col·lapsen, assolint una situació de desestabilització".³⁰¹ També podria atacar el tràfic aeri i fer que dos gran avions civils topessin; maniobres similars podria fer en les línies del ferrocarril; podria alterar les fórmules dels productes farmacèutics o canviar la pressió dels gasoductes i desencadenar un seguit d'explosions i incendis. "De la mateixa manera, la xarxa elèctrica esdevé cada dia més vulnerable".³⁰² En resum, un ciberterrorista podrà fer que la població d'un país no pugui menjar, beure, viatjar ni viure: "Les persones encarregades de vetllar per la seguretat de la Nació no estaran advertides ni podran anul·lar al ciberterrorista, que probablement es trobarà a l'altra

A Proposal for a *Different* Military Service http://www.ideaminer.com/gregconti/publications/cyber_corps.doc

³⁰⁰ Per aquesta introducció al ciberterrorisme, veure Masana, Sebastián (2002), *El ciberterrorismo: ¿una amenaza real para la paz mundial?*. Tesis de maestría. FLACSO – Facultad Latinoamericana de Ciencias Sociales.

<http://www.argentina-ree.com/documentos/ciberterrorismo.pdf>

³⁰¹ Barry C. Collin, *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*

<http://afgen.com/terrorism1.html> i també a <http://buscalegis.ccj.ufsc.br/arquivos/theF.html>

³⁰² Ibid.

banda del món. Lamentablement aquests exemples no són de ciència-ficció. Tots aquests escenaris poden donar-se avui. Com molts saben, alguns d'aquests incidents ja han esdevingut en diverses nacions. Molts d'aquests actes tindran lloc demà.”³⁰³

Un dels principals crítics de les hipòtesis de Collin és l'agent del FBI Mark Pollitt, que va escriure, a finals dels 90, un assaig titulat *Cyberterrorism: Fact or Fantasy?*³⁰⁴, on analitzava les possibilitats reals d'atacs ciberterroristes, i arribava a la conclusió que actualment en la majoria de processos de control encara hi és present l'ésser humà i, per tant, l'abast del terrorisme no és, ni molt menys, el que descriu Collin. Pel que fa a la contaminació dels cereals infantils, Pollit indica que la quantitat de ferro que caldria per a posar malalt algú és tan gran que els operaris de la fàbrica ho notarien: es quedarien sense ferro en la línia de producció i, a més, el producte tindria un gust molt diferent i gens agradable. I això sense tenir en compte que, periòdicament, es fan anàlisis aleatòries. Pel que fa al control del tràfic aeri, Pollit manté que els pilots i els controladors prendrien les mesures adients, ja que són entrenats en el que s'anomena “*situational awareness*”: els pilots són conscients de la seva ubicació, direcció i altitud, descobreixen errors dels controladors i dominen el seu espai de vol. Són els errors humans els que deriven en col·lisions aèries. No afirma que els ordinadors siguin segurs i invulnerables, sinó que, tot i les vulnerabilitats, és quasi impossible que un ciberatac pugui tenir conseqüències devastadores.

William Church, ex-oficial d'intel·ligència de l'exèrcit nordamericà, va fundar el 1996 el *Centre for Infrastructural Warfare Studies (CIWARS)*³⁰⁵ amb l'objectiu de realitzar un informe sobre les vulnerabilitats de la infraestructura dels Estats Units. Aquest informe fou finançat per un grup privat anomenat *The Internet Science Education Project* i fou utilitzat com a referència per la *Presidential Commission On Critical Infrastructure Protection* creada per Bill Clinton. Les seves conclusions són molt properes a les de Pollit. En una entrevista del 1998, a la pregunta de si Bin Laden podria fer servir armes cibernètiques o si, pel contrari, l'impacte visual d'un edifici explotant seguia essent prioritari per a aquest tipus de terrorisme, Church va respondre: “Efectivament, ho acaba d'endevinar. Els grups terroristes amb els que llitem avui són altament proclius a l'impacte visual”.³⁰⁶ Tres anys després tenia lloc l'atac a les Torres Bessones. “Malgrat que el govern dels Estats Units ha citat alguns grups guerrillers de Sri Lanka com els responsables d'haver utilitzat les primeres armes ciberterroristes, això no té

³⁰³ Ibid.

³⁰⁴ Mark M. Pollitt, *Cyberterrorism - Fact or Fancy?* <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>

³⁰⁵ Seu d'iwars.org, <http://www.iwar.org/>

³⁰⁶ John Borland, “Analyzing The Threat of Cyberterrorism”. *TechWEb News*, 25 setembre 1998. <http://www.techweb.com/wire/story/TWB19980923S0016>

sentit. El que varen fer fou un atac per e-mail. Això és assetjament, no és terrorisme”.³⁰⁷ En una altra entrevista concedida a la revista argentina *CompuMagazine*, el febrer de 1998, Church afirmava: “La guerra infraestructural consisteix a fer servir una combinació de mitjans virtuals i físics per tal d’assolir el màxim efecte possible. Però per a això cal una organització i mitjans de magnituds militars, i no un grupet de hackers, com va assegurar fa uns mesos el FBI. (...) Amb 10 hackers professionals es podria aconseguir una acció única, com ara paraitzar les comunicacions durant un parell d’hores, però mantenir aquesta acció com requereix una guerra fa que calgui una organització molt potent que permeti que els atacs siguin continuats de tal manera que arribin a fer caure la infraestructura d’un país.”³⁰⁸

Malgrat aquestes declaracions, Clinton insistia el 1999: “Mentre que fins ara els nostres enemics es recolzaren en bombes i bales, terroristes i potències hostils podrien transformar un ordinador portàtil en una arma potent capaç de fer molt mal”³⁰⁹. En el mateix context, el conseller de la Casa Blanca Richard Clarke afirmava: “Hi ha un gegantí tsunami que està per impactar contra nosaltres... serà millor respondre-hi abans que tingui lloc un Pearl Harbor electrònic”³¹⁰. A l’abril del 2001, durant la presidència de George Bush (fill), el republicà Newt Gingrich, president de la Cambra de Representants dels Estats Units entre 1995 i 1999 va escriure un article titulat *La pregunta no és si hi haurà un ciber Pearl Harbor, sinó quan succeirà*: “La seguretat dels vols aeris estaria seriosament compromesa si els ordinadors que controlen el tràfic aeri fossin dominats per ciberterroristes (...) Una acció d’aquest tipus podria causar nombroses víctimes. Pensem en el cas que es generaria si un grup terrorista dominés els ordinadors de l’aeroport internacional O’Hare (a Chicago) que controlen el congestionat corredor aeri del mig oest. Des de paraitzar els nostres sistemes de comunicacions fins a bloquejar el nostre sistema financer, passant per la generació d’apagades elèctriques, hi ha una gran quantitat d’interrupcions que podrien perjudicar la nostra economia, disminuir la nostra qualitat de vida i desestabilitzar la Nació.”³¹¹ S’ha fet servir tant l’expressió *Pearl Harbor informàtic* que el *Crypt Newsletter*, una publicació virtual sobre seguretat informàtica la defineix de la següent manera: “Electronic Pearl Harbor (EPH): una trivialitat popularitzada per gent de l’estil d’Alvin Toffler, ex generals de la guerra freda, xarlatans empresarials i periodistes, per anomenar-ne uns quants. EPH es fa servir per a designar un nebulós apocalipsi

³⁰⁷ Ibid.

³⁰⁸ Gustavo Aldegani, “Entrevista a William Church”. *Revista CompuMagazine*, nº 115, febrer 1998

³⁰⁹ *Government Monitoring*. *Computer Law*, 13 de setembre de 1999.

http://www.mgrossmanlaw.com/articles/1999/government_monitoring_of_computers.htm

³¹⁰ Ibid.

³¹¹ Newt Gingrich, “A cyber Pearl Harbor is not question of if, but when”. *Infosecurity Magazine*, abril 2001
http://infosecuritymag.techtarget.com/articles/april01/columns_security_persp.shtml

electrònic que plana sobre els ordinadors i les xarxes dels Estats Units. En el món real, és un sinònim de la frase 'Watch your wallet!' (Compte amb la cartera!) perquè els qui la utilitzen generalment ho fan per a convèncer els ciutadans que paguen els seus impostos de finançar projectes ultrasecrets o mal definits que tendeixen a protegir-los."³¹²

Pel gener del 2000, un alt directiu del FBI afirmava: "El subministrament d'energia elèctrica als Estats Units és vulnerable als hackers"³¹³. Un alt executiu del *North American Electric Reliability Council* desmentia l'afirmació del FBI i comentava a la revista *Wired* que no tenia notícies que cap mecanisme de control energètic estigués connectat a mòdems ni a línies telefòniques".³¹⁴ Aquest debat tenia lloc en el moment que l'*Electronic Privacy Information Center* (EPIC), una organització civil dedicada a vetllar per la protecció de la privacitat dels ciutadans, va denunciar públicament que la iniciativa FIDNET (*Federal Intrusion Detection Network*)³¹⁵ elaborada per l'administració Clinton tenia com objectiu encobert vigilar els ciutadans. És fàcil, doncs, demostrar que les prediccions més apocalíptiques dels atacs ciberterroristes emergeixen quan es produeix un enfrontament entre els organismes de seguretat i les organitzacions civils de defensa de la privacitat al voltant de les comunicacions electròniques; la infowar o la softwar esclata, doncs, quan a la societat de la informació s'enfronten la llibertat amb el control.

El primer gran conflicte al voltant de la privacitat a l'era de la informació va tenir lloc durant els anys 80. L'eix va ser el xip Clipper, un petit artefacte criptogràfic destinat a protegir les comunicacions privades però deixant oberta la possibilitat que agents governamentals obtinguessin les claus electròniques per a desxifrar les comunicacions després de la corresponent autorització legal. El 1984, el president Ronald Reagan va decretar la *National Security Decision Directive 145*³¹⁶ que va atorgar a l'agència secreta NSA el control sobre tots els sistemes computacionals governamentals que continguessin informació sensible però desclassificada. Com a resposta, el congrés va aprovar el 1987 la *Computer Security Act*³¹⁷ que limitava el paper de la NSA, però aquesta va aconseguir el 1989 que es creés un grup de treball per a desenvolupar el xip Clipper, destinat a l'encriptació de trucades telefòniques. El 1993, Bill Clinton va

³¹² <http://www.soci.niu.edu/~crypt/other/harbor.htm>

³¹³ Declan McCullagh, "Cyber Safe of Gov't Surveillance?". *Wired*, 1 febrer 2000

<http://www.wired.com/news/politics/0,1283,34027,00.html>

³¹⁴ Ibid.

³¹⁵ *Federal Intrusion Detection Network*, <http://www.cdt.org/security/fidnet/>; veure també

http://www.pigdog.org/auto/Enemy_Action/link/974.html

³¹⁶ National Security Decision Directive Number 145, <http://www.fas.org/irp/offdocs/nsdd145.htm>

³¹⁷ *Computer Security Act*, <http://www.epic.org/crypto/csa/csa.html>

anunciar públicament la iniciativa del xip Clipper: “Durant massa temps, no hi ha hagut pràcticament diàleg entre el nostre sector privat i els organismes de seguretat per a resoldre la tensió entre la vitalitat econòmica i els vertaders desafiaments que implica la protecció dels ciutadans dels Estats Units. (...) En lloc de fer servir la tecnologia per a conciliar els interessos de vegades contraposats del creixement econòmic, la privacitat i la seguretat, les polítiques prèvies han enfrontat al govern amb la indústria i als drets a la privacitat amb els organismes d'intel·ligència”.³¹⁸ Per a conciliar els interessos citats, la iniciativa del xip Clipper va ser proposada com a obligatòria per als organismes governamentals, però optativa per a les empreses i organismes civils. El govern, amb una autorització legal, podia interceptar les comunicacions.

Els debats sobre els límits a la invasió governamental de la privacitat en relació amb els ordinadors s'accentuaren durant el govern de Bill Clinton (1993-2001), degut en part a tres grans fets: l'expansió massiva d'Internet, la democratització del hacking i el *Millenium Bug*. A mitjan 1999, a través de la *Cyberspace Electronic Security Act*³¹⁹, el Departament de Justícia va proposar modificar la legislació de manera que, sota algunes circumstàncies, es postergués per 30 dies l'avís de notificació als sospitosos les cases o llocs de treball dels quals havien de ser violats; es tractava de permetre als agents federals que poguessin entrar als habitatges dels sospitosos per a revisar els seus ordinadors, desxifrar els seus codis d'enciptació i posar “forats” per espiar el seu flux d'informació³²⁰. “El projecte és perillós. Si s'implementés, seria difícil demostrar que les dades utilitzades com a evidència no han estat posades als ordinadors pels mateixos agents federals. Estan proposant alterar arxius d'ordinadors. Això és molt seriós”³²¹ va comentar Barry Steindardt, director associat de l'*American Civil Liberties Union*. Finalment, la iniciativa va ser desestimada. Un cas similar va esclatar quan, el juliol del 2000, es va informar de l'existència d'un sistema de monitoreig de comunicacions a través d'Internet del FBI anomenat *Carnivore*³²². Segons el FBI, Carnivore filtra el tràfic d'informació i envia als investigadors només aquells paquets de dades que legalment poden ser utilitzats³²³.

³¹⁸ Statement by the press secretary, 16 abril 1993,

http://www.epic.org/crypto/clipper/white_house_statement_4_93.html

³¹⁹ Cyberspace Electronic Security Act (CESA), <http://www.cdt.org/crypto/CESA/>

³²⁰ Veure l'article de Declan McCullagh, «Clinton Favors Computer Snooping». *Wired Magazine*, 19 gener 2000 <http://www.wired.com/news/print/0,1294,33779,00.html>

³²¹ Ibid.

³²² Veure Robert Graham, *Carnivore FAQ* <http://www.robertgraham.com/pubs/carnivore-faq.html>

³²³ Es pot consultar la pàgina on EPIC actualitza la informació del cas Carnivore

http://www.epic.org/privacy/carnivore/foia_documents.html i també <http://www.epic.org/privacy/carnivore/>

Pel gener de 1998, un detallat informe³²⁴ del parlament Europeu va revelar l'existència d'una xarxa massiva d'espionatge tecnològic manejada pels Estats Units. Es va comprovar que aquesta xarxa duia a terme rutinàriament el monitoreig de comunicacions telefòniques, faxes i e-mails de ciutadans de tot el món, però particularment de la Unió Europea i del Japó. El *New York Times* va revelar que el sistema nordamericà d'espionatge electrònic era dirigit per la NSA (*National Security Agency*) i duia el nom clau d'Echelon, que consisteix en una àmplia xarxa d'estacions d'espionatge electrònica en la que hi participen cinc països: Estats Units, Anglaterra, Canadà, Austràlia i Nova Zelanda. Aquests països, agrupats sota un acord secret anomenat UKUSA, espion als ciutadans interceptant diàriament les comunicacions electròniques. Els ordinadors de la NSA s'encarreguen després de revisar aquesta informació, cercant determinades paraules clau, a través dels anomenats "diccionaris Echelon"³²⁵. La columna vertebral d'Echelon es troba en els satèl·lits Intelsat i Inmarsat, responsables de la gran majoria de les comunicacions telefòniques entre els països i els continents. Els Estats Units negaren, d'entrada, l'existència d'Echelon, però al final les proves demostraren el contrari³²⁶.

Els atemptats de l'11 de setembre del 2001 varen provocar una mena de dretanització de l'opinió pública nordamericana³²⁷, que va ser aprofitada pel govern de Bush amb un seguit d'iniciatives que tendien a permetre que les investigacions governamentals vinculades al terrorisme poguessin ometre alguns drets civils. Per exemple, el fiscal general dels Estats Units, John Ashcroft, va declarar que ell, unilateralment, havia instituit l'espionatge de les comunicacions entre advocat i client per als sospitosos sense ciutadania nordamericana, violant, directament, les esmenes quarta i sisena de la Constitució que garanteixen el dret a la representació per un advocat.³²⁸ El 13 de setembre del 2001, el Senat va aprovar la Llei per a combatre el terrorisme del 2001, que va ampliar els poders de la policia per a intervenir les comunicacions i va autoritzar el sistema de vigilància *Carnivore* del FBI.³²⁹ Segons la nova llei contra el terrorisme, els fiscals podien autoritzar períodes de vigilància de 48 hores de durada com a màxim sense cap ordre judicial. La vigilància es va limitar al començament a les adreces de les seues web que es visiten i els noms i l'adreça de correu electrònic dels usuaris; tampoc feia falta una ordre judicial per als atacs contra la integritat o el

³²⁴ Es pot llegir l'informe sencer a <http://cryptome.org/stoa-atpc.htm>

³²⁵ CodeName: ECHELON DICTIONARY. Global Electronic Surveillance of EVERYONE. <http://www.ncoic.com/echelon.htm>

³²⁶ Veure el Butlletí de l'EPIC del 30 de maig del 2001, http://www.epic.org/alert/EPIC_Alert_8.10.html

³²⁷ Veure l'article de Carlos Escudé, *Un lugar peligroso* <http://www.geocities.com/smasana/torres1.htm>

³²⁸ Veure l'article de Carlos Escudé, "La crisis de los derechos cívicos en los Estados Unidos". *Diario BAE*, març 2002 <http://www.geocities.com/smasana/bae11.htm>

³²⁹ Declan McCullan, "Aprueban la ley que permite al FBI realizar espionaje en Internet". *Wired* en español, 17 setembre 2001. <http://ar.wired.com/wired/politica/0,1156,22745,00.html>

funcionament de sistemes de computació protegits: la major part de les activitats de hacking hi quedaven, doncs, incloses. La llei antiterrorista sancionada el 26 d'octubre del 2001 amb el nom d'*USA Patriot Act*³³⁰ sumava les potestats del FBI i la CIA: l'espionatge electrònic esdevenia, de fet, legal. Segons l'*Electronic Frontier Foundation*, "les llibertats civils del poble nordamericà varen experimentar un fort cop amb aquesta llei, especialment pel que fa al dret a la privacitat de les nostres activitats i comunicacions en línia. No hi ha cap evidència que les llibertats civils fins ara hagin obstaculitzat la investigació o el judici de grups terroristes".³³¹

Sembla que, de tot plegat, es pugui inferir que estendre entre la població la por al ciberterrorisme és una forma de guanyar suport polític per a la promulgació de lleis que atorguin més flexibilitat als organismes de seguretat per a dur a terme les seves tasques d'espionatge intern; sota el discurs de l'eix del mal ciberterrorista s'hi amaga una clara tendència a envair parcel·les de privacitat, encaminada a tenir més control sobre els ciutadans. Tanmateix, hi ha d'altres factors que ajuden a entendre el per què del sobredimensionament de l'amenaça ciberterrorista: els que més parlen dels possibles escenaris catastròfics són els qui obtenen més beneficis de la por, els executius de les empreses informàtiques de seguretat. Ja el 1997, un informe del *Defense Science Board* va recomanar la immediata inversió de 580 milions de dòlars en el sector privat per a la investigació i desenvolupament del hardware i el software necessari per a lluitar contra el ciberterrorisme. Un dels principals autors d'aquest informe va ser Duane Andrews, vicepresident executiu de SAIC, una empresa proveïdora de serveis de seguretat informàtica que també ofereix serveis de consultoria. Durant el discurs que va pronunciar pel gener de 1999 a l'Acadèmia Nacional de Ciències en relació al pla *Cyber Corps* per a combatre el ciberterrorisme, el president Bill Clinton va dir que li demanaria al Congrés la quantitat de 1.460 milions de dòlars en el proper pressupost federal per a finançar el projecte, cosa que representava un increment del 40 % de les despeses esmerçades en aquesta àrea fins el moment.³³² A l'octubre de 1999, el poder executiu va demanar 8,4 milions de dòlars per a posar en marxa el projecte FIDNET, i es va sol·licitar 50 milions per a la implementació de mesures de seguretat necessàries en totes les dependències governamentals, 17 milions per a la capacitació i entrenament en tecnologies de la informació per al personal del govern federal i 7 milions per a investigació i

³³⁰ *USA Patriot Act*, <http://www.epic.org/privacy/terrorism/hr3162.html>

³³¹ EFF Analysis Of The Provisions Of The USA PATRIOT Act
http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.php

³³² Suzan Revah, "Clinton outlines anti-cyberterrorism plan". *CNET News*, 22 gener 1999. http://news.com.com/2100-1023_3-220532.html

desenvolupament.³³³ El juny del 2000, superada ja la por al *Millenium Bug*, la NSA va anunciar la seva intenció de subcontractar parcialment la seva infraestructura tecnològica a empreses privades amb qui signaria un contracte de 5 mil milions de dòlars. Al mateix dia dels atemptats de l'11 de setembre, el govern Bush va destinar 10 milions de dòlars al finançament de la guerra contra el ciberterrorisme. "Pot ser que els polítics no sàpiguen la diferència entre un byte i un nibble [mig byte = 4 bits], però són experts a gastar diner. I després dels atemptats de l'11 de setembre, els legisladors semblen proclius a signar xecs inusualment grans"³³⁴. Per al pressupost de l'any fiscal 2003, l'administració Bush va demanar la quantitat de 52.000 milions de dòlars per a destinar a l'actualització tecnològica del govern federal.³³⁵ Alguns consideren, fins i tot, que les grans quantitats destinades a la seguretat informàtica pel govern federal podrien contribuir a emascarar casos de corrupció, com el de Compaq del juliol del 2000, però això ja queda lluny del món dels hackers.

³³³ Per veure com es varen repartir aquests milions de dòlars, cfr. Erik Ginorio, "Hunting Phantoms", *The Industry Standard Magazine*, 31 de juliol 2000 <http://www.landfield.com/isn/mail-archive/2000/Jul/0105.html>

³³⁴ Declan McCullagh i Ben Polen, "Fighting Evil Hackers with Bucks". *Wired Magazine*, 11 octubre 2001 <http://www.wired.com/news/conflict/0,2100,47479,00.html>

³³⁵ Per a veure més xifres, consultar Ross Kerber, Waiting for the security payout. *The Boston Globe*, 6 març 2002 <http://www.landfield.com/isn/mail-archive/2002/Jun/0010.html>