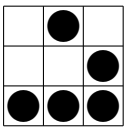
Etica Hacker:
L'imperativo è *hands-on.*

Luca Carettoni (luca.carettoni@ikkisoft.com)
David Laniado (aldivad@logorroici.org)

3 settembre 2005



Indice

1 Introduzione

"Tutto ciò che facciamo, lo facciamo in ultima analisi solo per divertirci"

Così risponde Linus Torvalds[1] spiegando il motivo che lo ha indotto a sviluppare il kernel di Linux. In quella sua piccola stanza, "just for fun" ha creato molto di più di un semplice programma informatico. Ma prima di lui, intere generazioni di persone hanno contribuito a creare e mantenere efficente la tecnologia che utilizziamo quotidianamente. È la storia di intere generazioni.

Piuttosto che voler dare l'ennesima definizione, ritracciare solamente l'ennesima storia alla base dell'etica hacker, vogliamo cercare di lasciare al lettore degli spunti su cui riflettere. Parlare di *hacking* non significa parlare di informatica ma di libertà.

Dopo un breve ed essenziale introduzione storica, riporteremo il manifesto principale dell'etica hacker cercando da questo, in maniera organica, di fornire al lettore degli esempi di reali esperienze, di progetti e situazioni in cui lo spirito hacker è stato la guida.

Questo percorso di valori ci porterà ad affrontare i temi della libertà d'informazione, della cooperazione, dell'amore per il prossimo, della passione come motore principale del lavoro e indubbiamente della grande dedizione ed intelligenza di alcuni personaggi. Per molti sono loro i veri artefici e protagonisti della rivoluzione informatica, proponendo al mondo una visione alternativa dell'informatica, basata su ideali di cooperazione e di condivisione della conoscenza. La loro etica si presenta come una provocazione soprattutto ora che, grazie alla New Economy, i computer e la rete sono diventati parte integrante del nostro modello economico e, per questo, si prestano a diventare importanti strumenti di controllo e di potere. La sfida del movimento hacker è allora quella di diffondere un uso nuovo degli strumenti informatici, permeato da collaborazione e libero accesso all'informazione, per far sì che quello che è stato il prodotto di un lavoro collettivo non possa essere utilizzato a sfavore della libertà degli individui.

Parlando di hacker non è poi possibile fare a meno di accennare tutti gli aspetti etici legati al software libero. La tecnologia dell'informazione digitale contribuisce al progresso mondiale rendendo più facile copiare e modificare le informazioni. I computer promettono di rendere questo più facile per tutti noi. Non tutti vogliono che sia così facile. Il sistema del diritto d'autore dà ai programmi software dei proprietari, molti dei quali mirano a nascondere i potenziali vantaggi del software ad altri. I sostenitori della filosofia del software libero, assimilando questo tipo di opere "soffici" alla scrittura ed alla musica, sostengono che il frutto dell'intelletto di qualche soggetto deve essere disponibile a tutti. La società moderna ha bisogno di libertà.

Prima di iniziare ad affrontare questo percorso vogliamo però dare una breve spiegazione del simbolo riportato in copertina. Questo semplice logo, chiamato *glider*, è un simbolo usato per identificare la cultura hacker. È uno schema che deriva da una simulazione matematica chiamata "Gioco della Vita", basata su semplici regole di comportamento di punti su una griglia; il gioco ha iniziato a

diffondersi contemporaneamente al sistema Unix e a Internet e ha affascinato da subito gli hacker. Nel "Gioco della Vita", semplici regole di cooperazione con l'ambiente circostante portano a situazioni inaspettate e sorprendentemente complesse, che non possono essere previste a partire dalle regole iniziali. C'è un netto parallelismo con il modo in cui fenomeni inaspettati e sorprendenti, come lo sviluppo open-source, emergono dalla comunità hacker.

2 Storie di Hacker

2.1 Il MIT e i primi *hacker*

L'origine della cultura hacker, come oggi la conosciamo, può essere fatta risalire alla fine degli anni '50 al MIT [1]. Il termine "hack" allora era usato nell'università per indicare scherzi spettacolari, innocui e goliardici, che alcuni ingegnosi studenti erano soliti fare. Il campus, ricco di tunnel sotterranei, offriva ampie opportunità esplorative per quegli studenti che non si facevano intimorire da porte chiuse e da cartelli come "Vietato l'ingresso"; fu così che "tunnel hacking" divenne l'accezione usata dagli stessi studenti per indicare queste incursioni sotterranee non autorizzate. In superficie il sistema telefonico del campus offriva analoghe opportunità; grazie ad esperimenti casuali ma accurati, gli studenti impararono a fare scherzi divertenti: questa nuova attività venne presto battezzata "phone hacking". La combinazione tra divertimento creativo ed esplorazioni senza limiti costituirà la base per le future accezioni del termine.

Una delle organizzazioni studentesche del MIT era la Tech Model Railroad Club (Tmrc), che gestiva una sofisticatissima ferrovia in miniatura; all'interno di questo gruppo, gli studenti del comitato *Signals and Power*, ovvero gli addetti alla gestione del sistema del circuito elettrico dei trenini, iniziarono a usare la parola "hack" in una nuova accezione, sintetizzata da Steven Levy [2] in "un progetto intrapreso non soltanto per adempiere a uno scopo specifico ma che portasse con sé il piacere scatenato dalla pura partecipazione". *Hacker* era così, tra loro, chi si dedicava con passione alle attività del gruppo, in un legame quasi morboso con la tecnologia, riuscendo a trovare soluzioni creative e geniali ai problemi.

Quando, nel 1959, venne inaugurato al MIT il primo corso di programmazione per computer, gli studenti del gruppo *Signals and Power* parteciparono con entusiasmo e si avvicinarono per la prima volta alle macchine gelosamente custodite nei laboratori dell'università. Quando fu donato all'ateneo un computer a transistor[2], il lontano antenato dei nostri personal computer divenne subito il loro "giocattolo" preferito. Gli hacker vi si appassionarono e iniziarono a dedicarsi incessantemente allo studio della macchina e al modo di perfezionarla attraverso la scrittura di nuovi programmi. "To hack" non indicava più l'attività di saldare circuiti dalle strane sembianze, bensì quella di comporre insieme vari programmi, con poco rispetto per quei metodi o procedure usati nella scrittura del software "ufficiale". Significava penetrare nelle viscere della macchina per carpirne i segreti. Rimanendo fedele alla sua radice, il termine indicava anche la realizzazione di programmi aventi l'unico scopo di divertire o di intrattenere l'utente.

Un classico esempio è *Spacewar*, il primo video gioco interattivo. Sviluppato nei primi anni '60 dagli hacker del MIT, Spacewar includeva tutte le caratteristiche dell'hacking tradizionale: era divertente e casuale, non serviva ad altro che a fornire una distrazione serale alle decine di hacker che si divertivano a giocarvi. Dal punto di vista del software, però, rappresentava una testimonian-

[1] Massachusetts Institute of Technology

[2] Si trattava di un TX-0, uno dei primi modelli di computer lanciati sul mercato

za incredibile delle innovazioni rese possibili dalle capacità di programmazione. Inoltre era completamente libero (e gratuito). Avendolo realizzato per puro divertimento, gli hacker non vedevano alcun motivo di mettere sotto scorta la loro creazione, che finì per essere ampiamente condivisa con altri programmatori. Verso la fine degli anni '60, Spacewar divenne così il passatempo preferito di quanti lavoravano ai mainframe in ogni parte del mondo.

Nel frattempo, lo spirito collaborativo veniva incentivato da un particolare sistema operativo utilizzato sugli elaboratori: l'ITS (Incompatible Time-sharing System), che fungeva da biblioteca collettiva dei programmi, a cui ogni hacker del Laboratorio di Intelligenza Artificiale poteva accedere. Questo sistema di scambio cooperativo di competenze permise sia la crescita delle abilità degli hacker, sia un avanzamento rapido nei risultati della ricerca sui calcolatori.

Presto la nascita e la crescita di *Arpanet*, la prima rete transcontinentale di computer ad alta velocità, permisero un collegamento tra centinaia di università e laboratori di ricerca. I ricercatori dei vari centri degli Stati Uniti cominciarono a condividere un senso di appartenenza a una comunità e a una cultura comune, provando il bisogno di divulgare ciò che andavano scoprendo per avere in cambio altre informazioni importanti per il loro lavoro. Lo spirito delle prime comunità hacker era fortemente comunitario, basato sulla volontà di cooperazione finalizzata allo sviluppo e sul desiderio di condivisione sia delle risorse che dei risultati.

2.2 L'*Homebrew Computer Club* e il primo personal computer

Negli anni '70 ci fu una nuova generazione di hacker, con epicentro nella *Bay Area* di San Francisco, caratterizzati dall'interesse a diffondere l'uso del computer anche al di fuori del ristretto ambito dei ricercatori, nella convinzione che questo avrebbe potuto portare un miglioramento qualitativo della vita delle persone. Il primo progetto di diffusione e uso sociale dell'informatica si realizzò nel 1969, anno di fondazione della *Community Memory* di Berkeley. Quest'organizzazione, formata da volontari patiti dell'informatica, aveva lo scopo di compilare una banca dati metropolitana e un annuario dei servizi per la popolazione; in questo modo, attraverso terminali posti in luoghi come lavanderie, biblioteche, negozi, etc, era possibile un piccolo scambio di informazioni e di opinioni tra gli abitanti della comunità.

Per migliorare le tecnologie in modo che fosse davvero possibile diffonderle fra la popolazione, nacque l'*Homebrew Computer Club*, un'associazione di ingegneri, ricercatori e tecnici accomunati dal sogno di rendere l'informatica un'abitudine popolare e di costruire un nuovo e rivoluzionario prototipo di computer. Dalla cooperazione dei membri del Club presero vita importanti progetti che, a partire dal 1976, vennero pubblicati su riviste a diffusione nazionale, contribuendo, insieme ad altri gruppi e riviste non istituzionali, a creare un quadro di riferimento e uno spazio di socializzazione per la comunità hacker.

Nel 1976 Steve Wozniak, un membro venticinquenne dell'*Homebrew Computer Club*, costruì il primo personal computer accessibile anche a persone comuni,

l'*Apple I*. Questa invenzione, resa possibile dalla condivisione dei saperi e delle informazioni all'interno del Club, segnò un momento cruciale nella storia degli hacker, poiché realizzò il sogno di avere un mezzo di facile uso e che non contrapponesse barriere tra l'utente e le informazioni. Fino ad allora i computer erano per lo più grosse macchine che dovevano essere tenute in stanze climatizzate e non c'era da parte delle aziende commerciali nessun interesse a progettare qualcosa di diverso e più accessibile.

"Non c'è ragione per cui uno debba volere un computer in casa propria "
Ken Olsen, presidente del consiglio di amministrazione della *Digita Equipment Corporation*, 1977.

Sempre in quel periodo in California si registrò anche probabilmente il primo problema che un hacker ebbe con la legge; si tratta dell'ingegnere John Draper, meglio noto come "Captain Crunch". Secondo la leggenda egli apprese da un cieco che soffiando in un fischietto distribuito in omaggio con una famosa scatola di cereali (*Cap'n Crunch*) vicino alla cornetta, si otteneva come risultato di resettare la centralina telefonica della Ma Bell; inventò così un circuto, il "blue box", in grado di riprodurre la stessa frequenza del fischietto (2600 Herz), grazie al quale era possibile effettuare chiamate senza che venissero addebitate.

Proprio Wozniak, da studente, si era avvicinato a Draper e vendeva le *blue box* nel campus dell'università. Più tardi, Draper rivelò che praticando il "Boxing" nei dormitori di Berkeley era capitato tra l'altro che Wozniak facesse una incredibile telefonata in Vaticano, facendosi passare per il Segretario di Stato Henry Kissinger; per poco non era riuscito a parlare con il Papa.

2.3 Richard Stallman e la *Free Software Foundation*

Gli anni '80 segnarono una fase di riflusso per la cultura hacker. Molti di loro iniziarono a lavorare per le aziende, accettando i compromessi che una tale scelta comportava. Le nuove leve di programmatori erano cresciute in modo solitario, non avevano quel senso di appartenenza ad una comunità che aveva animato i primi hacker, e non sentivano la necessità della condivisione delle tecniche e della libertà di circolazione delle informazioni. Le leggi del mercato prevalsero e le aziende di software proprietario si imposero. Anche il Laboratorio di Intelligenza Artificiale del MIT, a causa di minacce di tagli dei finanziamenti, si dovette adeguare alle nuove regole ponendo dei limiti al libero collegamento ai computer del Laboratorio. "Gli hacker che non accettavano quel fatto erano destinati a lavorare nella solitudine (anche se beata), oppure a rimanere confinati in strette comunità finanziate dall'Arpa" [2].

Uno dei "nostalgici" che scelsero la solitudine fu Richard Stallman, che Steven Levy elogiò come "l'ultimo vero hacker"; descrizione che, con le parole di E. S. Raymond "si rivelò fortunatamente errata" [3].

" Avrei potuto guadagnare, e forse mi sarei divertito a programmare. Ma sapevo che al termine della mia carriera mi sarei voltato a guardare indietro, avrei visto anni spesi a costruire muri per dividere le persone, e avrei compreso di aver contribuito a rendere il mondo peggiore"
Richard Stallman [4]

Il sistema operativo che si era nel tempo affermato era Unix, inventato da *Ken Thompson*, un hacker del laboratorio Bell, nel New Jersey; grazie anche all'invenzione del linguaggio C, ad opera di un altro hacker del Laboratorio, *Dennis Ritchie*, Unix poteva presentare la stessa interfaccia e le stesse funzionalità su macchine di diverso tipo e poteva fungere da ambiente software comune per tutte. "Gli hacker erano così in grado di utilizzare gli stessi strumenti software da una macchina all'altra, piuttosto che dover reinventare l'equivalente di fuoco e ruota ogni volta" [3].

Il sistema operativo Unix era però commerciale e protetto da copyright e non permetteva la libera circolazione di informazioni che aveva caratterizzato ITS; così Stallman decise intraprendere il grandioso progetto di realizzare una sorta di clone di Unix, scritto in C, con l'intento di "creare un sistema operativo libero, con cui avremmo potuto avere nuovamente una comunità in cui hacker possono cooperare, e invitare chiunque a unirsi al gruppo". Il nome che Stallman scelse per il nuovo sistema operativo fu GNU, acronimo di "Gnu's Not Unix", definizione ricorsiva in tipico linguaggio hacker.

Uno dei primi programmi per GNU scritti da Stallman fu *Emacs*, un programma di editing il cui sviluppo lo impegnò per un anno. Il software era distribuito gratuitamente, ma richiedeva un comportamento cooperativo da parte degli utilizzatori: in caso di distribuzione le modifiche apportate dovevano essere rese disponibili. Il programma si diffuse rapidamente attraverso la rete Arpanet e l'interesse per il progetto GNU crebbe. Così nel 1985 Stallman fondò la *Free Software Foundation* [5], un'organizzazione no profit basata su contributi volontari in lavoro e in denaro. La Fsf è diventata negli anni un punto di riferimento per i numerosi programmatori che condividono lo spirito comunitario di Stallman e per coloro che sono interessati alla qualità del prodotto e alla protezione dei diritti del software libero.

Limitarsi a distribuire liberamente il software prodotto ne avrebbe permesso una facile circolazione, ma avrebbe anche lasciato la possibilità alle case di software commerciale di utilizzarne delle varianti come software proprietario, spezzando la catena del lavoro e dell'uso cooperativo e vanificando l'impegno per la libertà del software. Così è nata la GNU *General Public Licence* [6], chiamata anche "permesso d'autore", o con un gioco di parole *copyleft*, in contrapposizione al *copyright*: una licenza solida e accurata in grado di proteggere e dare fondamento giuridico al mercato del software libero, proprio sfruttando le leggi relative al diritto d'autore. Il software rilasciato sotto questa licenza può essere modificato e distribuito a piacimento, gratuitamente o a pagamento, alle condizioni di distribuirlo in formato sorgente e di indurre chiunque lo acquisisca ad aderire allo stesso tipo di contratto.

2.4 La nascita di Linux

La FSF realizzò in pochi anni una grande quantità di programmi liberi; nel 1990 il sistema operativo era quasi completo ma mancava la parte più importante: il *kernel* ("nucleo"), ovvero l'insieme dei programmi di basso livello che consentono la gestione delle risorse del computer. E' qui che entra in gioco la storia del

giovane studente finlandese Linus Torvalds.

Non potendosi permettere l'acquisto di un sistema operativo Unix, nel 1990 Linus decise di scrivere un sistema operativo alternativo, simile a Unix, per il proprio computer. Dopo un anno di lavoro il nucleo del nuovo sistema operativo soddisfaceva già le funzionalità di base; il suo creatore lo chiamò "Linux" e decise di diffonderlo su internet affinchè circolasse liberamente, chiedendo in cambio agli utilizzatori soltanto collaborazione per migliorlo ed espanderlo.

Attorno a Linus si creò così attraverso la rete una comunità di giovani programmatori di tutto il mondo che con lavoro volontario e ben coordinato svilupparono in meno di tre anni un sistema operativo di grande qualità. Linus decise di aderire alla GNU GPL e il progetto fu fatto rientrare nel progetto GNU: GNU/Linux era così un sistema operativo completo, in grado di competere con le migliori versioni commerciali di Unix.

A studiare il caso di Linux come innovazione tecnica e sociologica al tempo stesso fu Eric Steven Raymond nel suo saggio di grande successo "La cattedrale e il bazar" [7]; così riassume Raymond il processo che permise lo sviluppo di Linux: "La qualità fu mantenuta non da rigidi standard o autocrazia, ma dalla strategia semplice e naive di proporre settimanalmente delle idee e di ricevere opinioni in merito da centinaia di utenti ogni giorno, creando una sorta di rapida selezione darwiniana sulle modifiche introdotte dagli sviluppatori. Con stupore da parte di quasi tutti, il progetto funzionava piuttosto bene." [3]

3 Storia degli Spaghetti Hacker

Mentre è semplice trovare informazioni riguardo a storie, progetti ed esperienze hacker riferite all'altra parte dell'oceano, è sicuramente meno semplice cercare di tracciare una cronologia degli avvenimenti qui in Italia. Quello che è possibile fare, è cercare di capire in quale contesto sono cresciuti quelli che definiremo *Spaghetti Hacker*, quali caratteristiche avevano (ed hanno!) e in che modo hanno affrontato la crescità dell'informatica all'interno della società italiana.

Perchè parlare di spaghetti hacker? In primo luogo perchè sicuramente il loro modo di pensare è avvicinabile come valori alla cultura hacker anche se con modalità diverse. L'aggettivo spaghetti, ricordando quella che è in fondo una "caratteristica nazionale", mette però l'accento sul fatto che in Italia l'evoluzione di questa cultura è stata assolutamente diversa ed almeno per i primi tempi indipendente da quella americana. E' difficile ammetterlo, ma gli hacker nostrani hanno vissuto una cultura diversa perchè le condizioni tecnologiche in termini di infrastutture e di risorse nelle università e negli uffici sono sempre state scarse rispetto al contesto americano; a causa di questa condizione gli spaghetti hacker sono sempre stati tecnicamente meno capaci dei colleghi americani perchè spesso, almeno sino all'avvento delle vere reti di telecomunicazioni, non avevano la possibilità fisica di "mettere sù le mani" su attrezzature e manuali tecnici che potevano dar a loro la conoscenza di cui avevano bisogno.

Oggi si sente spesso parlare di "smanettone"; uno spaghetti hacker è molto di più di un semplice soggetto interessato alla tecnologia e che la padroneggia senza problemi. Uno spaghetti hacker è forse uno "smanettone" che mette al centro del suo lavoro e delle notti passate a scrivere codice o a studiare un sistema, un'etica di libertà delle informazioni. Tra mille vicende giudiziare ed centinaia di *script-kiddies* che cercavano di simulare gesti eroici, ci sono state delle esperienze reali guidate da quello spirito puro che è stato formalizzato nell'etica hacker anche se, come detto, la "via" italiana è stata decisamente meno intensa e più di emulazione verso i veri eroi della rivoluzione informatica. Come affermato da Stefano Chiccarelli e Andrea Monti [8]: "Forse, quando si smetterà di guardare i computer con la lente deformata dell'ignoranza e del sensazionalismo, si potrà cominciare a riflettere nitidamente sulle nuove generazioni di smanettoni italiani...i veri spaghetti hacker".

3.1 Console-mania

Per capire a fondo come questa cultura abbia attirato un innumerevole quantità di persone anche nel nostro paese, dobbiamo tornare indietro sino al 1982 quando apparvero sul mercato i primi veri elaboratori, che paragonati alla macchine di oggi sembrano oggetti primitivi, ma che allora erano la prima vera risorsa informatica ad ampia diffusione. Qualsiasi persona con un *Commodore 64* oppure un *ZX Spectrum*, a seconda della scuola di pensiero, poteva eseguire programmi; i più smaliziati potevano addirittura modificarli o crearne di nuovi avendo a disposizione degli strumenti molto potenti quali il *BASIC* e *l'ASSEMBLY*, a patto di essere abbastanza abili da riuscire a far stare nelle poche decine di KB disponibili in memoria tutte le istruzioni che avrebbero dato vita alla "nuova

creatura". E' in questi anni che gli spaghetti hacker abbandonano il flipper per dedicarsi al nuovo dispositivo, trovando nei primi microcomputer il compagno ideale per intere nottate di gioco. Enormi folle di ragazzini iniziano a riversarsi nei primi negozi di computer per espandere la ram o per avere l'ultimo gioco disponibile. Ed è proprio grazie all'estrema diffusione dei videogame che si formano due diverse tipologie di utenti: quelli che sono unicamente interessati all'aspetto ludico e quelli che invece sono decisamente più interessati a capire il funzionamento del gioco e spesso le modalità di protezione dello stesso.

Passa qualche anno, nuove macchine vengono introdotte sul mercato, ed iniziano ad essere disponibili i primi veri esperimenti di reti di telecomunicazione. In questo contesto, il fedele rapporto tra il venditore di computer ed il ragazzino smaliziato si fa sempre più intenso sino al punto che i due soggetti si scambiano favori. Molti dei software analizzati e sprotetti vengono rivenduti nei negozi. Poichè eliminare o *bypassare* la protezione di un software non è certamente un'operazione accessibile a tutti poichè richiede una buona conoscenza del linguaggio macchina, spesso il software arrivava *cracckato* dall'estero ed i nostri connazionali si divertivano a modificare gli *splash screen*, ovvero le schermate di inizio del videogame mostrando la loro abilità nel gestire le librerie grafiche allora disponibili.

3.2 Connessi alla rete

Nel 1985, giunti anche in Italia i primi modem a 300 baud che venivano per lo più autocostruiti, lo "sport" nazionale diventa quello di effettuare delle scorribande lungo quella rete assolutamente primitiva che non ha nulla a che vedere con l'Internet di oggi. Sono i tempi di *QSD*, una messaggeria francese su Minitel, a cui molti smanettoni italiani si collegavano per conoscere i "veri" hacker o per conoscere semplicemente delle ragazze come avviene tutt'ora tramite gli applicativi di instant-messaging. Raul Chiesa aka Nobody ricorda, con la stringa di risposta alla connessione, quello che qualche anno dopo era il suo modo di passare le serata, digitando alcuni comandi e scrivendo messaggi per interminabili ore e lunghe nottate.

```
>> SET HOST /X
>> Address: 0208057040540
ACP: CALL CONNECTED

Q S D
Software SICOMM France
**********************
You Are on QSD (France)
International Chat System
Free Access
**********************
For fun and friends!
No pirating nor hacking Please!
```

Per una persona normale collegarsi ad un servizio di messaggistica era poco più che vedere delle scritte sbiadite su di un monitor bicromatico, ma per uno

"smanettone" queste lettere significavano comunità e libertà. Nel 1983 esce, anche in italia, il film Wargames[9] e quei pochi ragazzi colpiti da dubbi sull'utilità delle lunghe ore passate davanti al computer, intravedono un nuovo scopo e soprattutto una nuova sfida da affrontare. Nel 1986 arriva anche il servizio *VideoTel* con cui l'allora SIP pensava di creare la prima vera rete telematica anche in Italia. L'alto costo dei terminali e la scarsa disponibilità di servizi in realtà non farà mai raggiungere gli scopi previsti, ma per gli smanettoni è stato il primo vero fenomeno completamente italiano: iniziano a scambiarsi le password per l'accesso, creano le prime pagine di consultazione e le prime chat, senza rendersi conto di essere i primi "esploratori" di questo nuovo mondo.

Già in questa fase di apertura verso il mondo, anche in Italia, si adotta una precisa scelta etica che denota come non era, almeno per molti, un semplice stare davanti ad un terminale. In quel tempo, il pagamento per la connessione veniva addebitata al soggetto che si era connesso, utilizzando come identificazione l'ID e la PASSWORD che erano state immesse durante la fase di login, che precedeva la vera e propria connessione. Sebbene nelle chat "girassero" anche password associate a semplici utenti privati, c'era un'attenzione comune nell'usare unicamente account appartenenti a grosse società o enti pubblici in maniera da non addebitare ulteriori costi all'ignaro cittadino. Questi momenti sono ricordati da molti come gli istanti in cui il singolo cittadino scopre di avere un certo potere in questo nuovo mondo dove l'informazione diventa il bene più prezioso. Azioni attuate nel mondo virtuale hanno una reale influenza nel mondo reale. Alcuni di questi "esploratori" raccontano che la sensazione è paragonabile a quella vissuta da Davide mentre sconfigge Golia.

Con l'avvento delle nuove reti di telecomunicazione, anche qualche smanettone inizia a sentire il desiderio di fare *hacking* nel senso puro del termine ed a questa attività se ne affiancano altre correlate quali il *social engineering* ed il *phone phreaking*. La prima è l'arte e la scienza di guidare l'interlocutore ad assecondare i propri desideri; è basata sulla la capacità di raccogliere da una persona le informazioni di cui si ha bisogno operando su due piani distinti: il livello fisico e il livello psicologico. La componente fisica riguarda tutte le persone e i luoghi, reali o virtuali, da cui si possono raccogliere le informazioni. La sede dell'obiettivo, le società con cui collabora, gli uffici, i terminali incustoditi. Ma anche gli archivi online, i newsgroup, i dipendenti raggiungibili tramite telefono o e-mail. Infine, perchè no, il cestino della spazzatura (ed in questo caso parliamo di *trashing*). L'aspetto psicologico invece sfrutta la debolezza e l'insicurezza delle persone, oltre al lato del comportamento umano che tende a far diventare le persone molto cordiali e disponibili durante il lavoro. Quando parliamo di *phone phreaking* invece ci riferiamo a tutte quelle tecniche che sfruttano la rete telefonica per poterne capire meglio il funzionamento e per evitare di pagare cifre esorbitanti, in maniera da poter essere sempre collegati.

In Italia si inizia a parlare solo intorno all'85 di questa tecnica, che è ben più antica, come è stato raccontato nel capitolo precedente legato alla storia americana. Anche in questo caso, le vicende italiane sono state diverse a causa dell'arretratezza tecnologica delle nostre centrali telefoniche che non permettevano di esportare tutti i trucchi che invece in negli Stati Uniti erano diffusissimi. Da noi si assisteva per lo più ad alcuni "escamotage" utilizzati per non paga-

re le telefonate dalle cabine telefoniche e nei casi più evoluti sino all'uso delle cosidette *blue box*. Una *blue box* è in pratica un dispositivo elettronico, spesso sostituito da software che comanda i chip *DSP*[3] e che permetteva di generare diverse tonalità ad una precisa frequenza. Il *phreaker* telefonava ad un numero verde; la centrale telefonica registrava che aveva chiamato un *green* e non iniziava nessun addebbito per la chiamata. Il telefono squillava. A questo punto il *phreaker* emetteva, tramite la *blue box*, il tono ad una determinata frequenza (in italia 2040/2400 Hz) nella cornetta. L'estremità del canale a cui faceva capo il *green*, pensava che l'utente avesse deciso di attaccare e si sconnetteva mentre l'estremità su cui si trovava il *phreaker* continuava a pensare che il tizio stesse telefonando al green. Il *phreaker* ora aveva il canale a sua disposizione e poteva, tramite l'uso di altri toni (i famosi kp & co.) indirizzare la chiamata su un numero a piacere.

3.3 *Italian Crackdown*

Con l'arrivo delle *BBS*, nel 1988, si iniziano a creare delle vere e proprie aggregazioni di utenti, intorno alle storiche *MC-Link*, *Agorà* e *Galactica*. Ed è qui, a nostro avviso, che si iniziano a "sporcare la acque": in questo periodo c'erano molti utenti che vedevano queste nuove comunità online come un reale strumento di comunicazione per poter accedere ad informazioni che altrimenti non sarebbero state raggiungibili, ma anche molti altri utenti (che oggi chiameremo "script-kiddies", "cracker" o "warez courier") il cui unico scopo era quello di utilizzare questi nuovi strumenti come canale di comunicazione per "piratare" il software, dimostrare la propria superiorità penetrando nei sistemi o creare danni, per il solo piacere di farlo. L'abuso del termine hacker, in Italia, nasce da qui e da queste due scuole di pensiero: un gruppo interessato ai soli fini materialistici ed uno, invece, profondamente motivato, che vuole conoscere come funzionano le cose "mettendoci su le mani" e vuole l'informazione libera.

I più estremi sostenitori della controcultura hacker sentono la necessità di creare un loro spazio per poter parlare di vera etica hacker ed in generale di cultura cyperpunk. Nasce così il canale telematico *Cyberpunk.ita*, il cui motto sarà "INFORMATION WANTS TO BE FREE", e la cui azione di propaganda all'interno del movimento risulterà importante per consolidare l'etica degli spaghetti hacker. Poichè l'Italia non ha sviluppato un movimento culturale diffuso ed eterogeneo che coprisse tutti gli aspetti tecnici oltre alla nuova visione del mondo, che passava attraverso l'analisi del rapporto uomo-macchina, spesso i nostri smanettoni prendono in prestito da alcuni autori storici del genere letterario cyperpunk idee e stili di vita. Non possiamo non citare "Neuromancer" di Willian Gibson[10], "The Hacker Crackdown" di Bruce Sterling[11] e "Mind-Players" di Pat Cadigan[12].

La Rete non aveva ancora una vera identità quando, nel 1994, una vastissima operazione di polizia denominata "Hardware1" darà inizio ad un brutto periodo per la scena hacker italiana. Il periodo buio, chiamato "Italian Crackdown", per la triste analogia alle vicende dell' "Hacker Crackdown" americano, si apre

[3]Digital Signal Processing chip.

con una serie di perquisizioni a tappeto in alcuni delle sedi delle BBS storiche. Ma non fu una normale operazione di polizia visto che le sedi delle BBS non erano altro che le camere di quei sysadmin che, per passione, dedicavano il loro tempo a mantenere tali nodi. Gli ufficiali della polizia giudiziaria sequestravano di tutto in maniera assolutamente insensata e senza la minima consapevolezza degli strumenti che stavano prelevando; si raccontano storie di operazioni che hanno portato a sequestri di tastiere, tappetini per mouse e, a volte, addirittura il sigillo della stanza stessa. Il reato contestato era quello della detenzione di software illegale: dopo una fase di indagine, la polizia aveva individuato una serie di nodi strategici per lo scambio di software pirata, di numeri di carte di credito e software per fare *boxing*. Spesso però nelle BBS gli scambi avvenivano soltanto e di fianco alle persone che lucravano su questi fatti, c'era una schiera di *sysop* che non era nemmeno cosciente di quello che era successo all'interno del loro nodo.

Nelle ore e nei giorni successivi ai primi sequestri, per la rete Fidonet si assistette ad un fermento generale, attraverso l'invio di messaggi di richieste di aiuto, di sfogo, di consiglio e spesso di delucidazione su quanto accaduto. Anche in questo caso, la risposta organizzata ai fatti e alle accuse degli organi di stampa verso l'intera comunità hacker italiana, arrivò da una comunità: Peacelink, una rete di pacifisti che usavano (e usano) internet per coordinare le loro azioni di mediaattivismo e per promuovere l'informazione indipendente [13]. Peacelink cercò di organizzare una serie di incontri con esperti del settore e con avvocati, per capire quanto era accaduto e per fare dell'anti-propaganda, cercando di pulire il nome di tutti quelli che in quegli anni interagivano con il sistema per pura passione e senza la minima intenzione di dolo.

L'"Italian Crackdown" si conclude senza un nulla di fatto, con una serie di processi in prescrizione e qualche patteggiamento, ma l'opinione pubblica era minata, e il riflesso si sarebbe fatto sentire negli anni a venire. Sicuramente gli avvenimenti avevano portato alla luce una situazione che di fatto esisteva: il mondo digitale era diventato parte integrante della vita delle persone ed era utilizzato da alcuni come canale per effettuare azioni illegali. Grazie a tutto questo la gente aveva (e forse ha?!?) problemi a capire la vera differenza tra *sysop* onesti e semplici *courier* che spostavano software da un posto all'altro, tra gente appassionata a capire il funzionamento delle cose e gente interessata solamente a telefonare gratis ed ancora, tra fautori della "full disclosure"[4] e quelli che "hackavano" un sistema solo per potersi vantare.

Ma oltre alla disfatta italiana questo è anche il periodo di *Linux*, del software libero e del preludio dell'introduzione di Internet. Con il lancio di "ItaliaOnLine" e "VideoOnLine", si può iniziare a parlare della diffusione di Internet come rete accessibile a basso costo e con un numero di servizi sempre in crescità. In breve tempo, siti, servizi email ed ftp diventano il paradiso di questa nuova generazione di smanettoni, a cui forse un po' apparteniamo anche noi. In questo vorticoso boom di tecnologia molti ragazzini, che avevano "giocato" con *Linux* qualche volta, diventano improvvisati *sysadmin* di importanti nodi della rete a

[4] la pratica del rivelare le vulnerabilità di software e dispositivi in maniera pubblica, all'interno di mailing-list e forum dedicati alla sicurezza

causa della pressochè inesistente figura di *sysadmin* professionista. Ora, la Rete e la possibilità di avere tra le mani macchine potenti poichè pagate da queste nuove società di telecomunicazione, fornisce a questi smanettoni la possibilità di imparare ed accrescere la loro cultura tecnica in maniera impensabile qualche anno prima. L'infrastruttura "bacata" del sistema Internet italiano rappresenta l'ambiente perfetto per sperimentare e capire il funzionamento della tecnologia. E se è vero che l'aumento di interesse da parte dei mass-media ha contribuito, spesso, a rafforzare la concezione sbagliata dell'hacker come pirata informatico, è anche vero che ha permesso a molti giovani di poter conoscere un mondo interessante e altrimenti difficilmente avvicinabile come quello di Internet.

3.4 L'*HackMeeting*

Per concludere, vogliamo riportare quello che a nostro parere è un momento che incorpora il vero spirito degli spaghetti hacker e che rappresenta la manifestazione più evidente di tali valori: l'*HackMeeting*.

È a partire dal 1998, che gli hacker italiani hanno iniziato ad organizzare raduni a livello nazionale; da allora gli hackmeeting si svolgono in luoghi autonomamente gestiti e si compongono di seminari, di dibattiti, di scambi di idee, di apprendimento collettivo, ma anche di giochi e di feste. Ciò che differenzia questi incontri da quelli americani è l'assenza di sponsor e di aziende, dal momento che tutta l'organizzazione è autogestita e coordinata da un collettivo virtuale che lavora durante tutto l'anno. Il cuore di questi meeting è il "lan-space", uno spazio dove è possibile collegare il proprio computer alla Rete per sperimentare, giocare e condividere gratuitamente i propri materiali e le proprie conoscenze con gli altri partecipanti.

Il manifesto del movimento hacker italiano recita così:

"...Esprimiamo una visione dell'hacking come attitudine, non esclusivamente informatica. Il nostro essere hacker si mostra nella quotidianità anche quando non usiamo i computer. Si mostra quando ci battiamo per far cambiare quanto non ci piace, come l'informazione falsa e preconfezionata, come l'utilizzo delle tecnologie per offendere la dignità e la libertà, come la mercificazione e le restrizioni imposte alla condivisione delle conoscenze e dei saperi. Siamo sinceramente spaventati dalla velocità con la quale la tecnologia viene legata a doppio filo al controllo sociale, alle imprese belliche, a una malsana e schizofrenica paura del proprio simile: il nostro approccio è diametralmente opposto" [14]

L'ideale hacker italiano, oggi, è perciò influenzato da un atteggiamento contestatario e politicizzato, che porta a organizzare cortei telematici e *netstrike* di protesta, oltre alla caratteristica attrazione verso i computer e all'amore per la scoperta di ciò che la macchina cela. I frequentatori degli hackmeeting italiani sono informatici alternativi, che hanno dai venti ai trent'anni circa, perlopiù professionisti che si occupano della sicurezza on line di importanti società.

Da questo punto in poi, difficilmente possiamo parlare di storia visto che

gli avvenimenti sono quasi contemporanei. A nostro avviso, anche in Italia, in questi anni si sta riuscendo a far comprendere meglio alla gente la vera essenza del termine spaghetti hacker, dei pregi del software libero e della reale necessità di porre attenzione agli aspetti legati alla sicurezza e alla privacy dei sistemi informatici. Molto è stato fatto, ma altrettanto è da fare.

4 L'etica Hacker

Abbiamo visto, nella storia americana e in quella italiana, come a fronte delle padronanze tecniche si andavano formando anche gli elementi di una cultura che cominciava ad accumulare esperienze e leggende. In nessun momento della storia di questa cultura i concetti alla base dell'etica sono stati discussi formalmente ma vengono piuttosto accettati tacitamente da tutti coloro che davanti a delle macchine che eseguono dei programmi, rimangono a bocca aperta. Non ci sono manifesti ufficiali o regolamenti: una persona nasce hacker.

"Gli hacker possono fare qualsiasi cosa e rimangono hacker.
Puoi essere un falegname Hacker... "
- Burrell Smith -

Si sente spesso parlare di hacker e non si capisce perchè questo termine venga usato con significati così diversi. Richard Stallman fu definito come "l'ultimo dei veri hacker" e data la sua notorietà, almeno nell'ambiente informatico, siamo convinti che sia l'esempio più lampante di quanto essere un hacker non significhi essere un criminale. Stallman si occupa di *free software*, di quel software che oltre ad essere gratis è soprattutto disponibile tramite codice sorgente in maniera libera e può essere modificato e ridistribuito. Quello del *free software* è un'ideale puro, con aspetti quasi evangelici che non ha nulla a che vedere con attività criminali, la penetrazione in sistemi protetti o la scrittura di virus.

Ma che cosa distingue un hacker etico e perchè il termine viene così abusato? Essere hacker non dipende, in prima approssimazione, dalle sole capacità tecniche ma dal modo con cui si affrontano i problemi. Comportarsi da hacker significa non poter evitare di "mettere le mani" sul computer, e non accettare che faccia cose diverse da quelle che servono; e quando (come purtroppo succede spesso) un software fa i capricci, o si comporta in modo diverso da come si vorrebbe, in un'hacker parte un impulso basato su un fermo principio filosofico: la macchina deve lavorare per me, e non viceversa. Ne nascono talvolta battaglie impegnative, ma alla fine le cose devono andare come si vuole che vadano. In questa fase servono assolutamente le capacità tecniche, ma la componente fondamentale è lo spirito. Sistemi, protocolli, procedure di comunicazione in rete, eccetera, devono adattarsi alle esigenze delle persone; non noi alle fisime di qualche progettista o di qualche prepotente software house.

Come abbiamo visto anche nella storia italiana, esiste un grosso problema: utilizzando queste tecnologie il confine tra "bravo tecnico" e "pirata informatico" è sottile. Anche alcuni veri hacker ha compiuto azioni illegali ma il loro scopo non era quello di nuocere o creare danno ma solamente scoprire vulnerabilità, capirne il funzionamento e dimostrarsi abili e senza barriere. Gli hacker sono degli inguaribili curiosi, con una tendenza ad andare oltre la superficie delle cose, a cercare notizie e informazioni diverse da quelle più diffuse. Ma questa caratteristica li porta spesso ad uscire dal confine tra legalità ed illegalità delle azioni, confondendo la percezione delle persone davanti ad avvenimenti che riguardano la rete o il mondo dell'informatica in generale.

Danneggiare un sistema per puro divertimento, rubare informazioni da rivendere, scaricare software piratato non sono occupazioni per queste persone che hanno una precisa morale. Se però il sistema vuole aggredire il loro mondo, limitare la loro libertà in rete attraverso censure e filtri, allora qualsiasi azione diventa giustificata.

Nel tempo sono stati scritti parecchi documenti non ufficiali che cercano di dare una definizione, quanto meno schematica, di cosa significa essere hacker. "How To Become A Hacker" di Eric Steven Raymond[15] evidenzia bene come:

"Un hacker costruisce le cose mentre un cracker le rompe e basta."

Successivamente nel suo documento, Raymond cerca di dare enfasi a come il mondo sia pieno di cose stupende da scoprire e di problemi da risolvere. Non vale quindi la pena di risolvere lo stesso problema più volte; conoscere la soluzione data dai nostri predecessori basterebbe ma per fare questo abbiamo bisogno di informazioni: la società moderna ha un oggettivo bisogno della libertà dell'informazione.

Parlando poi della figura dell'hacker, Raymond spiega come questi soggetti non riescano a fare per lungo tempo lavori ripetivi che non stimolino la creatività e la logica che rappresenta la linfa vitale del loro modo di pensare il mondo. L'attitudine non può però essere un sostituto della competenza. Ogni hacker ha particolari competenze in qualche campo, e padroneggia qualche argomento in maniera da poter essere utile all'interna comunità hacker. Questa necessità di autoriconoscimento unito alla reale voglia di "giocare" con le cose li porta a realizzare una pura società "del dono" in cui ogni componente collabora per la crescita di un'ideale globale, sviluppando nuovo software, scrivendo documentazione o anche semplicemente seguendo attivamente qualche progetto. Tramite la Rete, l'individuo sperimenta la condivisione di risorse e di opportunità, può soddisfare i suoi desideri personali e può cooperare, allo stesso tempo, alla produzione di un bene collettivo. Per queste ragioni, la diffusione della logica del software libero e dell'open source in generale, sembrano essere presupposti importanti verso la riduzione del gap tecnologico, perchè consentono di adeguare le tecnologie alle necessità locali e culturali e perchè si pongono come stimolo alla crescita e all'innovazione.

Dopo aver cercato di dare un'inquadratura generale dell'etica, partendo dall'analisi dell'hacker stesso, vogliamo però tentare di riassumere gli aspetti chiave[2] che guidano il lavoro di queste persone attraverso alcuni punti fondamentali, che sono stati definiti negli anni:

- L'ACCESSO AI COMPUTER - E A TUTTO CIO' CHE POTREBBE INSEGNARE QUALCOSA SU COME FUNZIONA IL MONDO - DEV'ESSERE ASSOLUTAMENTE ILLIMITATO E COMPLETO. DARE PRECEDENZA ALL'IMPERATIVO DI METTERCI SU LE MANI !
  Gli hacker credono nella possibilità di imparare smontando le cose, mettendoci su le mani e osservando come funzionano. E' un invito a buttarsi in primo piano per creare cose nuove e ancora più interessanti. Tutto ciò

che è guasto o necessita di miglioramenti deve essere modificato e nessuna persona, barriera fisica o legge deve impedirglelo.

- TUTTA L' INFORMAZIONE DEVE ESSERE LIBERA.
  Un libero scambio di informazioni promuove una maggiore creatività complessiva.Dal punto di vista hacker, qualsiasi sistema trae beneficio da un libero flusso d'informazioni. Se una persona ha già creato un programma perchè altre trenta persone devono perdere tempo a fare la stessa versione dello stesso programma? Conviene che queste trenta, conoscendolo già, lo rendano più completo e funzionale per metterlo al servizio di tutti. L'informazione è vitale per una società libera.

- DUBITARE DELL' AUTORITA'.PROMUOVERE IL DECENTRAMENTO.
  Il modo migliore per promuovere il libero scambio di informazioni è avere sistemi aperti. L'ultima cosa di cui c'e' bisogno è la burocrazia; di qualunque tipo essa sia è pericolosa perchè inconciliabile con lo spirito di ricerca dei veri hacker. La burocrazia si nasconde dietro regole arbitrarie, norme istituite solo per implementare il potere di qualche autorità facendo aumentare di conseguenza costi e tempi.

- GLI HACKER DOVRANNO ESSERE GIUDICATI PER IL LORO OPERATO, E NON SULLA BASE DI FALSI CRITERI QUALI CETO, RAZZA O POSIZIONE SOCIALE.
  Gli hacker si curano meno degli aspetti superficiali di un individuo, prestando più attenzione alle capacità e al potenziale di far progredire lo stato generale dell'hacking. Non si effetuano discriminazioni in quanto ognuno, in base alle proprie capacità, può aiutare e sostenere la comunità.

- CON UN COMPUTER PUOI CREARE ARTE.
  La bellezza di un programma può stare anche nel modo in cui è scritto il codice. In ogni listato ognuno ci mette del suo, lo personalizza, lo migliora e lo arrichisce. Ogni hacker è in continua ricerca della *cosa giusta* per fare in modo che il programma faccia operazioni complicate con pochissime istruzioni; questo porta a sperimentare, ingegnarsi e ad inventare nuovi metodi. E' più che una semplice sfida, uno stimolo continuo ad innovare e a conoscere sempre meglio la macchina.

- I COMPUTER POSSONO CAMBIARE LA VITA IN MEGLIO.
  Per prima cosa i computer ci forniscono una miriade di vantaggi aprendo le vie della conoscenza. Di sicuro hanno arricchito le vite degli stessi hacker, rendendole utili alla società e in qualche modo anche avventurose. Se tutti potessimo interagire con i computer con lo stesso impulso creativo, produttivo e innocente degli hacker, la loro etica potrebbe spargersi attraverso la società come un'onda benefica e i computer cambierebbero davvero il mondo in meglio.

Partendo proprio da questi punti, nel seguito del testo vorremo approfondire i valori fondamentali che hanno animato e che animano gli hacker, e riportare al lettore una serie di esperienze attuali che interpretano bene lo spirito etico di questa controcultura. Una sorta di "raccolta di approfondimenti" atomici, per non fermarsi alla superficialità dei concetti ma per andare in fondo alle cose, come vuole il vero spirito hacker.

4.1 Dare precedenza all'imperativo di metterci su le mani

Per quanto, come abbiamo detto, si possa essere hacker in ogni campo, per capire la cultura hacker non possiamo prescindere dal contesto in cui essa è nata, ovvero quello dell'interazione fra l'uomo e il computer.
Dal manifesto di un noto hacker:

> Oggi ho fatto una scoperta. Ho trovato un computer. Ehi, aspetta un attimo, questo è incredibile! Fa esattamente quello che voglio. Se commetto un errore, è perchè io ho sbagliato, non perchè non gli piaccio...
> The Mentor [16]

Il computer ha qualcosa di intrinsecamente diverso da tutta la tecnologia prodotta precedentemente dall'uomo, qualcosa che può apparire come magico. Se la tecnologia meccanica può essere considerata come espansione "muscolare" delle possibilità dell'uomo, perchè ci permette per esempio di spostarci più in fretta o di spostare oggetti pesantissimi, il computer rappresenta invece un'espansione dell'intelletto umano; le potenzialità che esso offre e gli usi che se ne possono fare sono infiniti e superano qualsiasi limite di immaginazione. Non deve quindi stupire il fatto che dall'uso del computer sia nata una nuova cultura, basata su un modo diverso di approcciarsi alle cose e di interagire con la realtà.

Il primo sentimento di fronte a un computer, o a un programma, deve essere la curiosità. Capire come funziona e perchè, e come eventualmente si può migliorarlo, o modificarlo e usarlo per nuovi scopi. Per fare tutto questo bisogna guardarci dentro, capire il significato delle varie componenti, e sperimentare, in un continuo "dialogo" con la macchina. Il computer permette un tipo di interazione nuovo in cui l'utente è totalmente attivo e deve continuamente inventare nuove strategie per risolvere i problemi che man mano incontra. Questo processo richiede intelligenza e rigore logico, e allo stesso tempo creatività e fantasia; è estremamente stimolante, "divertente" per usare il termine di Linus Torvalds [1], ma possiamo dire anche "appassionante", e porta a grandi gratificazioni per chi riesca a far fare quello che vuole ad un computer. Questa è la prima grande scoperta degli hacker, da cui nasce tutto il resto. Tom Pittman nel suo manifesto *Deus ex machina, or the true computerist"* ha provato a rendere l'idea della sensazione che può accompagnare il vero hacker in questo processo creativo:

> "In quel momento io che sono cristiano sentivo di potermi avvicinare a quel tipo di soddisfazione che poteva aver provato Dio quando creò il mondo".

Questo tipo di esperienza, basata su un atteggiamento estremamente attivo nei confronti della tecnologia, purtroppo oggi è riservato a pochi. Il modello che si sta imponendo è quello di ridurre le persone a un uso passivo e prevedibile dei computer come delle altre tecnologie.

Il simbolo della modalità prevalente di interazione con le tecnologie dell'informazione nella nostra società è la televisione; l'apoteosi della passività cui questo mezzo ci vuole portare, come ha sottolineato un sociologo francese, Jean Baudrillard [17], si è raggiunta con le risate preregistrate nei telefilm, un mezzo per togliere agli spettatori anche il ruolo stesso di pubblico.

4.1.1 Software proprietario vs *Open Source*

Il software proprietario, il cui codice sorgente è tenuto segreto, può solo essere eseguito così com'è; non è possibile, a meno di riuscire a decifrare il codice binario (lavoro complicatissimo che alcuni pazienti smanettoni riescono talvolta a svolgere) apportare modifiche, miglioramenti o adattamenti, o anche solo capire come funziona il codice. Ragioni economiche, come quella di poter guadagnare dal proprio lavoro vendendo ogni singola riproduzione di un software, vengono così a limitare gli usi più intelligenti e innovativi che possono essere fatti di un programma.

I sistemi operativi Microsoft sono un esempio di come l'utente viene trattato dalle case produttrici di software commerciale: il codice è segreto e gli usi che si possono fare sono limitati e definiti al massimo. Il problema principale sembra quello di semplificare la vita all'utente, che dal canto suo, generalmente, non chiede altro che avere la vita semplificata. Vige un rapporto generale di sfiducia tra l'uomo e la macchina, in cui il massimo che ci si possa aspettare da questa è che non crei dei pasticci; dunque anche l'utente è ben contento di delegare il più possibile a degli "specialisti" il rapporto con questo mondo sconosciuto e dispettoso dell'informatica. Si può parlare per certi versi di una forma di "alienazione".

Per fare un esempio di casi che visti con un occhio estraneo alle dinamiche economiche possono sembrare veramente folli, ci sono programmi commerciali di contabilità aziendale dove anche modifiche come l'aggiornamento di un parametro, per esempio la percentuale dell'IVA, richiedono l'intervento della casa produttrice del software. In questo modo chi produce un programma si assicura rendimenti spropositati tenendo gli utenti nella condizione più passiva possibile di uso del software per i soli scopi precisi per i quali è stato progettato.

Secondo l'etica hacker, ciascuno dovrebbe essere il primo a poter mettere le mani sui programmi che utilizza per adattarli e renderli migliori per sè ed eventualmente per altri. I limiti che l'attuale sistema di proprietà intellettuale del software pone sono inaccettabili per gli hacker e questa è stata da sempre un delle pirincipali battaglie che essi si sono trovati ad affrontare.

Un sistema per dare veste legale ad un modello di condivisione dei saperi e per tutelare chi decida di rendere libero il codice che ha sviluppato, come abbiamo visto nelle "Storie di hacker" è quello del cosiddetto *copyleft* proposto da Richard Stallman; gli aspetti tecnici e differenze fra le varie licenze possibili saranno illustrati nel prossimo capitolo.

4.1.2 Il *digital divide* e la pratica del *trashware*

Prima ancora del problema dell'accessibilità e della libera circolazione delle informazioni, c'è quello dell'accessibilità delle tecnologie stesse: un altro tema particolarmente caro agli hacker, fin dai tempi dell'*Homebrew Computer Club* e dell'invenzione del primo personal computer.

Parlando di computer, oggi, non possiamo non ricordarci che la maggior parte della popolazione mondiale non ne ha probabilmente mai visto uno.

Per questo motivo è particolarmente interessante parlare di *trashware*, un tipo di esperienza molto diffusa fra le comunità hacker di tutto il mondo, finalizzata a diffondere l'uso del computer e a dotare di questa tecnologia anche persone, realtà o associazioni, spesso situate in altre parti del mondo, che non se la possono permettere.

Figura 1: Il logo del sito t r a s h ! i t a l i a [18], nato per permettere un facile accesso alle risorse italiane di *trashware*

La parola *trashware*, coniata con la consueta fantasia degli hacker, deriva da "trash" che in inglese significa "spazzatura" e indica la pratica del riciclo di vecchie macchine, o parti, considerate inservibili dalla mentalità comune, ma che assemblate con passione e pazienza possono rivelarsi utilissime e possono significare per qualcuno la possibilità di avvicinarsi a un computer.

Da Wikipedia [19]:"Parte integrante del trashware è l'installazione di software libero sul sistema, ad esempio il sistema operativo GNU/Linux, per portare avanti lo spirito di libertà dell'iniziativa.
Il materiale informatico così ottenuto viene consegnato o regalato a persone ed enti che ne abbiano bisogno, in particolar modo legandolo ad iniziative che tentano di colmare il divario digitale (digital divide), ossia la differenza di mezzi a disposizione tra chi è informaticamente alfabetizzato e chi ancora non lo è."

4.2 Tutta l'informazioni deve essere libera

4.2.1 Il software libero

Nei nostri discorsi abbiamo spesso definito la libertà dell'informazione come una componente essenziale per la crescita della società. Il software libero nasce e viene prodotto da una grossa comunità composta da utenti e sviluppatori, in uno spirito di collaborazione e scambio tra pari.

Prima di cercare di comprendere le ragioni ed i vantaggi nella produzione e nell'adozione di software libero per le proprie attività, vogliamo tentare di fornire al lettore una breve introduzione sulle categorie di licenze e su cosa intendiamo quando stiamo parlando di *Free Software*.

Qualsiasi software è legalmente equiparato alle *opere di ingegno*, la cui tutela ricade sotto la normativa del diritto di autore. Per questo motivo quando si acquista un programma non se ne ottiene la proprietà ma solo la possibilità di utilizzarlo secondo quanto previsto dalla legge relativa e dalla licenza: un contratto tra il titolare dei diritti sul software e l'utente, che stabilisce diritti e doveri di entrambe le parti. Diventa di fondamentale importanza capire le diverse tipologie di licenza, per poter comprendere sino in fondo le diverse condizioni di libertà concesse. In maniera sintetica e certamente non esaustiva possiamo catalogare le principali licenze in questo modo:

Software Libero
È quel software la cui licenza soddisfa le condizioni richieste dalla Free Software Foundation[5] di Richard Stallman, ovvero:

- la libertà di utilizzare il programma, per qualunque scopo,
- la libertà di studiarne il funzionamento e di adattarlo ai propri bisogni,
- la libertà di redistribuirne copie, in modo tale da poter aiutare il prossimo,
- la libertà di migliorare il programma e di distribuire tali migliorie al pubblico, in modo tale che l'intera comunità ne tragga beneficio.

La disponibilità del codice sorgente è considerata prerequisito per la seconda e la quarta libertà.

Dal 1985, anno di costituzione dell'associazione no-profit FSF (Free Software Foundation), moltissimi software sono stati rilasciati con questa licenza, compreso il sistema *GNU-Linux.* Come abbiamo visto nella storia hacker americana, l'importanza di Stallman e delle sue idee nel processo di creazione di un'identità hacker è stata fondamentale per consolidare sino a noi questi valori. Tutt'ora la FSF è il punto di riferimento per i progettisti di software libero poichè oltre a promuovere un'ideale etico basato su un nuovo modo di lavorare e di vedere il prodotto dell'ingegno umano, assicura ai piccoli sviluppatori un supporto di garanzia della qualità del prodotto e di protezione legale.

Il termine *Free Software* deve essere interpretato in due sensi, poichè la traduzione nella nostra lingua lo ha privato del significato originale. Il termine

free che, nella lingua inglese, ha il doppio significato di libertà e gratuità, deve essere inteso nella prima accezione, "come in *free speech*, e non come in *free beer*" [4]. Le ragioni di fondo del progetto di Stallman richiamano l'importanza di costruire e mantenere un legame sociale all'interno della comunità dei produttori e sviluppatori di software, in quanto il valore principale è rappresentato dal valore d'uso per l'intera comunità e non dal semplice valore economico.

Software Open Source
È quel software la cui licenza soddisfa le condizioni della *Open Source Definition* realizzata dell'*Open Source Initiative*, simili a quelle della *Free Software Foundation*, ma non identiche, in quanto pensate per motivi e destinatari diversi.

In particolare le condizioni della OSI sono più dettagliate di quelle della FSF da un punto di vista pratico, ma meno interessate agli aspetti morali.

Software Copylefted
È un tipo di software libero la cui licenza impone che ogni prodotto da esso derivato sia ancora libero, solitamente sotto la stessa licenza: licenze di tale tipo sono la GPL (la licenza principale del *Free Software*), ma non ad esempio la BSD[5].

Software proprietario
È quel software che viene rilasciato sotto licenze che concedono all'utente solo ed esclusivamente l'utilizzo del prodotto, sotto condizioni restrittive.

Il termine può trarre in inganno in quanto anche il software libero è "proprietario", nel senso che appartiene ad una persona (fisica o giuridica, il titolare del copyright).

Software closed source
È un altro termine usato per indicare il software proprietario, in contrapposizione a quello "open source".

Se si usa questo termine è opportuno ricordare che possono essere "closed source" anche programmi il cui codice sorgente è a disposizione degli utenti, ad esempio sotto un contratto di non divulgazione, o magari anche solo come una licenza che ne vieta la distribuzione modificata.

Software semi-libero
È quel software la cui licenza offre alcune delle libertà richieste dal software libero, ma non tutte: in particolare di solito vengono posti vincoli sulla vendita o sull'utilizzo a scopo di lucro del programma.

Software di pubblico dominio
È software privo di un proprietario: chi lo utilizza gode della maggior parte dei diritti offerti dal software libero, ma non c'è nessuna garanzia che questi diritti rimangano, in particolare chiunque potrebbe appropriarsene e rendere proprietarie le versioni modificate.

Davanti ad una molteplicità di licenze con cui rilasciare il proprio lavoro, è necessario capire perchè una moltitudine di sviluppatori preferisce il modello

[5]Berkley Software Distribution

del “Free Software” o “OpenSource” piuttosto che la controparte proprietaria; come abbiamo anticipato le due definizioni non sono esattamente identiche ma, almeno in italiano, si utilizzano in maniera indistinta poichè il termine “Open-Source”, sebbene rappresenti una definizione meno filosofica, fa capire meglio la vera natura del discorso.

A livello economico, l’utilizzo di software già scritto da altri e riutilizzabile in progetti personali è una reale possibilità di business per i piccoli imprenditori che si trovano così a combattere le grandi multinazionali del software con il supporto di un’interà comunità di sviluppatori. Ma la vera forza dell’*OpenSource* deriva da qualcosa di più profondo, da una reale necessità di crescita sociale e democratica libera da controlli dall’alto e dai pericoli tecnocratici. L’utilizzo giova allo sviluppatore, come all’utente, che può scegliere e può valutare un prodotto “aperto” in maniera da capire se il prodotto stesso possa realmente soddisfare le sue richieste. Qualità non funzionali, come l’affidabilità e la sicurezza di un prodotto informatico, sono difficilmente valutabili in un software “chiuso” e spesso inducono un falso senso di sicurezza. L’utente attraverso l’uso di un software libero può verificare, volendo, il codice punto per punto o comunque affidarsi allo sguardo attento di migliaia di sviluppatori che giorno dopo giorno segnalano errori, bug e vulnerabilità.

Fare considerazioni riguardo l’uso o meno del *software libero* significa continuare a considerare due livelli: il primo legato unicamente ad una pura scelta etica che mette la libertà come elemento cardinale del discorso e l’altro che invece valuta le caratteristiche intrinseche del software sviluppato in questo modo, per il ciclo di sviluppo e revisione continua a cui è sottoposto[7].

In questo mondo, fatto di un continuo scambio di “doni”, sono stati create molte delle tecnologie e del software che noi oggi utilizziamo quotidianamente. *Linux* è il caso più noto attualmente, ma forse non il più ecclatante per quanto se ne dica. Se pensiamo ad Internet ci accorgiamo come sia il risultato di singoli contributi personali, all’interno di un contesto libero e fuori dal controllo della logica di mercato[20]. La rete, intesa come infrastuttura a supporto di Internet, è stata sviluppata e viene gestita con tantissimi prodotti liberi. Connettendo programmatori e studiosi in tutto il pianeta è poi diventato anche lo strumento fondamentale per lo scambio di informazioni e di software libero.

“...Internet oltrechè madre è stata anche figlia del software libero. ”
- Angelo Raffaele Meo -

4.3 Dubitare dell'autorità, promuovere il decentramento

La cultura hacker nasce nel contesto degli anni '60 negli Stati Uniti, in seno al movimento di contestazione della guerra del Vietnam, ed è forte in essa la matrice anarchica del movimento *hippie*. L'anticonformismo e la critica radicale del sistema, delle istituzioni e dei valori dominanti della società borghese sono alla base dell'etica hacker.

L'hacker è antropologicamente insofferente verso l'autorità in quanto limitante dell'iniziativa, dell'intelligenza e della creatività dell'individuo, e si distingue in questo dal *droid*, termine coniato dagli hacker per definire chi tende ad essere succube dell'autorità. Ne riportiamo parte della definizione, estratta dal *Jargon file* [21], una sorta di dizionario *hackerish-english* curato da E. S. Raymond:

Droid (nome, da "androide", terminologia per un un robot umanoide di costruzione biologica e non meccanico-elettronica). Una persona che presenta la maggior parte delle seguenti caratteristiche: (a) fiducia cieca nella saggezza della propria organizzazione e del "sistema"; (b) propensione a credere ciecamente nell'ovvio nonsenso di quanto proviene dalle autorità (o dai computer!); (c) mentalità governata da regole, incapace o non interessata a guardare oltre la "lettera della legge" in situazioni eccezionali; (d) terrore paralizzante delle reprimende ufficiali e (e) nessun interesse a fare qualcosa che vada al di là del proprio lavoro strettamente inteso, e in particolare a porre rimedio a quello che non va, sulla base dell'attitudine: "Non è compito mio".

Ecco un altro termine interessante, sempre tratto dal *Jargon file*, che da l'idea della mentalità anticonformista che sta alla base della cultura hacker:

Suit.1. (nome) Brutta e scomoda giacca da business, portata spesso dai non hacker. Invariabilmente accompagnata da un dispositivo di strangolamento chiamato "cravatta", che riduce il flusso di sangue al cervello. Si ritiene che ciò spieghi molto del comportamento di un portatore di *suit* 2.(nome) Una persona che abitualmente veste *suit*, in contrapposizione a un "techie" o "hacker".

L'avversione all'autorità è dunque prima di tutto qualcosa di antropologico: l'hacker è quel tipo di persona che ama pensare con la propria testa e potersi confrontare liberamente con gli altri. Autorità, burocrazia e gerarchie sono viste come ostacoli al libero scambio di idee e al libero confronto di punti di vista, che devono essere alla base della ricerca.

Seguendo una analogia introdotta da Pekka Himanem [22] possiamo vedere come modello dell'etica hacker l'*accademia*, in contrapposizione al *monastero*. Come gli hacker, gli scienziati procedono in un processo di ricerca collettivo, basato sull'apertura, sullo scambio e sull'*autoregolazione*. Quest'ultimo concetto di autoregolazione, fondamentale per l'etica scientifica, è lo stesso su cui si basava l'accademia platonica, in cui l'avvicinamento alla verità era ricercato attraverso il *dialogo critico*. Il punto di partenza è lo spirito di iniziativa dei singoli scienziati, o programmatori, che propongono delle aggiunte al patrimonio culturale della comunità; in questo passaggio sono fondamentali la citazione delle fonti o delle versioni precedenti, da una parte, e la libera circolazione dei nuovi

risultati, dall'altra. E' poi la comunità scientifica nel suo complesso ad accettare e fare propri modifiche e miglioramenti, in una sorta di processo spontaneo di "selezione naturale".

Il modello dell'accademia si contrappone storicamente a quello del monastero, ovvero un modello chiuso e autoritario, in cui l'obiettivo viene stabilito una volta per tutte e un ristretto gruppo di persone viene incaricato di lavorarci sopra. Il risultato raggiunto dovrà essere accettato da tutti, senza che sia prevista la possibilità di intervenire da parte di altri.

Come appare chiaro, il rifiuto del modello autoritario non è determinato solo da ragioni etiche, ma anche pratiche. La maggiore efficienza di un modello aperto è una delle tesi più care agli hacker; l'esempio più tipico è quello del sistema operativo GNU/linux, sviluppato da una rete di volontari. Secondo le parole di Raymond a proposito della nascita di Linux, nel suo noto saggio "La cattedrale e il Baza" [7], l'innovazione più grande portata da Linus Torvalds non è tecnica, ma sociale. Con lo sviluppo di Linux si è affermato un nuovo paradigma sociologico, quello del bazar, corrispondente al modello aperto dell'accademia, in contrapposizione a quello classico della cattedrale, dominante nelle grandi aziende commerciali di software, dove il progetto viene definito da una o poche persone e portato avanto in modo chiuso e lineare.

Strumento fondamentale per la riuscita di linux, come abbiamo già detto, è stata la rete, attraverso la quale centinaia di volontari sparsi in tutto il mondo hanno potuto coordinare il proprio lavoro. Internet, altra invenzione fondamentale degli hacker, decentrata e difficilmente controllabile per sua natura, si è rivelata anch'essa essere molto di più di un'invenzione tecnologica, e ha portato a un cambiamento profondo della nostra società, determinando un nuovo paradigma, quello della *network society* [23].

4.3.1 *Tor*: un sistema anonimo di comunicazione su internet

Proprio intorno al futuro di internet si combattono tuttora battaglie molto importanti: infatti se è vero che la rete è per sua natura anarchica, decentrata e difficilmente controllabile, lo spettro dell'autorità incombe sempre. Per difendere la libertà di internet e i diritti fondamentali del *cyberspazio* è nata nel 1990 la *Electronic Frontier Foundation* (Eff) [24], fondata dagli hacker M. Kapor e J. P. Barlow [25]

Molti governi già oggi impongono restrizioni ai motori di ricerca nel proprio paese o controllano l'accesso a determinati tipi di siti; per esempio in Arabia Saudita gli Internet provider sono obbligati a tenere la registrazione delle attività di tutti gli utenti e a mandare messaggi automatici quando questi cercano di visitare siti sgraditi al governo.

Ma la più grande minaccia per la libertà di internet forse non viene dai governi, bensì dal mondo del business. Attraverso le informazioni che il *browser* di un utente scambia con il *server* per esser identificato (mediante il sistema dei *cookie*) per esempio, è possibile per aziende specializzate costruire il pro-

filo e identificare lo stile di vita degli utenti del web monitorando le pagine che visitano. Allo stesso modo possono essere analizzati i messaggi postati sui *newsgroup*. Le tracce elettroniche che un utente del web lascia, per lo più inconsapevolmente, sono innumerevoli ed è ormai aperta una vera e propria caccia alle informazioni personali a cui è difficile sfuggire. Una sfida interessante per il mondo degli hacker, che hanno sempre visto nella privacy un bene prezioso e una forma di libertà da difendere a tutti i costi.

Uno dei progetti più recenti portati avanti dalla Eff è un programma, Tor [26], che permette di mantenere nascosto il proprio indirizzo IP sulla rete. Il programma si basa sulla crittografia a chiave pubblica e sull'utilizzo di catene casuali di server, chiamati *onion router*. Quando un utente collegato a internet tramite Tor richiede una pagina web o un qualsiasi servizio a un server, la richiesta non viene inoltrata direttamente alla destinazione, ma attraverso un percorso casuale nella rete dei server a cui il programma si appoggia; in questo modo è reso molto più difficile, se non impossibile, ricostruire le destinazioni delle comunicazioni di un utente.

Attraverso una rete di server che mettano a disposizione le proprie risorse è così possibile visitare siti, pubblicare pagine, utilizzare programmi di chat con la libertà di decidere se si vuole essere identificati oppure no. Il software è ovviamente libero, sviluppato da una rete di volontari.

4.4 Giudicare i soggetti in base al loro operato

"Come la maggior parte delle culture non basate sul denaro, quella degli hacker si basa sulla reputazione.
E. S. Raymond [15]"

Fondamentale nella cultura hacker è il concetto di *comunità*. Gli hacker stessi si definiscono come una comunità ed essere hacker significa appartenere a questa comunità, come spiega Raymond nel noto manifesto *Come diventare un hacker* [15]. È fuorviante lo stereotipo di hacker come persona asociale. La grande valorizzazione delle capacità del singolo, della sua creatività e intelligenza, è subordinata alla misura in cui esse portano un contributo alla comunità.

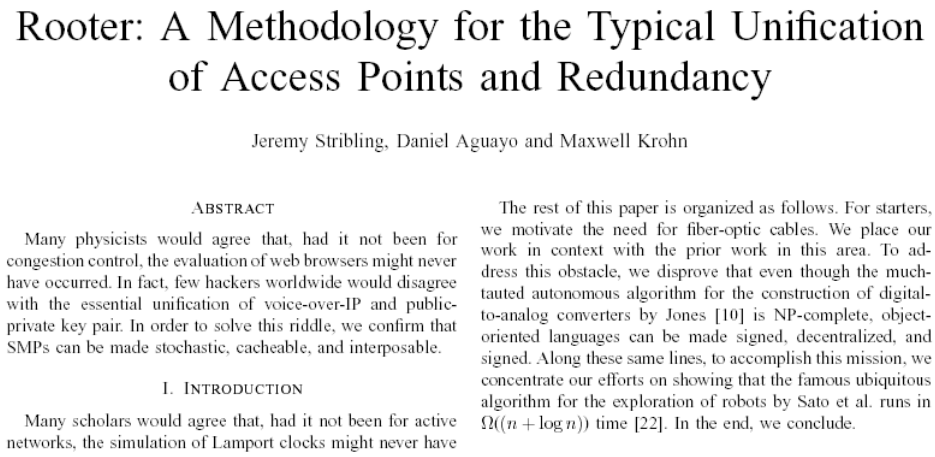
Poichè quello che conta sono le capacità e il contributo che un individuo riesce a dare alla comunità, tutti i falsi criteri dominanti nella società come ceto, razza e posizione sociale sono rifiutati come fasulli. All'interno della comunità hacker questi criteri si annullano, e lasciano il posto ad altri. La reputazione all'interno della comunità deve essere conquistata attraverso i propri meriti. Per Raymond gli hacker sono motivati dalla *forza del riconoscimento fra pari* [27]; Pekka Himanem parla del *valore sociale* come motivazione che insieme alla passione si sostituisce, nell'etica hacker, a quella classica del denaro.

Quest'idea forte di comunità è un tratto distintivo dell'etica hacker, in decisa controtendenza rispetto ai valori fondanti della nostra società, dove la spinta è sempre data dall'interesse economico del singolo. Crediamo che la difficoltà di capire il movimento hacker da parte della cultura dominante sia dovuta proprio soprattutto all'incapacità di cogliere questo aspetto della comunità come elemento fondante e come contesto di motivazione delle azioni individuali. Questo è forse uno dei motivi per cui è molto più facile sui mezzi di comunicazione parlare degli hacker come pirati informatici, ossia parlare in realtà dei cracker, che giocano a scassare i computer degli altri e a svuotare le carte di credito. I cracker non hanno quel collante di valori comuni e di senso di appartenenza forte ad una comunità, proprio degli hacker, ed è rimasta loro solo una certa abilità nell'usare le tecnologie, attraverso le quali essi perseguono spregiudicatamente i propri obiettivi personali; per questo essi rientrano più facilmente nelle categorie che la cultura dominante ci offre per interpretare la realtà.

Il riconoscimento all'interno della comunità hacker viene ottenuto grazie al contibuto innovativo dato ad essa e dimostrando le proprie capacità, fantasia e intelligenza. Oltre allo sviluppo di nuovo software, o all'uso originale delle tecnologie per scopi che non erano stati previsti, un'altra manifestazione di bravura tipica della cultura hacker è lo "scherzo tecnologico creativo", che può anche prendere le forme di una rivendicazione dei valori della comunità attraverso un'azione creativa. Due esempi attuali di manifestazioni di questo tipo, concepite una nello storico MIT, che ancora fa parlare di sè, e una nel panorama hacker milanese, possono mostrare bene lo spirito che anima questo tipo di azioni, dove la forma è fondamentale e diventa una cosa sola insieme al contenuto del messaggio che si vuole comunicare.

4.4.1 Articoli scientifici generati da un computer

La prima azione ha per protagonisti tre studenti del MIT, che hanno voluto sfidare una prestigiosa conferenza scientifica internazionale, la World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI), in programma a luglio di quest'anno in Florida. I tre studenti hanno realizzato un software, che hanno chiamato SCIgen, in grado di generare automaticamente articoli fatti di frasi casuali senza senso in gergo scientifico; un articolo generato in questo modo è stato accettato dalla commissione tecnica della conferenza, la cui mancanza di credibilità è stata così mostrata in modo eclatante.



Rooter: A Methodology for the Typical Unification of Access Points and Redundancy

Jeremy Stribling, Daniel Aguayo and Maxwell Krohn

Abstract

Many physicists would agree that, had it not been for congestion control, the evaluation of web browsers might never have occurred. In fact, few hackers worldwide would disagree with the essential unification of voice-over-IP and public-private key pair. In order to solve this riddle, we confirm that SMPs can be made stochastic, cacheable, and interposable.

I. Introduction

Many scholars would agree that, had it not been for active networks, the simulation of Lamport clocks might never have

The rest of this paper is organized as follows. For starters, we motivate the need for fiber-optic cables. We place our work in context with the prior work in this area. To address this obstacle, we disprove that even though the much-tauted autonomous algorithm for the construction of digital-to-analog converters by Jones [10] is NP-complete, object-oriented languages can be made signed, decentralized, and signed. Along these same lines, to accomplish this mission, we concentrate our efforts on showing that the famous ubiquitous algorithm for the exploration of robots by Sato et al. runs in $\Omega((n + \log n))$ time [22]. In the end, we conclude.

Figura 2: L'articolo generato casualmente, accettato dalla commissione tecnica della WMSCI

Un modo decisamente hacker di smascherare un certo sistema di convention scientifiche, delle prenotazioni negli alberghi di lusso, dei pass rilasciati su invito, dei regali di partecipazione; un mondo di apparenza e di giri di denaro, a cui non corrispondono contenuti di reale valore scientifico.

Il programma creato dai tre studenti è ovviamente open source ed è disponibile sul sito [28] dove ognuno si può divertire a generare articoli a proprio piacimento scegliendo il nome degli autori. Attraverso il sito, i tre studenti stanno raccogliendo sottoscrizioni per pagare il viaggio e la propria partecipazione alla conferenza e portare avanti la loro creativa azione di denuncia andando a tenere un discorso generato casualmente.

4.4.2 Serpica Naro: "hackerata" la settimana della moda

" Serpica naro, giovane artista e stilista anglonipponica, presentera' a Milano (il 26 febbraio [6] dalle 19.00 alle 22.00 sul cavalcavia Bussa) durante la settimana della

[6] Anno 2005

moda le proprie opere.
Le sue performances hanno conquistato l'attenzione dei critici ma hanno sempre lasciato uno strascico di polemiche per il suo uso spregiudicato di tematiche sociali e di ambienti metropolitani
L'Italia, paese in cui l'artista viene per la prima volta, non sembra fare eccezione.
Serpica naro si ispira al total design che tratteggia artisticamente non solo abiti, accessori ed ambienti ma stili di vita e di prospettive sociali. [...]
Nelle sue parole "we are not the high class, we are not the low class, we are the new class" c'e' tutta la sua ambizione ma è proprio dai suoi spregiudicati atteggiamenti che nasce il contrasto con i giovani attivisti gay di Milano "

Questo è l'inizio della presentazione di Serpica Naro sul sito della settimana della moda [29], evento di interesse internazionale, attorno al quale girano ogni anno decine di migliaia di euro.

Ma la giovane e attesissima stilista, incaricata di chiudere la settimana della moda di quest'anno, si è rivelata essere soltanto l'anagramma di *San Precario*, patrono e simbolo dei lavoratori precari milanesi. Davanti agli occhi increduli di stilisti, vip e giornalisti, i lavoratori precari hanno sfilato sulla passerella, mostrando abiti come pancere nascondi-gravidanza, adatte a lavoratrici precarie che non vogliano perdere il proprio posto di lavoro, gonne anti-mano morta piene di trappole per topi, minigonne sexy per fare carriera più in fretta, abiti da sposa per donne senza cittadinanza italiana, tute da lavoro con pigiama, per essere sempre pronti a lavorare notte e giorno.

La beffa, in cui la Camera Nazionale della moda è caduta senza nessun sospetto, è stata preparata in tre settimane di lavoro ben coordinato di circa duecento persone, che hanno approntato un *look book* di grande qualità, un sito internet dedicato alla stilista [30], diversi altri siti falsi creati ad arte che parlavano di lei e rassegne stampa fasulle. A rendere tutto più reale è stato anche un passato scabroso inventato per la stilista, che si sarebbe finta attivista gay per convincere alcuni modelli omosessuali giapponesi a posare per una rivista alternativa e avrebbe poi sfruttato le loro immagini per la propria pubblicità; la divulgazione di questa notizia nelle mailing list gay italiane aveva suscitato una polemica intorno alla stilista. Importante è stata anche la collaborazione con una rete di persone all'estero, che ha dotato Serpica Naro di un ufficio stampa a Tokyo e uno a Londra, oltre a quello italiano.

Oltre ad avere attirato l'attenzione dei media sul tema assai caro della propria condizione di lavoro, i lavoratori precari del mondo della moda milanese hanno anche creato e pubblicizzato un nuovo *meta-marchio*, come l'hanno definito, per la rete di autoproduzioni a livello europeo con cui sono in contatto. Il marchio di Serpica Naro è infatti già stato registrato, perchè diventi "un l(u)ogo di reti di autoproduzioni tessili, di condivisione dei saperi, di creatività e immaginario di contrapposizione alla moda [31]. I materiali saranno tutti raccolti nel laboratorio/sito ufficiale della finta stilista, a condizione di essere "open source". Tutti quelli che si riconosceranno in questo *metabrand* potranno firmarsi Serpica Naro.

Elementi come la fantasia, un abile uso delle tecnologie, la valorizzazione

delle proprie competenze in un modo originale e lo sbeffeggiamento di un mondo basato sull'apparenza e sul denaro come quello della moda, fanno di questa una tipica azione hacker, mostrando come l'etica hacker sia pervasiva e si stia diffondendo in ambiti che vanno al di là dello sviluppo di hardware e software. Le abilità tecniche richieste per questa azione, in particolare, non erano legate tanto al livello del software (e ancora meno dell'hardware), ma a quello che può essere definito *infoware*[32].

4.5 Con un computer puoi creare arte

Pensare ad un'elaboratore come una semplice macchina per effettuare calcoli è alquanto limitativo. Ogni hacker sa che dietro ad ogni meccanismo si può nascondere una nuova sfida e un nuovo modo di esprimere le proprie capacità tecniche ed espressive. Spesso l'immaginazione permette di superare i confini imposti dalle tecnologie, dando luogo ad applicazioni decisamente fantasiose. Il computer non è solo uno strumento funzionale per facilitare compiti ripetitivi, ma un reale mezzo per estendere l'immaginazione personale. Cercare di realizzare qualcosa di concreto, sfruttando al massimo le potenzialità dello strumento, permette di liberare la mente e realizzare qualcosa che può essere paragonato ad un prodotto artistico.

Potremmo presentare decine di applicazioni, più o meno serie, di tecnologie usate in contesti o in modalità diverse da quelle per cui erano state inizialmente progettate; ci teniamo però a presentare due progetti tutti italiani.

4.5.1 L'*Ascii Art* e il progetto *HasciiCam*

L'*Ascii Art* è una tecnica, usata inizialmente nei manuali tecnici in mancanza di figure, che permette di disegnare all'interno di qualsiasi documento di testo attraverso un'opportuna composizione di caratteri. L'effetto di questi disegni è spesso straordinario in quanto con la giusta collocazione dei caratteri è possibile creare effetti di chiaro e scuro, che ad una certa distanza, fanno assomigliare la figura ad una vera e propria immagine. Sebbene esistessero già da tempo dei software che dato in ingresso una fotografia, generano una rappresentazione della medesima in modalità *ascii*, difficilmente si poteva pensare ad un'applicazione tanto fantasiosa.

Stiamo parlando di *HasciiCam*[33], un software in grado di "convertire" l'input proveniente da una scheda di acquisizione video (come le normali schede TV) o da una webcam ridisegnando in tempo reale l'immagine, frame per frame, in puro testo. L'immagine è riconoscibilissima, le sfumature vengono realizzate con grande precisione e con l'utilizzo di particolari librerie è addirittura possibile sfruttare la colorazione dei caratteri per creare effetti stupefacenti. Sebbene il progetto si appoggi su librerie già precedentemente sviluppate (le *aalib*), il merito del lavoro è tutto di un italiano residente in Austria, attivista convinto nel mondo della contro-cultura hacker italiana. Oltre l'aspetto prettamente ludico, dietro a questo stravagante esperimento si nasconde un'applicazione utile nel caso sia necessario effettuare dello *streaming* video attraverso reti a bassa velocità. Trasmettere semplici caratteri, invece che immagini, permette di ridurre notevolmente la banda occupata durante una videoconferenza oppure durante la proiezione di film in streaming rendendo interessante la tecnologia anche per i paesi in via di sviluppo che hanno infrastrutture vecchie e difficilmente a banda larga.

Figura 3: Uno screenshot del progetto Hasciicam

4.5.2 *Polygen*: un generatore di frasi casuali

Cambiando completamente ambito,vogliamo ora presentare un'applicazione software per la generazione automatica di stringhe di testo di senso compiuto: *Polygen*. Una tecnica normalmente utilizzata per l'analisi semantica di testi[7], basata sulle grammatiche non contestuali, viene in questo caso utilizzata in un modo completamente diverso. Attraverso un file di testo, chiamato *file della grammatica*, contenente le definizioni della struttura sintattica di una frase nella lingua italiana ed una raccolta di termini di un particolare settore, il programma genera le frasi in maniera automatica e casuale ad ogni esecuzione. Il risultato è sicuramente divertente ed imprevedibile come dimostrano queste generazioni casuali, legate ai nomi di possibili comuni lombardi: "Arconate san Salvatore", "Garlano Masciago" e "Tavazzano". Utilizzando poi diversi file della grammatica è possibile cambiare il soggetto della generazione; i visitatori sono invitati a usare il motore della grammatica per arricchire il sito con nuovi contesti.

Dal sito web del progetto (*http://polygen.org/*[34]), oltre a scaricare il software stesso, è possibile utilizzarlo nella versione online con una serie veramente lunga di grammatiche: dalla generazione di nomi di "boy-band" ai nomi degli esami per ingegneri gestionali, da storielle zen sino a edizioni del telegiornale Studio Aperto, a comunicati di girotondini o annunci pubblicitari.

Ecco come un potente strumento tecnico, utilizzato in un modo diverso da quello per cui era stato progettato, si può trasformare in uno strumento di satira che, grazie alla fantasia degli sviluppatori e dei visitatori del sito, non risparmia nessun aspetto della nostra società.

[7]Nel senso più generale, è una tecnica utilizzata per la determinazione del significato di una frase

Ordinazione

I lor signori desiderano?
Una cioccolata calda.
Altro?
Si, anche un the bollente, un caffe' freddo e nove the tiepidi.
Altro?
No, e' ok.

Generane un'altra | Pubblica sul tuo sito | Classifica della settimana

GRAMMAR INFO

title:	**Facciamo ordinazione**
author:	**Pan <pan@spinningkids.org>, Pasu & Pete**
language:	**italian**
status:	**refinable**
topic:	**misc**
audience:	**anybody**
disclaim:	**e' estate, prendiamoci un una grappa macchiata bollente corretta cognac in bicchiere**
created:	**03/08/2004**

Ordinazione

Dite pure
Un caffe' tiepido in tazzina grande di peltro e un marocchino bollente in tazzina grande fredda.
Basta?
No, anche quattro grappe, sei caffe', nove grappe tiepide ristrette sbagliate di cui una in tazzina calda con due manici e cinque the ustionanti.
Altro?
Si, anche un marocchino.
Altro?
Si, anche un the gelato, una cioccolata in bicchiere e una cioccolata corretta mandarinetto.
Basta?
No, dimenticavo... ci porti anche un caffe' corretto in tazza media calda di terracotta.
Altro?
No, grazie.

Figura 4: Polygen: due generazioni casuali di ordinazioni al bar

Gli esempi di progetti ed applicazioni fantasiose di vecchie tecnologie riutilizzate con estrema ingegnosità potrebbero essere moltissimi altri. In tutte queste creazioni, la componente tecnologia è stata utilizzata nella maniera migliore per creare qualcosa di nuovo. Osservando criticamente il risultato di questo lavoro, cercando di andare oltre all'aspetto ludico spesso presente, non è possibile fare a meno di notare con quale entusiasmo e perfezione sono create molte di queste cose. Ogni hacker vuole esprimere la propria creatività e lo fa nel modo a lui più congeniale; che questo significhi assemblare vecchi pezzi *hardware* per realizzare una scultura oppure scrivere un software per creare musica non è importante.

4.6 I computer possono cambiare la vita in meglio

L'idea che le macchine si sarebbero sostituite al lavoro umano, almeno nei compiti più pesanti e noiosi, ha sempre accompagnato lo sviluppo delle nuove tecnologie, dando luogo a una sorta di utopia, quella della "fine del lavoro" per usare le parole di Jeremy Rifkin[35]. Quasi un ritorno alla fase dell'Eden, quando l'uomo non aveva bisogno di lavorare; una nuova epoca storica in cui il tempo da dedicare al lavoro sia sempre meno, e resti più spazio per l'"ozio" e per coltivare i propri interessi; in cui anche il lavoro, quello che rimane, sia stimolante, intellettuale, fatto di interazione fra le persone.

Questa resta purtroppo un'utopia, tanto più distante dalla realtà in quanto la ricchezza prodotta dalle macchine non viene redistribuita e gli squilibri sociali aumentano. L'accentramento dei saperi sottoforma di brevetti non fa che aumentare i profitti di poche aziende lasciando un numero sempre crescente di persone nella miseria.

Nella cultura hacker è forte la consapevolezza di questi meccanismi di accentramento di potere e di esclusione sociale, che passano ormai spesso dall'esclusione all'accesso alle tecnologie e alle informazioni [36]; ma altrettanto forte è anche la consapevolezza delle potenzialità che le tecnologie possono offrire per migliorare la nostra vita.

Accanto alle battaglie politiche, sociali e culturali portate avanti instancabilmente dalla comunità hacker perchè i benefici portati dalle nuove tecnologie possano ricadere su tutti, vi è la convinzione di essere dei privilegiati. Per gli hacker l'utopia della "fine del lavoro" è più vicina di quanto possa sembrare, se pensiamo che il loro lavoro, quello che viene lasciato dalle macchine, ovvero di programmarle, assomiglia di più a un gioco che al lavoro tradizionale. La cultura hacker porta con sè una nuova etica del lavoro, come ha mostrato Pekka Himanem nel suo libro "L'etica hacker e lo spirito dell'età dell'informazione" [22], dove la motivazione al lavoro non è data dal denaro ma in primo luogo dalla passione per quello che si fa: "c'è una certa differenza tra l'essere permanentemente tristi e l'aver trovato una passione nella vita, per la cui realizzazione ci si può anche impegnare nelle parti meno divertenti ma comunque necessarie".

4.6.1 *Wikipedia*: un enciclopedia redatta collaborativamente

Il progetto Wikipedia [19] è nato nel 2001 con l'intento di costruire un'enciclopedia libera, aperta e multilingue. L'enciclopedia è libera, perchè è coperta dalla *GNU Free Documentation License*, ma questo non è il suo aspetto più innovativo. La novità più grande sta nel fatto che i redattori sono i lettori stessi, cioè potenzialmente tutti gli abitanti del nostro pianeta. L'encicolpedia è un tentativo azzardato di dare la parola a tutti, di raccogliere quel pezzetto di sapere che ciascuno possiede e vuole mettere a disposizione degli altri, e ricomporre il contributo di tutti come in un puzzle.

Grazie all'uso del *wiki*[8], ovvero di un tipo di pagina che può essere modifica-

[8] *wiki*: parola hawaiiana che significa "veloce"

Figura 5: Il simbolo di Wikipedia

ta e visualizzata molto rapidamente è molto facile per chiunque, anonimamente, aggiungere una nuova voce e modificare quelle esistenti; al termine di ogni pagina dell'enciclopedia c'è, in risalto, un tasto "modifica" attraverso il quale chi legge una definizione può ampliarla o specificarla, se lo ritiene opportuno. Tutti sono invitati e spronati esplicitamente a perdere quel poco di tempo che serve per migliorare quello che leggono se non li soddisfa. Ogni intervento viene registrato nella "storia" della wikipedia, attraverso la quale è possibile consultare tutte le modifiche e le versioni precedenti di ogni voce. L'unico controllo effettuato è a posteriori, per cancellare rapidamente interventi "vandalici"

Il progetto è azzardato e può sembrare ingenuo, perchè se chiunque può scrivere la sua opinione l'enciclopedia si può riempire presto di falsità, scritte in buona o cattiva fede. Eppure il risultato, dopo quattro anni di continue aggiunte, modifiche e raffinamenti da parte dei lettori-autori, mostra che il livello di qualità e di precisione dei contenuti è mediamente alto. L'assioma su cui si basa il progetto è che in un processo assolutamente spontaneo la verità tenderà ad emergere.

Oggi la Wikipedia esiste già in moltissime lingue, dal lettone al basco, del tamil al siciliano; la sezione inglese del sito conta oltre 585000, e quella italiana oltre 45000; il 22 settembre 2004 il numero totale di articoli ha superato il milione. Gli aggiornamenti effettuati sono migliaia al giorno, e la quantità di articoli nuovi scritti ogni giorno è in continua crescita. Il progetto è ancora in una fase quasi embrionale, rispetto alle proporzioni che può raggiungere.

Il processo di scrittura collettiva su cui si basa la wikipedia non può non ricordare quello con cui viene sviluppato il software libero; riprendendo la metafora di Raymond della cattedrale e del bazar [7], il progetto Wikipedia rappresenta un'ambiziosa applicazione del modello del bazar che vuole comprendere tutti i campi del sapere.

L'accessibilità, la partecipazione attiva, la passione come motivazione, la condivisione delle conoscenze, il decentramento e la fiducia in un modello totalmente privo di autorità sono gli elementi su cui si basa questo progetto e che ne fanno a nostro parere una bel simbolo dell'ideale hacker del mondo come una comunità.

5 Conclusioni

Parlando di hacker abbiamo utilizzato più volte il termine "controcultura"; l'adeguatezza di questo concetto è stata spiegata bene da Federica Guerrini nel suo articolo "Gli Hacker come controcultura tra identità e rappresentazione" [37]. L'opposizione ai modelli sociali dominanti è portata avanti dagli hacker cercando di costruire un modello alternativo; si tratta di una comunità con un suo linguaggio, uno stile di vita, e soprattutto un insieme di valori forti e condivisi, differenti da quelli della cultura dominante.

Il rapporto con la società non è di sterile opposizione, nè di rinuncia; gli hacker sono creativi per definizione, hanno un rapporto privilegiato con le cose e sono portati per vocazione a risolvere i problemi ribaltando le situazioni e cercando sempre strade nuove e imprevedibili per agire sulla realtà. Sono consapevoli di avere in mano un'arma formidabile, il loro rapporto simbiotico con la tecnologia, e non vogliono rinunciare a usarla per affermare i valori che condividono. Per questo a loro dobbiamo molte invenzioni che hanno portato profondi cambiamenti nella società, come il personal computer, internet e il software libero.

Speriamo di aver mostrato che queste invenzioni non devono essere considerate come il frutto dell'ingegno di singoli personaggi, ma dell'attività di una comunità basata sulla condivisione, sul decentramento e sulla collaborazione; su un'etica in cui non c'è distinzione fra mezzi e fini, in quanto la libertà si esprime attraverso la creatività e la socializzazione, e la passione è il motore delle azioni di ciascuno.

La controcultura hacker è oggi più che mai viva, come abbiamo cercato di mostrare attraverso degli esempi di esperienze attuali che la incarnano, e tende a estendersi al di là dell'ambito in cui è nata, contagiando con i propri valori l'intera società.

Glossario

Assember: Programma che traduce in linguaggio macchina un programma scritto in linguaggio assembly. E' l'opposto di un disassembler.

Assembly: Linguaggio di programmazione di basso livello. Strutturalmente simile al linguaggio macchina, utilizza nomi convenzionali invece di codici di istruzioni ed etichette simboliche invece di locazioni di memoria.

Basic: Acronimo di "Beginner's All-purpose Symbolic Instruction Code", linguaggio di programmazione nato nel 1964. Ne sono state realizzate molte versioni differenti.

Baud: Unità di misura che indica il numero di valori che viene trasmesso in un secondo.

BBS: Acronimo di "Bulletin Board System", è un computer che utilizza un software per permettere a utenti esterni di connettersi ad esso attraverso la linea telefonica, dando la possibilità di utilizzare funzioni di messaggistica e file sharing centralizzato.

Browser: Un programma che fornisce uno strumento per navigare e interagire con i contenuti che si trovano nel World Wide Web.

CHIP: Componente di materiale semiconduttore su cui vengono miniaturizzati circuiti integrati con diverse funzionalità.

Client: Dispositivo o programma che, all'interno di una rete, viene utilizzato da un utente per contattare una sorgente di informazioni situata in un altro punto della rete, il *server*.

Codice sorgente: Insieme di istruzioni e dati utilizzati per implementare un algoritmo. Prima dell'esecuzione deve essere compilato con un compilatore.

Commodore: Nome con cui viene chiamata la nota "Commodore International", azienda statunitense di computer fondata nel 1955 da Jack Tramiel, che diede alla luce i primi esempi di personal computer: Commodore PET, VIC-20, Commodore 64 e la famiglia Amiga.

Compilatore: Programma informatico che traduce un linguaggio di alto livello in linguaggio macchina eseguibile.

Crackare: In gergo informatico, superare i dispositivi di sicurezza di un programma, di una rete, di un computer o di un dispositivo informatico in generale.

Ftp: Acronimo di "File Transfer Protocol", protocollo internet per lo scambio di file tra computer collegati in rete.

Geek: In gergo informatico, è un incrocio tra il "secchione" e lo "smanettone", per esteso chiunque sia molto appassionato di informatica.

KB: KiloByte, unità di misura della quantità di informazione elementare. E' pari a 1024 Byte.

LAN: Acronimo di "Local Area Network", rappresenta la rete locale costruita connettendo diversi computer all'interno di un ambito fisico delimitato.

Login: Sessione di un singolo utente, all'interno di una rete o di un computer multiutente. Per esteso il termine viene utilizzato per indicare il nome dell'utente e della sessione.

Mainframe: Computer multiutente generalmente utilizzati da grandi corporation come controllori di rete, di sistemi o gestori di banche dati.

Netstrike: Si tratta di un attacco informatico in cui, in generale, il besaglio viene avvisato che in forma di protesta un numero considerevole di utenti farà accesso al sito in un determinato giorno e ad una determinata ora. Se l'attacco ha successo (cioé se il numero di manifestanti è sufficiente) il sito diventa inaccessibile per chiunque voglia visitarlo.

Prompt: Messaggio inviato da un computer a una periferica (generalmente sul monitor) per informare l'utente che il sistema è pronto a ricevere un comando.

Ram: Acronimo di "Random Access Memory", è la memoria centrale volatile di un computer, utilizzata per l'esecuzione di programmi.

Script-kiddies: In gergo informatico, ragazzino o persona non molto competente che penetra o danneggia i sistemi solo per divertimento e senza alcuna etica morale.

Server: Computer che fornisce servizi a un'altro computer detto client o agli utenti della rete locale.

Sysadmin: In gergo, l'amministratore di un sistema. Il termine, dalle storiche BBS, viene utilizzato anche oggi.

Sysop: Vedi Sysadmin.

Unix: Sistema operativo multiutente nato nel 1969 nei Bell Labs per opera di Ken Thompson. E' alla base dello sviluppo di Linux.

Riferimenti bibliografici

[1] David Diamond Linus Torvalds. *Rivoluzionario per caso*. Garzanti, 2001.

[2] Steven Levy. *Hackers, Gli eroi della rivoluzione informatica*. ShaKe, 1996.

[3] Eric Steven Raymond. A brief history of hackerdom. http://catb.org/

[4] Free Software Foundation. Gnu. http://www.gnu.org.

[5] Free Software Foundation team. Free software foundation. http://www.fsf.org/.

[6] Free Software Foundation. Gnu general public licence. http://www.gnu.org/copyleft/gpl.html.

[7] Eric Steven Raymond. *The Cathedral and the Bazaar*. 2000.

[8] Andrea Monti Stefano Chiccarelli. *Spaghetti Hacker*. Apogeo, 1997.

[9] John Badham. Wargames, giochi di guerra, 1983. film.

[10] Willian Gibson. *Neuromancer*. Ace New York, 1984.

[11] Bruce Sterling. *The Hacker Crackdown*. 1992,1994.

[12] Pat Cadigan. *MindPlayers*. 1987.

[13] Peacelink. telematica per la pace. http://www.peacelink.it/.

[14] Hackmeeting team. Hackmeeting italiano. http://www.hackmeeting.org/.

[15] Eric Steven Raymond. How to become a hacker, 2001. http://www.catb.org/ esr/faqs/hacker-howto.html.

[16] The Mentor. The mentor's last words, 1986.

[17] Jean Baudrillard. *America*. Feltrinelli, 1988.

[18] trashitalia. http://trashware.linux.it/.

[19] Wikipedia. http://www.wikipedia.org.

[20] Angelo Raffaele Meo Mariella Berra. *Informatica Solidale*. Bollati Boringhieri, 2001.

[21] Eric Steven Raymond. The jargon file, 2003. http://www.catb.org/ esr/jargon/.

[22] Pekka Himanem. *The hacker ethic and the spirit of the information age*. 2001.

[23] Manuel Castells. *The rise of the Network Society*. Blackwell Publishers, 1996.

[24] Electronic frontier foundation. http://www.eff.org.

[25] John Perry Barlow. A not terribly brief history of the electronic frontier foundation. http://www.eff.org/pub/EFF/history.html.

[26] Electronic Frontier Foundation. Tor: An anonymous internet communication system. http://tor.eff.org/.

[27] Eric Steven Raymond. *Homesteading the Noosphere*. 1998.

[28] Daniel Aguayo Jeremy Stribling and Maxwell Krohn. Scigen project. http://pdos.csail.mit.edu/scigen/.

[29] Settimana della moda, 2005. http://www.settimanadellamoda.it/serpica.htm.

[30] Serpica naro home page. http://www.serpicanaro.com/.

[31] Rekombinant. operazione serpica naro. http://www.rekombinant.org/article.php?sid=2568.

[32] Tim O'Reilly. *Open Sources: Voices from the Open Source Revolution*. 1999.

[33] Jaromil. Hasciicam project. http://ascii.dyne.org/.

[34] Enrico Zeffiro Alvise Spanò. Polygen project. http://polygen.org/web/.

[35] Jeremy Rifkin. *The end oh the work: the decline of the global labour force and the dawn of the post-market era*. 1995.

[36] Jeremy Rifkin. *The Age of Access: The New Culture of Hypercapitalism Where All of Life Is a Paid-For Experience*. 2000.

[37] Federica Guerrini. Gli hacker come controcultura tra identità e rappresentazione. http://www.dvara.net/HK/hackcontrocultura.asp.