Università degli Studi di Roma “La Sapienza”
Facoltà di Sociologia
Cattedra di Teoria e Tecniche della Comunicazione di Massa

Corso di Laurea in
“Sociologia”

**HACKER: CURIOSITA' O CRIMINE?
IL FENOMENO IN ITALIA**

Candidato:

Marco Pennacchini

Matr. n. 897790

Anno Accademico 2003/2004

Relatore
Prof. Stefano Nobile

Correlatore
Prof. Marco Accorinti

*I do not believe in information,
I Just had to trust imagination*

INDICE

INTRODUZIONE	4
CAPITOLO 1 “RISCHIO E SICUREZZA”	7
1.1 Giù nel cyberspazio.....	7
1.2 Sistema sicuro.....	11
1.3 Riproduzione di massa	21
CAPITOLO 2 “GENERAZIONI”	29
2.1 Origine del fenomeno hacker tra passione e lavoro.....	29
2.2 La curiosità è un crimine?	37
CAPITOLO 3 “HACKER IN ITALIA”	54
3.1 Hacker e pirati.....	54
3.2 Dalle reti alla Rete	66
3.3 Evoluzioni.....	72
3.4 Intervista a Raoul Chiesa.....	76
CONCLUSIONI.....	83
<i>RINGRAZIAMENTI</i>	86
BIBLIOGRAFIA.....	87
WEBGRAFIA	90
DOCUMENTI VARI.....	92
SITI VISITATI.....	93
GLOSSARIO	94

INTRODUZIONE

La figura dell'hacker è da sempre circondata da un alone di mistero. Le varie rappresentazioni letterarie e cinematografiche lo hanno fatto immaginare come un ragazzo talentuoso in grado di fare qualsiasi cosa con il personal computer (si pensi a "Wargames" - di John Badham, MGM, 1983 - o ad "Hackers" - di Iain Softley, United Artists, 1995) oppure al "super uomo" che ci salverà dalla minaccia tecnologica (come lascia intendere la trilogia di "Matrix" dei fratelli Wachowski - Warner Bros, 1999-2004).

Riuscire a dare "la" definizione di "Hacker" è un'impresa ardua per via delle varie sfumature che dagli anni '50 ad oggi continuano a presentarsi.

Lo sperimentatore curioso dei primi elaboratori è divenuto il divulgatore della libera informazione negli anni 70 e si è trasformato, poi, nell'"oscura presenza" all'interno della rete dei giorni nostri. Ogni cambiamento, avvenuto principalmente in ambito informatico, seguiva o era accompagnato da mutazioni sociali importanti: la prima informatica americana degli anni '50 veniva supportata dal Ministero della Difesa in quella che è stata la guerra fredda; l'idea di libera circolazione delle informazioni venne fuori nel momento in cui si stavano sviluppando le comunità hippy e le rivolte studentesche cominciavano a scuotere il sistema sociale; infine l'avvento del "cyberspazio" ha portato alla conoscenza di un "mondo" praticamente infinito in cui l'individuo può virtualmente assumere tutte le personalità che desidera.

Proprio il cyberspazio, con i suoi pro e i suoi contro, ha portato alla ribalta il personaggio “hacker”, ora elevandolo a paladino della libertà (non solo) informatica, ora additandolo come principale causa dei mali della rete.

Basti pensare al problema della privacy e alla violazione del copyright: tutte questioni esplose dopo l'avvento della rete e che, volente o nolente, vedono gli hackers nel ruolo dei protagonisti.

Da una parte la comunità hacker ammette la propria indiscriminata curiosità, dall'altra le stesse persone vengono indicate come criminali.

La curiosità, quindi, può tradursi in un crimine?

Nei tre capitoli di questo lavoro si tenterà di trovare una risposta a questa domanda, o meglio, di verificare se tale questione può essere posta.

Il cyberspazio, la sua formazione e le varie teorie che nel tempo hanno cercato di darne una definizione esatta, sarà il tema centrale del primo capitolo, il quale si estenderà, poi, nell'esame di due odierne “paure tecnologiche” come la protezione della privacy e la violazione del diritto d'autore.

Nel secondo capitolo verrà affrontata la storia degli hackers in ambito statunitense, ovvero dove il fenomeno ha cominciato ad esistere. Non verrà presentata soltanto una ricostruzione storica, ma si terrà conto dell'evoluzione dell'ideologia hacker e di come questa figura abbia influito non solamente nella storia informatica ma anche nelle mutazioni sociali.

Con l'uso di vari aneddoti e l'esposizione del caso “Sundevil” il quale, nei primi anni '90, vide una serie di arresti nell'ambiente underground informatico statunitense, si darà una definizione del personaggio “Hacker” facendo notare come esistano innumerevoli sfumature che vanno dall'anarchico innovatore dei sistemi informatici fino all'intruso della rete.

Il fenomeno hacker in Italia è il tema del terzo capitolo nel quale, anche grazie ad un intervento di Raoul Chiesa – personaggio di spicco del panorama hacker italiano – si esaminerà l’evoluzione della scena hacker nostrana e i suoi rapporti con la stampa e la legge.

Importante per capire la caratterizzazione odierna dell’hacker sarà l’analisi dell’operazione di polizia “Hardware I” del 1994 che provocò un vero e proprio terremoto nell’ambiente – non solo informatico – italiano, destinato a essere ricordato come la più massiccia operazione di sequestri di servizi telematici al mondo.

Nello strutturare un profilo dell’hacker italiano si darà importanza non solo all’aspetto informatico ma, soprattutto, alle caratterizzazioni sociali che il personaggio ha preso negli anni, rendendolo una figura affascinante e di difficile comprensione.

CAPITOLO 1 “RISCHIO E SICUREZZA”

“Adesso era lunga e difficile la strada per tornare a casa, allo Sprawl, dall’altra parte del pacifico, e lui non era tipo da console, non era un cowboy del cyberspazio.”

W. Gibson, “Neuromante”

1.1 Giù nel cyberspazio

È bastata una sola parola per identificare moltissime persone: Cyberspazio. Il termine, coniato nel 1984 dallo scrittore americano William Gibson¹, è importante non soltanto per l’elemento identificante ma, soprattutto, perché arrivò in un’epoca in cui il personal computer e la rete erano ben lontani dall’essere affermati su larga scala.

Trovare una definizione esatta del cyberspazio è molto complicato perché, come per il termine “Hacker” che si esaminerà in seguito, ne esistono molte, tutte in un certo modo complementari.

Prendendo come base per la comprensione lo “Jargon File”², vero e proprio dizionario informatico-sociale presente in Internet, si arriva alla formazione di tre possibili caratterizzazioni della nuova struttura:

- Una prettamente fantascientifica che intende per cyberspazio la matrice o “information-space” che si apre durante una connessione

¹ William Gibson, “Neuromante”, Milano, Mondadori, 2003.

² Eric S. Raymond – “The Jargon file”, documento in perenne aggiornamento all’interno del quale si trova il dizionario dell’hacker. Qui si fa riferimento alla versione 4.4.2 del 22 maggio 2003.

con elettrodi installati nel corpo umano. Semplificando si può pensare ad un odierna connessione ad Internet.

- Una valida alternativa al mondo reale così come suggerito, ad esempio, dal film “Matrix”³. Tale rappresentazione fu molto usata durante gli anni del netbang, ossia dell’aumento esponenziale delle connessioni ad Internet.
- La situazione in cui si trova un hacker durante una sessione di hacking.

Pur rimanendo valide tutte e tre, la prima definizione sembra la più vicina alla realtà. Il cyberspazio è un non-luogo, in quanto non esistente fisicamente, nel quale domina la comunicazione orizzontale, non gerarchica e interattiva, in cui non c’è una divisione netta tra emittente e destinatario del messaggio.

Siamo di fronte ad un nuovo passo del processo di demassificazione dei media teorizzato da Alvin Toffler, il quale afferma che i nuovi mezzi di comunicazione, in questo caso la rete, il cyberspazio, propongono un modo di comunicare diverso rispetto ai media tradizionali. Non troviamo più un messaggio unico e non modificabile, ma una serie di informazioni continuamente analizzate e discusse.

Pierre Levy nel suo libro “L’intelligenza collettiva”, parla del cyberspazio come di un sapere distribuito ovunque, continuamente valorizzato, coordinato in tempo reale tramite l’uso di strumenti digitali, che porta una mobilitazione effettiva delle competenze⁴.

³ “Matrix”, dei fratelli Wachowski, Warner Bros, 1999.

⁴ Pierre Levy, “L’intelligenza collettiva. Per un’antropologia del cyberspazio”, 1994, Milano, Feltrinelli.

Appunto per questo è opportuno precisare che risulta necessario colmare al più presto il “digital-gap” esistente tra le nazioni con alto tasso di tecnologizzazione e quelle rimaste indietro, perché, Levy lo ribadisce, l’intelligenza collettiva è formata da tutta l’umanità⁵: “lo sviluppo di Internet non sfugge alle logiche sociali e al divario tra ricchi e poveri, in termini sia di contenuto che di accesso alle informazioni.” (Alain Gresh, in Carlo Gubitosa, “Oltre Internet”, documento on-line, 1996).

Ma il “gap” non è soltanto tra ricchi e poveri: analizzando il Rapporto 2004 Censis “XXXVIII – Rapporto sulla situazione sociale del paese” si rileva che in Italia quasi tre persone su quattro non si connettono mai a Internet, e alla domanda sul perché accade questo il 74% risponde che non usa Internet in quanto non sa usare il computer. Dallo stesso rapporto si evince un uso “ridotto” della rete, basti considerare che la maggioranza degli intervistati, 60.6%, si connette ad Internet solamente per scaricare la posta elettronica⁶.

Generalizzando si può affermare che gli individui quando sono all’interno del cyberspazio accomunano sensazioni e valori formando una “coscienza collettiva”⁷, ampliandone, però, il significato rispetto al concetto originario di Emile Durkheim.

Siamo molto vicini a McLuhan e al suo “villaggio globale” dove i nuovi media sono riusciti a cancellare i confini geografici e l’essere umano sta

⁵ Pierre Levy, conferenza presso il CTM di Milano del 14 novembre 1996. Tratto da “Decoder” n° 11, Shake ed.

⁶ Rapporto 2004 Censis “XXXVIII – Rapporto sulla situazione sociale del paese”. Documento consultabile on-line all’indirizzo www.censis.it

⁷ Emile Durkheim, “La divisione del lavoro sociale”, Edizioni di Comunità, Milano, 1971, in Ruth Fallace, Alison Wolf, “La teoria sociologica contemporanea”, Il mulino, Bologna, 2000.

vivendo un processo di ritribalizzazione nel quale il sapere è vissuto collettivamente così come i miti dell'uomo antico⁸.

In alcune opere cyberpunk, filone fantascientifico "figlio" delle nuove tecnologie, si pensa al cyberspazio come ad una valida alternativa del mondo reale. Tornando alla citazione di inizio capitolo, nel "Neuromante", il protagonista Case, impossibilitato alla connessione si sente prigioniero del proprio corpo.

Seguendo questa filosofia, arriveremo in un futuro in cui l'individuo dovrà avere una doppia personalità: quella reale e quella per il cyberspazio, ossia si avvererà la teoria di Timothy Leary secondo il quale l'uomo diventerà un "anfibia culturale", abituato a vivere in entrambe i mondi⁹.

Come si può notare si parla di vere e proprie realtà alternative dove non solo ci si rifugia per qualche momento ma per vivere come nella realtà quotidiana.

Il Metaverso di "Snow Crash"¹⁰ è una copia della realtà nel quale non si può, ad esempio, teletrasportarsi perché tale processo non si può effettuare nella realtà materiale. Ci sono addirittura dei parchi di divertimento da usare come "svago nello svago".

Oltre all'identità corporea, quindi, l'individuo connesso al cyberspazio ha sviluppato un'identità digitale. Basti pensare, per fare un esempio molto semplice, all'avatar¹¹ e ai nick-name usati in Internet.

⁸ Anna Carola Freschi e Laura Leopardi, "Una ragnatela sulla trasformazione", Firenze, City Lights Italia, 1998.

⁹ Timothy Leary, "Caos e cibercultura", Apogeo-Urra.

¹⁰ Neal Stephenson, "Snow Crash", Milano, Shake edizioni, 1995.

¹¹ L'Avatar è una sorta di clone digitale dell'individuo che permette la partecipazione all'interno dei forum di discussione sulla Rete.

Il cyberspazio permette l'esistenza di grandi sistemi, come quello finanziario e commerciale, con lo scopo di facilitare la comunicazione trasparente tra utente e sistema. Allo stesso tempo questo tentativo di linearità convive con il caos, rendendo il cyberspazio "un labirinto più terribile di quello di Dedalo"¹².

Essendo quest'ultimo aspetto quello più curato dai media tradizionali quando si parla di Internet e dei suoi contenuti, alcuni politici e legislatori, non avendo una conoscenza diretta della cybercultura e una visione mediata dai mass-media, sono spinti da una naturale paura a tentare di controllare e stringere il campo d'azione del cyberspazio.

1.2 Sistema sicuro

In molte affermazioni fatte da giornalisti, politici e legislatori permane la convinzione che il cyberspazio sia una realtà de-responsabilizzata dalle norme del diritto e rispondente solamente a regole interne, come la Netiquette, e ai vari codici di auto-regolamentazione dei gruppi di comunicazione elettronica¹³.

La Netiquette è un documento nato nella seconda metà degli anni 90 dalla collaborazione dei primi gestori della neo-nata Internet, all'interno del quale ci sono delle regole che, in teoria, dovrebbero essere rispettate da tutti i navigatori¹⁴.

¹² Pierre Levy, conferenza presso il CTM di Milano del 14 novembre 1996. All'interno del suo intervento, Levy parla anche del cyberspazio come "Sistema di sistemi". Tratto da "Decoder" n° 11, Shake ed.

¹³ Su queste posizioni si basa l'intervento di Marco Calamari durante l'E-privacy 2004 tenutosi a Firenze.

¹⁴ "Netiquette", © Arlene Rinaldi & Florida Atlantic University, 1995-96.
<http://wise.fau.edu/netiquette/net/index.htm>

Ad esempio:

- Non userai un computer per danneggiare altre persone.
- Non userai o copierai software che non hai pagato.
- Non spedite mai catene di Sant'Antonio (chain letters) su Internet. Il farlo potrebbe causare la perdita dell'accesso.

Le raccomandazioni continuano fino all'ultima sezione in cui c'è un vero e proprio decalogo per un uso etico del personal computer.

Riflettendo sul contenuto della Netiquette si arriva alla conclusione che la maggior parte delle regole in essa contenute è “regolarmente” violata, altrimenti non si spiegherebbe l'utilità del documento presente sul sito della Polizia di Stato “I consigli della Polizia di Stato a tutti i navigatori”, nel quale, con un'insistenza inquietante, si consiglia di stare attenti a tutto ciò che avviene durante una navigazione.

Questo a conferma del detto circolante tra gli appassionati di informatica: “Il computer più sicuro è spento e disconnesso dalla rete”. Al giorno d'oggi tale affermazione non sussiste, visto che essere connessi alla rete è diventato un “must” per tutti.

Possiamo leggere il giornale, prenotare una vacanza, fare la spesa e avere rapporti sociali stando comodamente seduti in casa. Ma più la tecnologia entra nella nostra casa e nelle nostre vite, più noi lasciamo tracce. Le informazioni che cediamo il più delle volte sono le nostre generalità che, comunque, non ci curiamo di come vengano trattate.

Nel 1999, ad esempio, un provider¹⁵ italiano cominciò ad offrire l'accesso alla rete gratuito ma con una clausola poco chiara all'interno del contratto

¹⁵ Ved. Glossario.

offerto. L'accordo prevedeva la cessione da parte dell'utente dei propri dati personali con l'inclusione di questi ultimi all'interno di un database accessibile a molte società commerciali.

Accesso gratuito a patto di vedere sul monitor messaggi pubblicitari.

In modo analogo agiscono i software "Spyware". Considerati alla stregua di un virus, questi programmi si installano all'interno del computer e "spiano" tutto quello che avviene durante una navigazione su Internet. I dati raccolti vengono poi inviati a varie società che forniscono pubblicità mirata durante i "viaggi nel cyberspazio".

Mantenere una riservatezza durante una connessione alla rete è molto difficile, perché non sono soltanto i software maliziosi¹⁶ a violare la nostra privacy, ma altri mezzi già inseriti all'interno del computer come ad esempio i file log¹⁷, veri e propri cervelli automatici che registrano ogni operazione compiuta con il personal computer. Questi files hanno una doppia faccia: da una parte tracciano ogni nostra attività ma dall'altra, proprio per questa funzione, registrano anche eventuali intrusioni.

Un metodo per ovviare al controllo delle nostre attività potrebbe essere quello di utilizzare strumenti alternativi e poco conosciuti (e pubblicizzati) come "Freenet", progetto di rete alternativa e anonima, o alcuni anonymous remailer che permettono l'invio di e-mail in modo anonimo e cifrato¹⁸.

Lo scenario delineato sembra non lasciare molto speranza alla privacy dell'individuo che usa tranquillamente il suo computer; si pensi anche al progetto statunitense di inserire all'interno dei software di cifratura i

¹⁶ Con questo aggettivo si intendono i software che hanno funzioni nascoste.

¹⁷ Ved. Glossario.

¹⁸ L'Italia è una nazione molto impegnata in questo campo. Per dettagli www.winstonsmith.info

cosiddetti “Clipper chip”, ossia fare in modo che il governo degli Stati Uniti abbia la priorità nel decifrare i messaggi cifrati scambiati da chiunque.

Dov’è , quindi, il confine tra privacy e sicurezza?

La questione sorge ben prima dell’11 settembre ma è divenuta rilevante solamente dopo i tragici fatti di quella giornata. Noi siamo le nostre informazioni e, sempre di più, la nostra identità è ricomponibile attraverso le tracce, elettroniche e non, che lasciamo.

Quindi, oltre ad aver bisogno della tutela del nostro corpo fisico, sentiamo anche l’esigenza di proteggere il nostro nuovo corpo elettronico.

Una riformulazione della precedente domanda la fa il presidente del garante per la protezione dei dati personali Stefano Rodotà in un articolo de “La Repubblica” del 10 Giugno 2002: può la privacy sopravvivere nell’era del terrore?

C’è il pericolo che dietro la promessa di maggiore sicurezza ci sia la seria minaccia di essere monitorati in ogni momento con il rischio di sentirci veramente sicuri solamente all’interno dei nostri spazi privati, avendo un’immagine ostile del mondo esterno: Robert Heinlein, uno dei maggiori scrittori di fantascienza, una volta disse che l’unica conseguenza di qualsiasi legge sulla privacy è di rendere più piccole e più invisibili le microspie e le altre tecnologie di controllo.

Un elevato sviluppo tecnologico può portare a due conseguenze dal punto di vista del diritto: una in cui c’è una lentezza nell’adeguamento legislativo, con conseguente aumento di crimini, legati ai nuovi mezzi a disposizione, non puniti o addirittura non denunciati. Questo provoca insabbiature di eventuali intrusioni all’interno delle reti aziendali e, in casi frequenti, l’assunzione di ex-hacker come responsabili della sicurezza informatica

dell'azienda¹⁹. Il secondo caso è di un aumento senza logica di norme e leggi provocato dal timore verso le nuove tecnologie.

Berners-Lee, creatore del sistema web, intuì tempo fa questa situazione accusando le autorità di aver lasciato diventare Internet un mezzo di comunicazione troppo grande per essere controllato²⁰.

Ma non serve controllare il cyberspazio, “bisogna strutturare leggi per Internet senza tentare di colonizzarla”²¹.

La rete nacque con l'intento di essere un mezzo di comunicazione senza censure all'interno del quale ognuno cercava l'informazione di cui aveva bisogno, quindi è probabile che ogni tentativo di chiudere gli sbocchi alle informazioni su Internet, provochi l'effetto contrario.

Bisognerebbe trovare adeguate soluzioni per il trattamento delle informazioni sensibili perché “Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata²²”.

Nel cyberspazio tutte le attività sono tracciate, e tutto quello che non viene seguito per legge o per scelta commerciale potrebbe, comunque, essere tracciato e conservato. I dati diventano un importante merce di scambio e, con gli attuali mezzi per raccogliervi e conservarli, la quantità di tali

¹⁹ Anche se molti non sono d'accordo sull'assunzione di ex-hacker. Marco Strano parla della “reale affidabilità a lungo termine di tali soggetti e sulla rapida obsolescenza delle loro conoscenze una volta abbandonato il mondo dell'hacking attivo”. (Marco Strano, “La psicologia degli hackers”, ICT security 2003, documento on-line sul sito www.criminologia.org).

²⁰ Articolo su www.repubblica.it dal titolo “Internet devasta la privacy”, del 16/04/1998.

²¹ Intervento di Marco Calamari durante l'E-privacy 2004 tenutosi a Firenze.

informazioni è enorme in quanto si incrociano le raccolte automatiche con quelle non permanenti.

Si comprende facilmente che la protezione dei nostri dati sensibili è un problema molto serio che va affrontato sia per quanto riguarda la sfera pubblica, come la video-sorveglianza, la rete GSM ed altri momenti in cui le nostre informazioni vengono trattate da altri, sia per i dati inseriti all'interno del personal computer.

Al giorno d'oggi esistono numerosi mezzi per la protezione dei dati all'interno del computer: firewall, antivirus e l'uso di password sono soltanto pochi esempi.

Si ritiene, però, che bisognerebbe raggiungere una maggiore consapevolezza da parte dell'individuo per la sicurezza dei propri dati perché, citando Kevin Mitnick: "Gli individui possono seguire le migliori tattiche consigliate dagli esperti, installare supinamente tutti i prodotti raccomandati (...) ed essere ancora totalmente vulnerabili." (Kevin D. Mitnick in collaborazione con William L. Simon, "L'arte dell'inganno, i consigli dell'Hacker più famoso del Mondo", Milano, Feltrinelli, 2003, pag. 23).

Questo a significare che l'anello più debole della catena, per quanto riguarda la sicurezza, è l'uomo, perché sta a lui installare software, configurare personal computer e scegliere le password. Se una di queste operazioni è compiuta con scarsa apprensione si rischia di aprire letteralmente il proprio computer ad altri.

²² Brano tratto dalla Nota direttiva 2002/58/CE del parlamento europeo e del consiglio. Integrata nel D.L. 196/2003 "Testo Unico sulla Privacy".

Qualche anno fa una società telefonica italiana fece una campagna pubblicitaria recitante lo slogan “Richard Kust, Hacker: e pensate di fermarlo con una password?”.

In tempi recenti hanno creato, e continuano a creare, scalpore casi di bollette del telefono elevate a causa dei Dialer, ossia software che, una volta installati all'interno del computer, connettono quest'ultimo alla rete tramite un numero telefonico a costo altissimo. È bene precisare che la maggior parte di questi programmi non si installano automaticamente ma devono essere scaricati dall'utente.

Si ritorna, quindi, al discorso fatto in precedenza del bisogno di una maggiore consapevolezza da parte di chi usa il computer. Basterebbe leggere tutto quello che ci compare sui monitor durante una navigazione ed evitare determinati siti, per non cadere nelle trappole.

Di casi che sfruttano le distrazioni degli individui per ricavarne informazioni ce ne sono molti.

Nel Natale 2001, ad esempio, molti clienti statunitensi del servizio PayPal, il quale permette di pagare merce a distanza con addebito in carta di credito, si videro arrivare una mail per una nuova registrazione al servizio. La particolarità di questo messaggio era quella di contenere un link ad una pagina web molto simile a quella di PayPal, ma non quella autentica. Molti, fortunatamente non tutti, risposero a questa registrazione ed inserirono tranquillamente i propri dati personali e il numero della loro carta di credito. Questo avvenne perché pochi si presero la briga di controllare l'esatto indirizzo contenuto nell'e-mail e ancora meno furono quelli che controllarono se, al momento della registrazione, la connessione alla pagina web era protetta²³.

²³ Tale tecnica è conosciuta con il nome di “Phishing”.

Tecniche come questa vengono inserite all'interno della cosiddetta ingegneria sociale ossia un insieme di strategie per ingannare gli individui e rubare informazioni, oppure, usando le parole di Mitnick: "Uso del proprio ascendente e delle capacità di persuasione per ingannare gli altri." (Mitnick, 2003, pag. 9).

Le informazioni, personali e non, oggi sono una merce preziosa e, quindi, più si è abili nell'ingegneria sociale e più se ne ricava.

Il fatto che negli ultimi anni molte aziende abbiano aperto dei corsi di addestramento del personale contro l'ingegneria sociale e che in molti corsi di informatica ci siano sezioni dedicate all'argomento, dà un quadro abbastanza chiaro di come il problema della sicurezza dei dati sia molto sentito non soltanto a livello strettamente personale ma anche a livello aziendale.

Significativo è il recente sondaggio "Eurobarometro – Data Protection" incentrato sulle opinioni, i livelli di informazione e gli atteggiamenti dei cittadini europei relativi al problema della protezione dei dati, all'interno del quale il 77% degli italiani ritiene che la consapevolezza del problema della protezione dei dati personali sia bassa nel suo paese, il 63% è preoccupato di lasciare i propri dati in Internet e un desolante 25% ritiene che la legislazione nazionale possa far fronte ai problemi di protezione dei dati derivanti dalla crescita del numero delle persone che lasciano le proprie informazioni personali in Internet²⁴.

²⁴ Eurobarometro, Data Protection. Rilevazione Settembre 2003, Pubblicazione dati Dicembre 2003. Dettagli della ricerca su www.cambio.unifi.it, laboratorio di ricerca sulle trasformazioni sociali dell'Università degli studi di Firenze.

La questione della protezione della privacy è al centro del sondaggio “Gli italiani lo sanno: siamo già tutti a rischio” comparso nell’estate del 2003 sulla rivista “SuperQuark” n°31²⁵.

Tra le altre, comparivano le seguenti domande:

PER LEI E' IMPORTANTE LA DIFESA DELLA PRIVACY?	
Molto	71%
Abbastanza	24%
Poco	3%
Per nulla	1%
Non indica	1%

QUALE SOLUZIONE AL PROBLEMA DELLA VIOLAZIONE?	
Maggior prudenza	29%
Leggi più severe	26%
Nuovi sistemi tecnologici	20%
Vietare scambi di informazioni	9%
Controllare Internet	8%

²⁵ Sondaggio condotto dalla CIRM per Quark su un campione di 950 intervistati. Il documento è scaricabile on-line all'indirizzo:
www.raiuno.rai.it/static/immagine/superquarkdossiersondaggio31.pdf

Non è importante	2%
Non indica	6%

Praticamente, da una parte si ammette l'importanza della difesa della privacy ma dall'altra ci si autoaccusa di essere poco prudenti nel lasciare informazioni personali.

PER COSA RINUNCEREBBE IN PARTE ALLA PRIVACY?	
Per la sicurezza di tutti	36%
Per tutelare la salute di tutti	19%
Per tutelare la propria salute	12%
Per la ricerca scientifica	6%
Per avere migliori servizi	4%
In nessun caso	19%
Altro	1%
Non indica	3%

Analizzando queste risposte si nota come quasi il 40% degli intervistati rinunciarebbe alla privacy per la sicurezza di tutti (ma senza limiti?), mentre il 19% rifiuta categoricamente ogni compromesso.

Come per l'”Eurobarometro” visto in precedenza, anche in questo sondaggio l'ultima domanda lascia l'amaro in bocca:

OGGI LA SUA PRIVACY PUO' ESSERE VIOLATA?	
Certamente si	34%
Probabilmente si	44%
Certamente no	3%
Probabilmente no	16%
Non indica	3%

Come si può notare, quasi l'80% degli intervistati è consapevole che la privacy viene violata: sarebbe stata utile un'ulteriore domanda che indagasse su chi, secondo gli intervistati, viola la privacy per dare, così, un'immagine chiara al posto dello “spettro” del “Grande Fratello”.

1.3 Riproduzione di massa

La rivoluzione digitale che stiamo vivendo da circa venti anni e che, probabilmente, non si fermerà mai, ha portato fino ad ora mutamenti rilevanti nell'ambito individuale mentre sembra ancora scarsa l'apprensione da parte della legge.

I fattori che determinano questa situazione storica sono molti, tutti riguardanti il nuovo modo di produrre e divulgare informazione. La facilità di duplicazione delle opere digitali e la conseguente facilità di trasmissione, sono gli elementi più importanti, che uniti ad altri, i quali possono essere la

compattezza dell'opera digitale e la sua malleabilità, rappresentano una sfida per l'attuale legislazione, non solo italiana, riguardante il copyright.

Soffermandoci sul primo fattore, la facilità di duplicazione, possiamo capire come siamo di fronte ad una situazione ambigua. Da una parte quasi quotidianamente vengono lanciati sul mercato prodotti per la duplicazione sempre più veloce di opere, dall'altra la legislazione sul copyright tende a perseguire la diffusione di materiale copiato senza autorizzazione. L'ideologia della duplicazione si è estesa nella società grazie ai nuovi mezzi di comunicazione e il ritenere che sia legale in ogni caso è consuetudine tra gli utenti.

La questione dei diritti d'autore è sempre stata centrale all'interno dell'etica hacker, correlata con la libertà di sperimentare sui programmi ma i contrasti con i grandi produttori di software sono enormi. Nella licenza di "Microsoft Windows Xp Professional edition", ad esempio, si legge che non si ha la possibilità di fare reverse engineering²⁶ sul prodotto e, soprattutto, se Microsoft cancella il contratto di licenza si è obbligati a "distruggere tutte le copie del prodotto e i suoi componenti"²⁷.

Ciò che si evince è che, in realtà, acquistando un programma per computer, non si acquista il software ma la sua licenza d'uso: non si è proprietari, ma utenti.

La libertà di sperimentare è ribadita nella licenza alternativa "GPL" creata da Richard Stallman e dalla sua fondazione per il software libero.

²⁶ La tecnica del Reverse Engineering permette di rendere leggibile (aprire) il codice di un programma chiuso (compilato).

²⁷ Contratto di licenza EULA. Microsoft Corporation. Il file si trova all'interno di ogni computer in cui è installato un sistema "Microsoft Windows".

Pur avendo posto un copyright sui programmi, la fondazione garantisce la libera distribuzione, lettura ed eventuale modifica di parte o di tutto il software da parte degli acquirenti²⁸.

Un probabile accordo tra chi porta avanti la filosofia del software libero e le grandi aziende produttrici di programmi è ben lontano e poco probabile. Basti considerare le due seguenti dichiarazioni per appurarlo:

“Era la prima volta che mi imbattevo in una clausola di non divulgazione, e mi resi conto immediatamente come questi accordi producano delle vittime. In questo caso la vittima ero io. Io e il mio laboratorio.” (Richard Stallman in “Codice libero”, Sam Williams, Febbraio 2003, edizione on-line sul sito www.apogeeonline.com):

“Due decenni di esperienza hanno dimostrato come un modello economico capace di tutelare la proprietà intellettuale e un modello commerciale in grado di recuperare gli stanziamenti per la ricerca e lo sviluppo, siano in grado di creare notevoli benefici economici e di distribuirli in maniera assai ampia.” (Craig Mundie, vicepresidente Microsoft, conferenza sul futuro del software libero, 2001)²⁹.

Strettamente correlato a questo dibattito è il tema del furto. Considerare l'informazione, in una sua caratterizzazione generale in cui si inseriscono anche le opere digitali, come una forma di proprietà permette, a chi lo vuole, di rubarla. Ma rubare è privare qualcuno del godimento di un bene e quindi, usando le parole di John Barlow, “se io rubo la vostra informazione, voi ce l'avete ancora. Se rubo il vostro cavallo, voi non potete più cavalcare.”

²⁸ La licenza è raggiungibile sul sito www.gnu.org.

²⁹ L'intero intervento è consultabile alla pagina www.microsoft.com/presspass/exec.craig/05-03sharedsource.asp

(John Barlow, "Proteggere la bottiglia, non il vino", tratto da "Cyberart", Miller Freeman INC, San Francisco, 1992. Traduzione in italiano in "No Copyright", Shake edizioni, Milano, 1994, pag. 125).

La posizione può sembrare troppo radicale ma è riferita al diritto dei programmatori di vedere e, possibilmente, modificare parti di un software.

Il perno della questione rimane il fatto che prendere un programma per computer, scambiarlo con altri, modificarlo e distribuirlo, per l'ambiente hacker è un comportamento modello ma per l'industria informatica è l'esempio tipico di pirateria.

La produzione di software è un settore dell'economia che fattura miliardi di dollari l'anno. Per questo, mantenere un controllo sulla pirateria e sugli abusi è fondamentale per i grandi produttori.

La BSA, Business Software Alliance, ha proprio questo compito: far sì che la legislazione venga rispettata ed ogni violazione denunciata. La società è stata creata negli Stati Uniti da varie aziende informatiche come Microsoft, Lotus Development ed Apple, e lavora nel nostro paese in collaborazione con l'associazione italiana per la tutela del software.

Un mutamento nell'attuale legislazione e gestione del copyright è necessario, per adeguare il diritto ai nuovi media e non viceversa come si sta già facendo.

Dimostrazione di quanto detto è l'attuazione, prima negli Stati Uniti e poi in Europa, della direttiva riguardante i brevetti nel campo della programmazione per computer. Il provvedimento introduce i sistemi DRM (Digital Rights Managements, gestione dei diritti di copia delle opere digitali) che permettono il controllo dell'uso che si fa dell'opera. Questo

fatto limita considerevolmente la libera programmazione. Un software usa varie tecniche e fornisce numerosi risultati che potrebbero violare numerosi brevetti. Una piccola società informatica non sarebbe in grado di affrontare spese legali o di acquistare brevetti come, invece, fanno le grandi società che comprano brevetti per ovviare alle loro violazioni.

Sempre di più l'individuo diventa utente e non proprietario del suo programma.

Il 22 dicembre 2003 si è chiusa in Norvegia con una assoluzione il processo a Jon Johansen, accusato di aver aggirato la protezione inserita nei DVD e di aver creato un software, DeCssh, che, oltre ad aggirare la protezione suddetta, rendeva visibile il contenuto del DVD su sistemi operativi alternativi.

Anche se dalla parte dell'accusa c'era la DVD-CCA, società americana che racchiude la maggior parte dei produttori cinematografici di Hollywood, è stata emessa una sentenza di assoluzione perché i DVD su cui era avvenuta la sperimentazione erano di proprietà del ragazzo norvegese, quindi era legittimo che li usasse come voleva.

L'esaltazione dei nuovi strumenti per il controllo e la protezione dei dati sarà l'implementazione all'interno del computer del sistema "Palladium" in grado di monitorare ogni operazione compiuta e di evitare l'uso di software non acquisito regolarmente compresi i file multimediali senza licenza come i musicali Mp3.

Proprio questi ultimi hanno acceso la battaglia di diritti tra utenti e l'industria musicale sempre per questioni di copyright.

Shawn Fanning entrerà nella storia del cyberspazio perché è stato il primo che con il suo sistema di scambio file musicali Mp3 ha tentato di scuotere il

mondo rigido dell'industria musicale. Napster, la sua creatura, vide la luce nel 1999, quando Fanning era poco più di un adolescente, e in breve tempo divenne uno dei software più usati dagli utenti internet³⁰.

Il sistema escogitato per scambiarsi i file era molto semplice. Con un'interfaccia grafica molto intuitiva si poteva cercare una canzone e scaricarla in breve tempo (a seconda della connessione posseduta) da un altro computer.

Di fatto Napster non aveva file Mp3 installati al suo interno, ma aiutava lo scambio tra utenti. Il gruppo rock dei Metallica si accorse che, comunque, anche se non direttamente, questo sistema di scambio violava il copyright e per questo Fanning venne denunciato dalla R.i.a.a. (Recording industry association of America, la società americana che gestisce i diritti d'autore, al pari dell'italiana S.I.A.E.) e dopo un lungo processo si accordò con varie case discografiche per permettere il download a pagamento di brani musicali scelti dalle major.

Fu una vittoria schiacciante per l'industria musicale che, però, ha portato ad un risultato inaspettato: se prima esisteva solamente Napster e lo scambio di file musicali, oggi siamo davanti ad un proliferare di software per la condivisione di file che vanno dalla musica, ai film fino ad arrivare ai libri.

Ultimamente ci sono vari tentativi per uscire dal "sommerso" della pirateria e del download selvaggio: Steve Jobs della Apple ha inventato un metodo per scaricare migliaia di canzoni a costi bassissimi, molti artisti stanno cominciando a pubblicare i loro dischi direttamente su Internet e c'è un sensibile aumento di software freeware, i quali possono essere usati gratuitamente o versando una somma all'autore decisa dall'utente.

³⁰ Si stima che dal 1999 al 2001, anno della chiusura del periodo gratuito, più di 60 milioni di persone abbiano usato Napster.

La suddetta situazione dimostra che il cyberspazio contiene, oltre ad elementi che causano problemi con la legge, anche fattori che risolvono le questioni causate.

Questo ci porta ad una riflessione ben precisa. Ogni volta che si è provato a chiudere, censurare e, passi il termine, colonizzare il cyberspazio, si è ottenuto l'effetto contrario. Sarebbe quindi utile mostrare, oltre al bastone, anche una piccola porzione di carota, intendendo con questa metafora che tentativi di regolamentare in maniera troppo rigida la rete hanno provocato scarsi risultati per la poca collaborazione nella costruzione dei provvedimenti con gli utenti.

Recentemente in Italia ha creato scalpore la chiusura di numerosi siti a causa del decreto-legge n° 72/2004, voluto dal ministro dei beni culturali Giuliano Urbani e per questo più conosciuto come “decreto Urbani”. Tale decreto ha l'obiettivo di porre un freno al download di materiale illegale.

Nel testo, che visto l'argomento spinoso, è ancora in fase di perfezionamento, si istituisce sia la responsabilità oggettiva per i provider che hanno anche l'obbligo di controllare ed eventualmente denunciare i propri clienti, sia il pagamento di un equo compenso sui supporti vergini che, ragionando per paradossi, renderebbe legale il materiale scaricato³¹.

In pratica da una parte si afferma che la copia privata è legale visto il pagamento della “tassa” sui supporti vuoti, ma dall'altra parte il decreto dichiara che se tale copia è eseguita da remoto, allora si commette un illecito.

³¹ Testo consultabile on-line all'indirizzo www.alcei.it/documenti/copyright/dlp2p0472.htm

Una contraddizione, non l'unica, che poteva essere evitata se ci fosse stata, probabilmente, una maggiore collaborazione tra chi deve scrivere la legge e chi deve rispettarla.

C'è il pericolo che le regole non solo non vengano rispettate ma addirittura aggirate con consapevolezza. Al momento della chiusura preventiva del sito www.fastsharing.it, è comparsa sulla pagina iniziale una comunicazione da parte del gruppo che gestiva il sito nella quale oltre ad esaminare i motivi della chiusura, elencava varie raccomandazioni degne di una "guerriglia", come ad esempio: non comprare DVD, CD, non andare al cinema, fai contropubblicità, non abbonarti a servizi internet e così via³².

Questo è il vero pericolo di provvedimenti presi troppo in fretta, con scarsa apprensione sul problema affrontato e con la tendenza a restringere le libertà piuttosto che ad allargarle. Molto spesso si legge della preoccupazione riguardo la troppa esaltazione delle libertà di Internet, giustificando tali dichiarazioni con il rischio di perdere contenuti e di "svuotare" la rete.

C'è il rischio, invece, di creare un circolo vizioso troppo difficile da controllare, in cui è ancora più complicato prendere una posizione netta.

I nuovi problemi derivati dalla rete come il copyright e la privacy devono essere affrontati da tutti, poteri forti ed individui-utenti, con la consapevolezza delle mutazioni continue nella società che la rivoluzione digitale porta con se.

³² Il documento promuoveva anche una raccolta di firme virtuali per l'abolizione del Decreto Legge. Pur se le adesioni sono state molte, le firme non hanno valore legale.

CAPITOLO 2 “GENERAZIONI”

“Sì, io sono un criminale.
Il mio crimine è la mia curiosità.
Il mio crimine è quello di scovare
qualche vostro segreto,
qualcosa che non vi farà
mai dimenticare il mio nome.
Io sono un Hacker e
questo è il mio manifesto.
Potete anche fermare me,
ma non potete fermarci tutti...
Dopo tutto, ‘siamo tutti uguali’.”

The Mentor, “Hacker Manifesto”

2.1 Origine del fenomeno hacker tra passione e lavoro

Ad una prima lettura può sembrare strano, ma la storia degli hackers nacque nel club del modellismo ferroviario del Massachusetts Institute of Technology, Stati Uniti.

Il club, situato al palazzo 20, aveva una divisione interna: un gruppo pensava alla pittura e alla fornitura dei modellini; un altro componeva il cosiddetto “Signal and power subcommittee”, all’interno del quale ci si occupava della fornitura dell’energia elettrica per i trenini. In questo secondo gruppo il termine “Hack” descriveva un progetto che, oltre ad adempiere ad uno scopo preciso, “portava divertimento solamente con la partecipazione” (Steven Levy, “Hackers. Gli eroi della rivoluzione informatica”, Milano, Shake ed., 1996, pag. 22), e i più meritevoli venivano chiamati hackers.

Dal 1959 il MIT istituì un corso di programmazione per elaboratori elettronici al quale parteciparono molti studenti e dove si cominciò a capire

l'importanza che il computer poteva avere con gli anni a venire: non solamente una macchina utile, ma intelligente.

Chi meglio degli altri sapeva destreggiarsi con gli elaboratori si sentiva membro di un'élite e difficilmente faceva entrare altri nella cerchia.

I nuovi macchinari e i nuovi corsi di programmazione aprirono le porte ad un nuovo stile di vita dotato di una filosofia condivisa da tutti e che aveva come base la libera circolazione delle informazioni: nasce l'etica hacker.

Non essendoci ancora stabilità nel campo informatico³³ i primi hackers avevano tutto l'interesse nella sperimentazione. Potevano creare cose nuove o scoprire funzioni celate degli elaboratori senza preoccuparsi di eventuali danni al copyright o di affrontare un codice chiuso. Nei primi gruppi di hackers non si era considerati per aver scoperto qualcosa, ma per averla condivisa con tutti. Con l'avvento di macchine sempre più evolute, come il PDP-1³⁴, si poteva "hackerare" qualsiasi programma: si passava da numerose versioni del gioco degli scacchi, a Peter Samson che si divertiva a programmare calendari maya.

La prima rivoluzione nell'ambiente fu "Spacewar", primo videogioco spaziale creato da Slug Russel. Grazie alla condivisione continua delle risorse, il programma divenne completo in poco tempo: musica, suoni e uno sfondo spaziale furono soltanto alcune delle migliorie apportate al videogioco.

³³ Basti pensare che nel dipartimento di matematica del MIT si diceva che "L'informatica non è una scienza: è stregoneria". (Levy, 1996, pag. 62)

³⁴ Arrivato nel MIT nel 1961, fu il primo computer da tavolo della Digital Equipment. Permetteva la sperimentazione continua e venne considerato una manna dagli hackers.

Tutto questo senza pensare ad una possibile vendita del gioco soprattutto perché in questi primi anni di “hacking” si pensava alla sperimentazione e non a fare soldi programmando.

Accanto al fenomeno ‘Hacker’ del MIT e all’ideale della libera programmazione, affiorava il concetto di industria informatica, rappresentato in pieno dall’IBM.

Secondo i primi programmatori il colosso informatico rappresentava il vero “male” della programmazione. L’astio nasceva dal fatto che all’interno dell’IBM regnavano i segreti e niente poteva (doveva) essere condiviso, di conseguenza l’etica hacker non poteva nemmeno essere nominata. La similitudine della porta chiusa rappresentava quello che per i primi hackers doveva essere evitato: “tutte le porte devono essere aperte!”

A conferma di questa concezione basti pensare ad una delle pratiche più in voga tra gli hackers che si è tramandata fino ai nostri giorni: il “Lock Hacking”, ossia riuscire ad aprire una serratura nel minor tempo possibile.

Una caratteristica tipica degli hackers, oltre alla passione per la programmazione, era la totale assenza di rapporti sociali, in particolar modo con ragazze: “L’informatica era molto più importante del trovarsi implicati in una relazione affettiva” (Levy, 1996, pag. 67).

I tempi stavano cambiando e, lentamente, l’ideale industriale cominciava ad insinuarsi all’interno del MIT. Un primo passo fu l’istituzione di sistemi Time-sharing, ossia modalità attraverso le quali le risorse dei computer potevano essere usate contemporaneamente da più persone. Un sistema del genere fu il CTSS³⁵ che, in pratica, chiudeva ogni tipo di sperimentazione sui programmi.

³⁵ Compatible Time Sharing System.

Non sopportando tale chiusura, Tom Knight e Peter Greenblat, hackers storici, svilupparono l'ITSS, incompatible time sharing system, il quale, oltre ad essere più affidabile rispetto al CTSS, era totalmente "aperto" ossia poteva essere modificato da chiunque e, soprattutto, non richiedeva l'immissione di password in entrata.

Questo fu considerato uno degli eventi più importanti della cosiddetta "età dell'oro" dell'hackeraggio situata a cavallo tra gli anni 50 e 60. Questa "età" aveva sicuramente apportato migliorie sostanziali alle capacità dei primi computer ed aveva messo in risalto l'informatica nell'ambiente accademici, ma, esaminando le vite di questi "pionieri" dell'informatica, si realizza un fatto inquietante: erano "evasi" dalla vita reale.

Sono gli anni delle rivolte studentesche: l'originario rifiuto della società consumistica e industrializzata, come dimostrano le comunità hippy nate in quegli anni - le quali formarono una vera e propria alternativa culturale fondata sulla non violenza e sulla riflessione sul senso della vita - sfociò nei movimenti di protesta universitari. Nel 1964 in California venne occupato l'ateneo di Berkeley con una doppia motivazione: da una parte l'alternativa culturale di cui sopra, dall'altra la protesta verso la cosiddetta "sporca guerra" del Vietnam. Quest'ultimo avvenimento fu un centro di discussione comune per tutte le dimostrazioni e sit-in di quel tempo. Purtroppo non mancarono momenti di guerriglia urbana come dimostrano le rivolte del 1965 e 1967 nei ghetti metropolitani da parte di elementi del "Black Power", movimento nato contro la segregazione razziale.

L'apice venne raggiunto nel 1968 quando le rivolte si estesero in buona parte dell'Europa occidentale³⁶ e in alcune regioni giapponesi. Nel vecchio continente i movimenti studenteschi, seppur in alcuni casi ideologicamente diversi (da un lato una forte ispirazione marxista, dall'altro un'ammirazione verso la "rivoluzione culturale" cinese di Mao Tse-tung) trovavano elementi unificatori come: la lotta contro l'autoritarismo tipico della società industriale e il disprezzo verso l'imperialismo americano sfociato nell'intervento USA in Vietnam.

Quando molti studenti cominciarono a protestare anche all'interno del MIT, molti hackers ignoravano il motivo di tali manifestazioni: le sperimentazioni informatiche degli anni 50 e 60 si erano rese possibili grazie ad un progetto del Ministero della Difesa americano.

La reazione che ebbero gli hackers segnò una svolta nella loro etica. I giovani programmatori furono costretti a chiudere tutte le porte ed usare i lucchetti: il mondo "di fuori", quello reale, era entrato all'interno del circolo degli hackers del MIT.

Con le contestazioni di fine anni 60 e con l'avvento del pensiero dei "figli dei fiori", il pensiero hacker prende nuove conformazioni.

Il "guru" di questa nuova era fu Lee Felsenstein per il quale l'etica hacker doveva essere esportata dai laboratori verso le strade. Il "Community Memory" da lui fondato doveva servire proprio a questo. Il sistema permetteva lo scambio di messaggi tramite dei terminali sparsi per Berkeley in California, e la ricerca di notizie su servizi e orari dei luoghi pubblici della città. Il nodo centrale del pensiero di Felsenstein era "un computer in ogni casa" ma, anche se la zona della Baia di San Francisco stava

³⁶ Prevalentemente Germania, Francia, Italia e, per motivi diversi, Cecoslovacchia.

velocemente diventando la “Silicon Valley”³⁷ e la “Intel” aveva inventato il primo microprocessore, questa idea era scarsamente considerata.

Il cambiamento avvenne nel 1975 quando su “Popular Electronics”³⁸ comparve la prima foto dell’Altair della MITS di Ed Roberts: il primo personal computer³⁹.

La nuova invenzione racchiudeva in sé lo spirito hacker. Si ordinava e per poco più di 300 dollari a casa non arrivava il computer intero, ma tutti i pezzi da assemblare.

Ora molti amatori dell’elettronica e dell’informatica avevano un argomento in comune su cui discutere. Fred Moore e Gordon French, per questo motivo, organizzarono i primi incontri tra appassionati di computer sotto il nome di “Homebrew computer club”. Durante le riunioni si discuteva delle recenti scoperte informatiche e si apportavano modifiche all’Altair. Una di queste fu quella di Steve Dompier che riuscì a far suonare alla macchina alcune canzoni dei Beatles e “Daisy”, ovvero la prima canzone in assoluto “suonata” da un computer⁴⁰.

Le riunioni vedevano sempre più affluenza anche da parte di professionisti del settore informatico. Tra i partecipanti si facevano notare: Steve Wozniak che diventerà uno dei principali innovatori nel campo informatico grazie all’Apple, il computer creato con la collaborazione di Steve Jobs; Bill Gates e Paul Allen.

Questi ultimi due portarono un elemento fondamentale nella storia hacker: il business.

³⁷ Vista la quantità di silicio presente nel territorio.

³⁸ Rivista di informatica e di elettronica in generale molto seguita.

³⁹ Il computer prendeva il nome da quello di una stella raggiunta dall’ Enterprise durante un episodio di Star Trek.

Gates e Allen, che in pochi anni divennero la “Microsoft”, riuscirono ad implementare il Basic, linguaggio di programmazione straordinariamente semplice creato da John Keney, all’interno dell’Altair e a venderlo a varie società.

Come da consuetudine all’interno dell’Homebrew Computer Club cominciarono a circolare copie del suddetto programma senza essere pagate e per questo Bill Gates scrisse un documento entrato nella storia dell’informatica: “Lettera aperta sulla pirateria”⁴¹.

“Una cosa che fate è di ostacolare che del buon software venga scritto. Chi può affrontare di fare del lavoro professionale per nulla? Quale hobbista può mettere tre anni di tempo-uomo nella programmazione, trovando tutti i bug, documentando il suo prodotto e distribuirlo, tutto gratuitamente? Il fatto è che nessun altro oltre a noi ha investito del gran danaro nel software hobbistico. Abbiamo scritto il BASIC 6800 (...), ma esiste solo un piccolo incentivo a rendere disponibile questo software agli hobbisti.

Francamente, la cosa che voi fate è rubare” (Bill Gates, in Scelsi 1994).

I toni duri della lettera non fecero assolutamente piacere agli hobbisti, i quali ricordarono a Gates che alle riunioni alle quali anche lui partecipava si poteva scambiare hardware e software liberamente.

Ci si stava spostando da un’atmosfera di passione per la programmazione in una in cui l’importante era fare soldi con i software. Anche i gruppi di

⁴⁰ Nel 1957 nei Laboratori Bell. Una nota cinematografica: “Daisy” fu anche la canzone “suonata” dal computer Hal quando venne smantellato in “2001: Odissea nello spazio” di Stanley Kubrick.

⁴¹ Pubblicata sulla newsletter dell’Altair e su quella dell’Homebrew Computer Club. La versione in italiano è consultabile su: Raf Valvola Scelsi, “No copyright”, Milano, Shake Edizioni, 1994 (pp. 114-115).

discussione mutavano in direzione degli affari: nel sud della California nacque il “Southern California Computer Security” frequentato all’incirca da 8000 membri molti dei quali lavoravano per le maggiori aziende high-tech della zona e nei programmi, oltre alle riunioni, c’era l’acquisto di progetti e la redazione di una rivista nazionale.

Gli hackers venivano ricercati non solo per la loro capacità di programmare, ma anche per la velocità con la quale tiravano fuori nuovi programmi per essere venduti.

Questo diede inizio alla terza generazione: “l’etica hacker incontra il mercato” (Levy, 1996, pag. 225).

L’ideale era avere programmi buoni con verifiche continue; il mercato voleva programmi buoni per quanto fosse possibile.

Molti hackers vennero assunti presso aziende informatiche con il solo scopo di proteggere i prodotti inserendo particolari codici all’interno del prodotto finale. La situazione creatasi aveva qualcosa di paradossale: da una parte hackers che proteggevano i software, dall’altra hackers, ma che divennero ben presto crackers, impegnati nel distruggere le protezioni.

Una figura rappresentativa del cambiamento in corso è quella di John Harris, programmatore talentuoso che scrisse il gioco “Jawbreaker”, il quale venne giudicato troppo simile a Pac-Man e per questo causò, cosa impensabile fino a 20 anni prima, lo scontro legale tra la Sierra online e la Atari⁴².

L’hacker come genio ed innovatore del computer stava sparendo; negli anni 80 si pensava a lui come ad una macchina per fare soldi. A dimostrazione di

⁴² Harris per la Sierra OnLine scrisse anche “Frogger”, videogioco che venne rubato prima dell’uscita sul mercato. Il fatto causò un ritardo enorme nella riprogrammazione del gioco e il licenziamento di Harris.

ciò nel 1982 Tom Tatum, autore televisivo, realizzò una serie di quiz denominati “Wizard Vs Wizard”, nei quali sette giovani appassionati di programmazione si sfidavano ai videogiochi più famosi.

L’hacking era diventato un fenomeno di massa da far vedere alla TV, la mentalità industriale era entrata nel campo informatico e la rete stava diventando il nuovo campo da gioco.

2.2 La curiosità è un crimine?

Per iniziare a capire cosa ci sia dietro il modo di pensare di un hacker bisogna distinguere, come fa Eric S. Raymond⁴³, tra lo stile di pensiero “Accademia”⁴⁴ e quello “Monastero”. Nel primo caso si trova un problema e la sua soluzione in collettività, la creazione di nuovo materiale è aperta a tutti e le idee sono messe a disposizione dell’“Accademia” per discuterne e tentare di trovarne di nuove. Merton nel suo “La struttura normativa della scienza” afferma che: “l’etica scientifica richiede un modello in cui le teorie vengano sviluppate collettivamente e i loro difetti percepiti e gradualmente eliminati per mezzo di una critica fornita dall’intera comunità scientifica” (Merton R., “The sociology of science: theoretical and empirical investigations”, a cura di Stoner N., University of Chicago Press, Chicago, 1973, traduzione in italiano in “La sociologia della scienza”, Franco Angeli, Milano, 1981).

Lo scetticismo sistematico mertoniano è la base del concetto di Accademia e di conseguenza del modo di pensare degli hackers.

⁴³ Uno dei più importanti “saggi” dell’Hacking, autore del famoso documento “Come diventare un Hacker”.

⁴⁴ In molti documenti Accademia è sostituito da “Bazaar”, con lo stesso significato.

Il punto di forza di questo stile di vita è che una persona impara e poi divulga agli altri senza pensare a nessuna ricompensa tranne che a quella del riconoscimento dei pari.

Contrapposto a questo modello di apertura vi è il concetto di “Monastero” usato anche dai primi hackers del MIT negli anni 50 e 60 per definire il modo di lavoro dell’IBM⁴⁵.

In questo caso lo sviluppo di nuove risorse o la soluzione di problemi avviene a porte chiuse e soltanto alla fine si potranno vedere i risultati finali.

La cultura hacker non è pensata solamente per la soluzione di problemi derivanti dalla programmazione, ma anche per risolvere casi di importanza mondiale. Nel 1999, ad esempio, grazie all’Electronic Frontier Foundation (associazione di hackers, programmatori professionisti e di imprenditori) dal Kosovo poterono partire numerose e-mail verso i mezzi di comunicazione stranieri per far capire come stavano andando le cose e, grazie a questo, molti fatti sconosciuti videro la luce.

Il discorso etico si è evoluto insieme a quello sociale e tecnologico portando con gli anni molte variazioni ma con un centro che è sempre rimasto unico: l’informazione deve essere libera.

Negli anni del MIT si crea una prima conformazione dell’etica hacker assimilandola al concetto di ricerca. Fare hacking significava ricercare problemi e tentare di risolverli, condividendo sempre le informazioni che si avevano. È facilmente comprensibile il perché di questo pensiero: negli anni 50 e 60 gli elaboratori elettronici erano ancora macchine sconosciute e per questo era di fondamentale importanza cercare di capire sempre meglio il funzionamento di tali macchine e condividerne con altri la conoscenza.

⁴⁵ Ved. Paragrafo 2.1.

La fase di ricerca si unisce a quella della sperimentazione degli anni 70, arrivata dopo le lotte studentesche del 68 che, come visto nel precedente paragrafo, causarono il “risveglio” della comunità Hacker dal torpore causato dal computer. In questi anni cominciano i primi scontri tra hacking e diritto. Nelle riunioni dell’ Homebrew computer club cominciano a spuntare le prime blue box: macchinari creati da John Draper, conosciuto ai più come Capitan Crunch, il quale riuscì, con un fischiello trovato proprio nei cereali marca “Capitan Crunch”, ad ingannare il centralino del sistema telefonico statunitense; il fischio acuto⁴⁶ mandava in tilt la centrale telefonica lasciando la linea libera per effettuare telefonate gratis.

Il passo dal fischiello alla scheda per il computer fu brevissimo e il passaggio dalla legalità all’illegalità fu ancora più breve.

Qui sta uno dei principali dubbi che viene alzato dall’etica hacker: fin dove è legittimo sperimentare?

La risposta nei primi anni di hacking fu quella di sperimentare tentando di rimanere nel lecito e, nel caso ci si fosse trovati di fronte ad un sistema chiuso, lasciarlo così com’era e tentare di progettare un altro aperto e possibilmente migliore. Si pensi al sistema ITSS di cui si è parlato nel paragrafo 2.1.

Con l’arrivo delle prime reti e, poi, di Internet il concetto di “Hacker” cambia radicalmente. L’hacking è passato da protezione dei sistemi informatici ed elaborazione e miglioramento di software ad attacchi a siti istituzionali, creazione di virus e altre azioni di cui si legge spesso sui mezzi di informazione, dal libero accesso alle informazioni al blocco dell’accesso

⁴⁶ Il fischio veniva emesso a 2600 hz. Da questo dato nacque un gruppo di discussione ancora oggi molto famoso www.2600.org

alle informazioni. Questa situazione ha creato una discussione che va tuttora avanti tra la “vecchia guardia” hacker: l’etica hacker è rimasta la stessa rispetto agli anni pre-internet?

Secondo Eric Corley, conosciuto nell’ambiente informatico underground come Emmanuel Goldstein⁴⁷, l’etica dei primi hackers deve permeare il lavoro della nuova generazione⁴⁸. Citando Steven Levy, Corley delinea le linee fondamentali dell’etica hacker:

- Accesso ai computer illimitato e totale.
- Non fidarsi delle autorità e proporre il decentramento.
- Le informazioni devono essere libere.
- Gli hackers, per mezzo dei computer (e della rete) devono cambiare la vita in meglio.

Proprio questo ultimo punto porta ad altre considerazioni: se gli hackers devono migliorare la vita tramite l’uso del computer, perché molti distruggono sistemi informatici o infestano Internet con Virus o Trojan⁴⁹ ?

La risposta è semplice: perché non sono hackers.

⁴⁷ Dal nome della persona da odiare in “1984” di George Orwell.

⁴⁸ Articolo “Hacking = Ricerca” di Giovanni Ziccardi. Da “H&C” n°2 , Piscopo Editore, 2004.

⁴⁹ Il nome “Trojan” è dato dalla similitudine di tali software al cavallo di Troia. Questi software si nascondono in altri programmi e permettono un controllo totale di un computer a distanza.

Definire esattamente un hacker è impresa ardua per via delle numerose conformazioni che può prendere. Nello Jargon File si legge:

1. Una persona che studia a fondo le capacità di software e hardware di un computer senza fermarsi, come fa la maggior parte delle persone, alle caratteristiche superficiali.
2. Un programmatore che si diverte (e a volte ossessiona) programmando e parlando di programmazione.
3. Una persona capace di apprezzare i giochi da hacker⁵⁰.
4. Una persona brava a programmare velocemente.
5. Un esperto di un particolare programma.
6. Un esperto o entusiasta di qualsiasi cosa. Si può essere anche hacker nell'astronomia per esempio.
7. Una persona a cui piacciono le sfide intellettuali.
8. Un programmatore che tenta di rompere sistemi informatici e di creare software che potrebbe creare danni a chi lo usa. In questo caso la persona si può definire "cracker". (Jargon File, versione 4.4.2)

Eric S. Raymond nel suo documento "Come diventare un hacker" (documento on-line disponibile in varie versioni e continuamente aggiornato) propone una definizione molto meno dettagliata ma molto più efficace: "Gli hacker costruiscono le cose, i crackers le rompono".

Ultimamente la linea che delinea il limite tra hackers e crackers è molto sottile. Questi ultimi sono coloro che "breaks security on a system"⁵¹. Il termine "Cracker" è stato coniato a metà degli anni 80 proprio dagli hackers

⁵⁰ Nel testo originale si legge "A person capable of appreciating hack value" dove per "Hack Value" si intende quelle migliorie non necessarie ma particolari inserite all'interno dei programmi.

⁵¹ Jargon File (4.4.2.)

per ovviare alle continue sostituzioni di termini che avvenivano sui giornali o sulle newsletter.

Il termine “Hacker” delinea, quindi, sia la voglia di esplorazione dei computer che la voglia di rendere l’informazione davvero libera da ogni vincolo. Ma nei meandri di queste definizioni si nasconde anche colui che si diverte a penetrare nei sistemi informatici creando danni a volte irreparabili. Essendo queste ultime persone le più pubblicizzate, oggi si ha la tendenza ad usare la parola “Hacker” per delineare solamente operazioni di frode, furti o di rottura di sistemi di sicurezza dando una visione di Internet come sede di una “Cybercultura deviante mondiale che recluta, indottrina, istruisce e prepara tecnicamente individui, specie adolescenti, alla commissione di svariati crimini” (G.R. Wynn “Cyberculture ad differential association: the Net effect on juvenile delinquency”, Georgia State University, 1998. Traduzione italiana in Marco Strano “Manuale di criminologia clinica”, See, Firenze, 2003).

Basta citare qualche definizione per comprendere la difficoltà di definire univocamente l’hacker: recentemente alcuni senatori repubblicani americani hanno affermato l’uguaglianza tra armi e mouse⁵²; Laura La Posta in un articolo de “Il Sole 24 ore” del 14 febbraio 2003 scrive “ma come si fa a difendere persone apparentemente indifendibili come gli hackers che entrano nei sistemi informatici altrui per il puro gusto di fare danno?”⁵³; nel dizionario inglese “Collins” alla voce “Hacker” si legge: “A computer hacker is someone who tries to break into computer system, especially in

⁵² www.punto-informatico.it, citato su “H&C” n° 1 , Piscopo Editore, 2004.

⁵³ “Hacker usati come parafulmine”, Laura La Posta da “Il Sole 24 ore” del 14 febbraio 2003.

order to get secret or confidential information that is stored there”⁵⁴, definizione molto simile a quella che lo “Jargon File” fa del “Cracker”.

Non mancano, però, le caratterizzazioni positive: Steward Brend, fondatore del “Whole Earth Catalog” afferma “penso che gli hackers, programmatori innovativi ed irriverenti che si sono consacrati al loro lavoro, siano stati la più interessante e sincera incarnazione dell’intellettuale (...). Riorganizzando l’era dell’informazione intorno all’individuo, attraverso il personal computer, gli hackers possono ben dire di aver salvato l’economia americana.” (Steward Brend, 2000; citato in Chiesa R., “Il difficile rapporto tra hacking e marketing”, da www.internos.it, 2000); gli fanno eco Di Corinto e Tozzi affermando che gli hackers “sono coloro che rivendicano un uso del computer come strumento di liberazione e di cambiamento sociale”(Di Corinto A. e Tozzi T., “Hacktivism, la libertà nelle maglie della rete”, Roma, Manifestolibri, 2002, pag. 15).

La definizione che, probabilmente, si avvicina di più allo spirito hacker è quella di Wark McKenzien nel suo “Hacker Manifesto 2.0” nel quale si legge: "Hackers create the possibility of new things entering the world. Not always great things, or even good things, but new things. In art, in science, in philosophy and culture, in any process of knowledge where data can be gathered, where information can be extracted from it, and where in that information new possibilities for the world produced, there are hackers hacking the new out of the old." (McKenzien, “Hacker Manifesto 2.0”, documento on-line, 2001).

Schierarsi da una parte o dall’altra risulta molto difficile perché, affermiamolo, la ragione sta nel mezzo.

⁵⁴ English dictionary “Collins”, edizione 1995.

A confermare questa constatazione c'è la nuova generazione hacker, “figlia” delle prime reti e della nascente Internet, la quale fu la prima ad affrontare un caso giudiziario di enorme portata: l'operazione “Sundevil”.

Tutto iniziò quando ad Atlanta tre hackers conosciuti come Prophet, Leftist e Urvile riuscirono ad entrare nel sistema della compagnia telefonica “Bellsouth” e a copiare un file chiamato “documento E911” nel quale erano contenute tutte le coordinate per amministrare il servizio 911 statunitense (il “nostro” 113).

Una volta fatto ciò, dispersero il file in numerosi computer di amici e non.

Ad aggravare la situazione, nel gennaio del 1990 il sistema di commutazione della “AT&T” per le chiamate telefoniche a lunga distanza si guastò disperdendo milioni di telefonate. Il problema derivò da un errore interno di programmazione del software che gestiva le suddette chiamate, ma la colpa venne data agli hackers. Questo perché il fenomeno stava lentamente prendendo piede: c'erano i primi tentativi di intrusione in sistemi informatici e nelle BBS⁵⁵ cominciavano a spuntare le prime riviste che trattavano di hacking come la storica “Phrack” nella quale venne pubblicato il documento E911 non nella sua forma completa in quanto mancavano gli avvisi anti-copia inseriti dalla “BellSouth” e alcuni dati tecnici.

Furono proprio le BBS a finire sotto il mirino della polizia perché identificate come centro della rivolta “elettronica”. Il primo scontro ufficiale tra Polizia, rappresentanti della “vita reale”, e “abitanti” del cyberspazio fu fonte per una riflessione importante: le BBS non erano stampa, telefonia,

⁵⁵ Bulletin Board System, una sorta di bacheca virtuale nella quale si scambiavano files e messaggi.

televisione e quindi non erano considerate dagli organi di legge come mezzi di comunicazione.

Le bulletin-board system furono un punto di partenza per la formazione di gruppi hacker storici come la “Legion of Doom”, vera protagonista dell’operazione “Sundevil”.

Ancora una volta, come gli hackers del MIT, molti ritenevano che, entrando in una BBS, quindi nel cyberspazio, le operazioni compiute al suo interno non avrebbero avuto conseguenze nella vita reale: “Facendo l’hacker uno può vincere o perdere, avere successo o fallire, ma non c’è mai l’impressione di ‘realtà” (Sterling B., “Giro di vite contro gli Hackers”, Milano, Shake ed., 1993, pag. 76).

Come avvenne e avviene in numerosi casi, la polizia sfrutta i mezzi usati dagli hackers per incastrare questi ultimi: nell’operazione “Sundevil” l’ FBI aprì delle “Sting Board” ossia delle BBS a trabocchetto nelle quali si lasciavano entrare molti utenti per poi fargli rivelare qualche nefandezza.

Purtroppo molte persone arrestate, la maggior parte facente parte della “Legion of Doom”, non erano a conoscenza del documento E911 ma per la polizia andava bene avere soltanto un requisito per essere indagato: essere un hacker.

Da esempio è la vicenda di “The Mentor”⁵⁶, hacker della “Legion of Doom” ma anche programmatore presso la “Steve Jackson Game”, una delle principali case di produzione di videogame del mondo. Gli inquirenti sequestrarono il suo computer personale, tutti quelli della casa di produzione di software e chiusero la BBS della suddetta “software-house” perché si

⁵⁶ Conosciuto nell’ambiente underground per il suo scritto “Hacker’s Manifesto”.

aveva il sospetto che il documento E911 fosse passato anche da quelle parti. Si narra che la Steve Jackson Game venne colpita perché era al lavoro su un nuovo gioco chiamato “Cyberpunk” dal quale, secondo la polizia, si potevano carpire tutte le tecniche per diventare un hacker perfetto⁵⁷.

Dall’operazione del gennaio 1990 nacque anche la “Electronic Frontier Foundation” fondata da Mitch Kapor, creatore del foglio elettronico “LOTUS”⁵⁸, e da John Perry Barlow, storico paroliere del gruppo rock Grateful Dead, il quale subì una perquisizione durante la “Sundevil” la quale gli fece capire che, in realtà, non si volevano colpire i responsabili delle azioni criminose, ma tutta la comunità hacker.

L’EFF si fece portavoce dei diritti degli indagati e riuscì a far cadere l’accusa di aver copiato un documento pericoloso come l’E911 trovando lo stesso documento stampato nel libro “The intelligent network” nel quale c’erano molte più informazioni a riguardo rispetto a quello pubblicato su “Phrack”.

L’operazione “Sundevil” fu importante per molti motivi: per prima cosa fece avvicinare, magari troppo bruscamente, l’ambiente hacker alla vita reale; fece capire alla Polizia e agli organi legislativi che un problema di inadeguatezza legislativa per l’ambiente informatico era esistente; aprì un discorso sui diritti “digitali” delle persone che va ancora avanti nei nostri giorni.

L’hacking non si ferma su una tastiera ed un monitor. Molte associazioni come la EFF di cui si è parlato in precedenza, o la “Witness”, nata grazie al musicista inglese Peter Gabriel, hanno lo scopo di far capire come esistono

⁵⁷ Nel 1993 la Steve Jackson Game fece uscire un gioco chiamato “HACKER” considerato molto più accurato di “Cyberpunk”. In questo caso la polizia non intervenne per bloccare il gioco.

⁵⁸ “Padre” dell’odierno Microsoft Excel. Permetteva di comporre un database.

dei diritti “digitali” ignorati dai più, ma di fondamentale importanza al giorno d’oggi. Si pensi all’associazione di programmatori ed appassionati di informatica “XS4ALL”⁵⁹ grazie alla quale, durante la guerra in Jugoslavia del 1998, si riuscì a far trasmettere la radio indipendente “B92”.

In questo caso non si parla di Hacker o Hacking ma, unendo il termine a quello di attivismo, si parla di Hacktivism: uso del computer, praticato in modo non convenzionale, finalizzato al miglioramento di qualcosa di utile per il mondo con implicazioni sociali, politiche o culturali.

L’evoluzione di questo movimento va di pari passo a quella della comunicazione di massa: le proteste si spostano dal volantino alle petizioni elettroniche e ai sit-in elettronici. Tra gli obiettivi prefissati dagli Hacktivist, oltre a quello di difesa e, soprattutto, riconoscimento dei diritti “digitali”, il diritto alla cooperazione (interscambio orizzontale), quello alla privacy che, come abbiamo visto, è da sempre centrale nel pensiero hacker, il diritto alla libertà di copia e quello di libero accesso alle risorse elettroniche.

Ma come si può adeguare l’etica hacker ai cambiamenti tecnologico-sociali? Una domanda di difficile risposta anche perché fonte di continue discussioni tra gli addetti ai lavori: da un lato ci sono persone come Richard Stallman, definito da molti “L’ultimo hacker”, che si battono per un rispetto dell’etica hacker “prima maniera”; dall’altro lato ragazzi dell’ultima generazione che, considerando le potenzialità positive e negative di Internet⁶⁰ e le prospettive

⁵⁹ Gioco di parole che indica “Access for all”.

⁶⁰ Tra le positive c’è sicuramente la maggiore possibilità di diffusione delle informazioni, tra le negative troviamo la possibilità di danneggiare sistemi informatici con maggiore velocità.

che si possono aprire con il software libero, tendono a prospettare una maggiore elasticità del pensiero hacker.

A rappresentazione di questa spaccatura c'è la denominazione "Open Source" scelta da Eric S. Raymond per definire il software con codice visibile e modificabile in contrapposizione alla concezione di Stallman di Free Software: mentre Stallman e la sua Free Software Foundation tendono ad avere un rapporto di contrasto verso il mercato del software e non vogliono scendere a compromessi, il movimento Open-source, nel quale viene incluso anche Linus Torvalds e il suo prodotto Linux⁶¹ (o altrimenti chiamato GNU/LINUX), tende a "sfruttare" alcune parti del mercato software. Emblematica rimane la frase di Torvalds commentando i prodotti Microsoft: "perché prendersela con il software proprietario soltanto per principio?": ormai la "vecchia" etica hacker non va più bene.

Nel 1989 ad Amsterdam si tenne una conferenza hacker molto importante, l'"ICATA 89", nella quale Hans Hübenr, alias "Pengo", membro rinnegato del "Chaos Computer Club" (CCC) uno dei più importanti gruppi hacker europei, affermò di fronte a Wau Holland, fondatore del gruppo stesso, che la morale e l'etica hacker non erano sufficienti a far fronte alle pressioni esercitate sui ragazzi dal denaro e dal potere politico. Davanti alle numerose obiezioni, Pengo rispondeva facendo notare che molti hackers erano diventati consulenti informatici vendendo le proprie risorse. Una piccola parentesi sul motivo dell'allontanamento dal "CCC" di Pengo: a 20 anni aveva rubato delle informazioni dal ministero della difesa tedesco e, vivendo la situazione come se fosse solamente un film o un romanzo di spionaggio, le rivendette al KGB.

⁶¹ Sistema operativo per personal computer. Considerato la vera alternativa al prodotto Microsoft "Windows".

Tutta la storia finì in un romanzo-documentario di Clifford Stoll, “The Cuckoo’s Egg” nel quale si legge: “Pengo had no scruples about selling information to Soviet bloc agents. He saw himself as ethically neutral, he didn’t want to give the Russians any advantage; he just wanted to have fun on the networks. And pick up some cash along the way.” (Clifford Stoll, “The Cuckoo’s egg. Tracking a spy through the maze of computer espionage”, 2000, pag. 231).

La nuova generazione hacker ha come figura da seguire Torvalds e come modello il bazaar di Raymond.

Durante l’ICATA 89 si posero le basi per una nuova etica hacker. Lee Felsestein ed altri tecnici informatici ed appassionati “profondamente turbati dalla prospettiva di una tecnologia dell’informazione e degli attori economici e politici scatenati da essa, senza controllo democratico né partecipazione popolare efficace”(Lee Felsestein in Scelsi, “Cyberpunk”, Milano, Shake ed., 1994, pag. 107)definirono che:

1. Lo scambio libero e senza alcun ostacolo dell’informazione sia un elemento essenziale delle nostre libertà fondamentali e debba essere sostenuto in ogni circostanza. La tecnologia dell’informazione deve essere a disposizione di tutti e nessuna considerazione di natura politica, economica o tecnica debba impedire l’esercizio di questo diritto.
2. Tutta intera la popolazione debba poter controllare, in ogni momento, i poteri del governo; la tecnologia dell’informazione deve allargare e non ridurre l’estensione di questo diritto.

3. L'informazione appartiene a tutto il mondo, essa è prodotta per tutto il mondo. Gli informatici, scientifici e tecnici, sono al servizio di tutti noi. Non bisogna permettere loro di restare una casta di tecnocrati privilegiati, senza che questi debbano rendere conto a nessuno del loro operato.
4. Il diritto all'informazione si unisce al diritto di scegliere il vettore di questa informazione. Nessun modello unico di informatizzazione deve essere imposto a un individuo, una comunità o a una nazione qualsiasi. In particolare, bisogna resistere alle pressioni esercitate dalle tecnologie "avanzate" ma non convenienti. Al loro posto, bisogna sviluppare dei metodi e degli equipaggiamenti che permettano una migliore convivialità, a prezzi e domanda ridotti.
5. La nostra preoccupazione più forte è la protezione delle libertà fondamentali; noi quindi domandiamo che nessuna informazione di natura privata sia stockata, né ricercata tramite mezzi elettronici senza accordo esplicito da parte della persona interessata. Il nostro obiettivo è di rendere liberamente accessibile i dati pubblici, proteggere senza incertezze i dati privati. Bisogna sviluppare delle norme in questo senso, insieme agli organismi e alle persone interessati.
6. Ogni informazione non consensuale deve essere bandita dal campo dell'informatica. Sia i dati che le reti devono avere libertà d'accesso. La repressione dei pirati deve divenire senza fondamento, alla maniera dei servizi segreti. Parallelamente domandiamo che tutte le legislazioni, in progetto o già in applicazione, rivolte contro i pirati e che non perseguono scopi criminali o commerciali, siano ritirati immediatamente.

7. L'informatica non deve essere utilizzata dai governi e dalle grandi imprese per controllare e opprimere tutto il mondo. Al contrario, essa deve essere utilizzata come puro strumento di emancipazione, di progresso, di formazione e di piacere. Al contempo, l'influenza delle istituzioni militari sull'informatica e la scienza in generale deve cessare.

Bisogna che sia riconosciuto il diritto d'avere delle connessioni senza alcuna restrizione con tutte le reti e servizi internazionali di comunicazione di dati, senza interventi e controlli di qualsiasi sorta. Bisogna stabilire dei tetti di spesa, per paese, per avere accesso a questi vettori di comunicazione di dati pubblici e privati. Si deve facilitare quei paesi senza una buona infrastruttura di telecomunicazione e la loro partecipazione nella struttura mondiale. Noi ci indirizziamo agli utilizzatori progressisti di tecnologie di informazione nel mondo affinché socializzino le loro conoscenze e specializzazioni in questo campo con delle organizzazioni di base, al fine di rendere possibile uno scambio internazionale e interdisciplinare di idee e informazioni tramite delle reti internazionali.

8. Ogni informazione è al contempo deformazione. Il diritto all'informazione è al contempo inseparabilmente legato al diritto alla deformazione, che appartiene a tutto il mondo. Più si produce informazione, e più si crea un caos di informazione sfociante sempre più in rumore. La distruzione dell'informazione come del resto la sua produzione, è il diritto inalienabile di ognuno.

9. Bisognerebbe sovvertire i canali regolamentari e convenzionali dell'informazione grazie a dei detournements e dei cambiamenti

surrealisti degli avvenimenti, al fine di produrre del caos, del rumore, dello spreco i quali, a loro volta, saranno considerati come portatori di informazione.

10. La libertà di stampa deve applicarsi anche alle pubblicazioni tecno-anarchiche, che appaiono in giro, per reclamare la liberazione dei popoli, la fine delle tirannie della macchina e del sistema sugli uomini. (Dichiarazione finale dell' ICATA 89, in Scelsi, "Cyberpunk", Milano, Shake ed., 1994, pp. 107-109).

I punti di maggior riflessione sono il terzo ed il quinto. Nel punto tre si parla di emancipazione dell'ambiente tecnico-informatico a differenza dei primi tempi hacker dove esserlo era far parte di un'élite. Nel punto cinque c'è la richiesta di collaborazione con gli organi legislativi per trovare insieme norme che tutelino la libertà di informazione: al posto dell'originario "Diffida dall'autorità" si è passati ad un "Tenta di collaborare con l'autorità".

Le nuove tecnologie e le potenzialità da esse fornite hanno portato ad un cambiamento radicale in tutto l'ambiente underground informatico, ridefinendo in maniera sostanziale l'etica ed allargando a dismisura le capacità del termine "Hacker" includendo in esso ragazzi alle prime armi, i cosiddetti "Lamer", che si appassionano nel programmare virus o nel danneggiare sistemi altrui sperando nella già citata riconoscenza dei pari ossia nel riconoscimento da parte dei più esperti di una sorta di bravura e talento innato. Questo, oltre a danneggiare sensibilmente l'immagine pubblica che hanno gli hackers, rende ancora più difficile il lavoro per chi deve mantenere la sicurezza dei sistemi informatici.

Commentando i risultati dell'operazione "Sundevil" il senatore statunitense Patrick Leahy disse: "Non possiamo indebitamente porre limiti a ragazzini dotati di spirito investigativo che, se saranno lasciati liberi di sperimentare oggi, domani potranno sviluppare le telecomunicazioni o la tecnologia informatica capaci di condurre gli Stati Uniti nel ventunesimo secolo. Questi ragazzini rappresentano il nostro futuro e la nostra migliore speranza di rimanere una nazione tecnologicamente competitiva." (Leahy citato in Sterling, 1993, pag. 230).

L'etica hacker dei nostri giorni deve tener conto, per quanto possibile, delle infinite possibilità fornite da Internet di espandere il concetto base di informazione libera rispettando comunque il diritto, ma, dall'altra parte, quest'ultimo deve essere elaborato in maniera tale da favorire la sperimentazione ed aprire la strada a nuovi modi di concepire il software ed Internet facendo in modo che futuri Jon Johansen (ved. Capitolo 1, par. 1.3) non si trovino ad affrontare processi contro colossi industriali solamente per aver elaborato un software ed averlo distribuito gratuitamente.

CAPITOLO 3 “HACKER IN ITALIA”

“Nel nostro mondo, qualunque cosa creata dalla mente umana può essere riprodotta e distribuita all’infinito senza alcun costo.”

John P. Barlow, “Dichiarazione d’indipendenza del Cyberspazio”

3.1 Hacker e pirati

Dalle analisi effettuate nei precedenti capitoli si può intuire come l’essere un hacker possa essere considerato un vantaggio nell’odierna società dell’informazione. Con innovazioni tecnologico-informatiche che si susseguono con una velocità superiore alla Legge di Moore⁶², chi riesce non solo a destreggiarsi in maniera disinvolta ma, soprattutto, riesce a capire a fondo le funzioni di macchinari futuristici viene considerato un elemento d’“élite”. Software come “Linux”, licenze per programmi come la già citata “GPL” e il concetto di programmazione “Open Source” sono venuti fuori in questi anni grazie alla passione di persone dedite completamente alla causa della libera circolazione delle informazioni e alla sperimentazione continua e senza ostacoli con i personal computer.

“Angeli o demoni, innocui idealisti o pericolosi criminali, sognatori o furfanti, anarchici o truffatori. Chi siano davvero gli hackers è difficile a dirsi.”. Comincia così l’articolo “Anarchici o truffatori – la vera storia degli hackers” di Giancarlo Mela comparso su “La Repubblica” del 27 febbraio 1999, denotando, anche all’interno della stampa, una certa confusione sulla

⁶² Legge di Moore: la velocità dei processori per personal computer raddoppia ogni 18 mesi.

definizione del personaggio “Hacker” in generale e nella caratterizzazione del “tipo” italiano.

Considerate le numerose divisioni interne al movimento nate per lo più nella metà degli anni 80 con l'avvento degli affari nell'ambiente underground informatico, si può tentare una sorta di classificazione dei personaggi: si va dai “Crackers” ai “Lamer”, dai “Courier”, ossia coloro che spostano i files “crackati” da un sito ad un altro permettendo, così, il download a tutti, ai “Supplier”, coloro che forniscono ai gruppi di crackers i programmi nei quali va eliminata la protezione.

Raoul Chiesa, il più importante hacker italiano, fondatore e CTO (Chief Technical Officer) di “@Mediaservice.net”⁶³, aggiunge tra gli altri i “Wannabe Lamer” (scarsamente pericolosi), gli “Script Kiddie” (più abili rispetto i precedenti ma poco pericolosi per i sistemi) e, soprattutto, gli “Ethical Hacker” ovvero coloro che amano e rispettano i sistemi, desiderano conoscerli a fondo per renderli migliori⁶⁴. L'intrusione nel sistema informatico c'è comunque, ma secondo il loro parere, è a scopo benevolo: entrano nel sistema, lo esplorano senza danneggiare nulla e poi avvertono gli amministratori del sistema stesso consigliando loro i “bachi”⁶⁵ da riparare.

Alcuni rispondono bene all'”intruso”, per esempio molti hackers sono divenuti “SysAdmin” – amministratori di sistema – oppure consulenti informatici, ma c'è anche l'altra faccia della medaglia: molti, la maggior

⁶³ Società nata nel 2000 dall'evoluzione di “Mediaservice S.a.s”. Sono principalmente due i campi di azione: nuovi media & comunicazione e sicurezza informatica.

⁶⁴ Per una descrizione accurata dell'Hacker etico si rimanda a “Ethical Hacking” manifesto dell'associazione “Italian Black Hats” disponibile on-line su www.dvara.net.

parte, non apprezzando il gesto denunciano il fatto o ignorano qualsiasi consiglio fornito dall'hacker - anche perché per una grande azienda è imbarazzante sapere che qualcuno è entrato nella rete interna e ha scovato qualche falla⁶⁶.

Come se una persona non autorizzata entrasse in casa nostra e, una volta uscita senza rubare nulla, ci consigliasse di chiudere meglio la porta. Saremmo disposti ad accettare il consiglio? Farebbe differenza se ad entrare fosse un ragazzino o un distinto gentiluomo?

Nella sua "Storia e realtà dell'hacker italiano", Flavio Bernadotti scrive "personalmente non avrei timore di un hacker professionista in quanto questo possiede obiettivi ben definiti che non coincidono quasi mai con la finalità di arrecare soltanto dei danni dentro ai sistemi a cui questo accede. I danni invece è facile che li possano fare i ragazzini i quali non avendo neppure ben presente i meccanismi su cui si basano alcuni software (..), li usano in modo indiscriminato arrecando danni ai computer che vivono sulle strutture dei sistemi attaccati." (Bernadotti F., "Storia e realtà dell'hacker italiano", documento on-line, www.bernadotti.it, 2003).

Con l'ausilio di queste classificazioni si è tentato negli anni di fare un ritratto dell'hacker italiano, ma capire dove comincia il comportamento da hacker ossia un uso etico del personal computer e, da quasi dieci anni, di Internet e dove inizia invece l'atteggiamento criminale è assai complicato. La diversa caratterizzazione del personaggio data da una parte dagli appassionati del web e dall'altra da stampa e mezzi di comunicazione in generale rende ancora più difficile la questione⁶⁷.

⁶⁵ Termine tradotto dall'inglese "Bugs" ossia difetto all'interno di un software o Hardware.

⁶⁶ Considerare anche il fatto che se l'intrusione non è denunciata per "imbarazzo" la Polizia non può intervenire.

⁶⁷ Per qualche esempio si veda il paragrafo 2.2.

Con l'introduzione delle nuove tecnologie, in questo caso di Internet, si ha un cambiamento sia nel crimine che nella concezione dello stesso. I crimini tradizionali si evolvono (si pensi alle possibilità di commettere un furto o a quelle di giocare d'azzardo che il cyberspazio propone), e ne nascono di nuovi come la diffusione di virus informatici, lo spamming⁶⁸ e l'hacking.

Il termine "Hacker" si sta espandendo e oltre ad accogliere appassionati di informatica che, comunque commettendo un illecito, "aprono" (decompilano) un software proprietario tentando di capire come possa funzionare, ha aperto le porte anche ai creatori di virus che con cadenza giornaliera invadono Internet. Sul supplemento "@lfa" de "Il Sole 24 ore" del 9 settembre 2004 si poteva leggere il titolo: "Ad agosto gli hackers hanno scatenato un'offensiva senza precedenti", rendendo sottinteso il fatto che l'esistenza di worm⁶⁹ nella rete è responsabilità diretta degli hackers.

Altro requisito richiesto per far parte della nuova generazione di "Smanettoni" (definizione usata per indicare gli hackers nostrani da Chiccarelli e Monti, "Spaghetti Hacker", Milano, Apogeo, 1997) è avere un briciolo di curiosità e sapersi destreggiare nel web. Soprattutto con questo ultimo elemento si ha la possibilità di aprire il vaso di pandora ovvero di trovare veri e propri kit per distruggere sistemi informatici, rubare password e identità con relativi numeri di carta di credito: per avere qualche prova il più delle volte basta digitare "Warez" in un qualsiasi motore di ricerca. Con questa parola si indicano i siti nei quali sono contenuti materiali per compiere azioni illecite verso siti o interi sistemi e, almeno in alcuni, si ha la

⁶⁸ Per Spamming si intende l'invio massiccio di e-mail non desiderate ad utenti. Ved. Glossario.

⁶⁹ Per worm si intendono software creati con il solo scopo di recare danno. Si consideri un virus o un trojan.

possibilità di scaricare nel proprio computer materiale protetto da copyright “doverosamente crackato”.

“C’era una volta il Robin Hood dei bit, che rubava ai ricchi computer delle università e delle grandi organizzazioni capacità di elaborazione per addestrarsi al mestiere di sistemista povero ma geniale” (Laura La Posta, “Hackers usati come parafulmine”, “Il Sole 24 ore”, 14 febbraio 2003), ma il quadro che si ha oggi è che Robin Hood sia diventato il compagno dello Sceriffo di Nottingham ed abbia capito che è più divertente usare arco e frecce a disposizione per il proprio guadagno piuttosto che ampliare le proprie conoscenze.

Un profilo dell’hacker come “cybercriminale” è dato da Marco Strano, criminologo e direttore tecnico psicologo dal centro di Neurologia e psicologia medica della Polizia di Stato, il quale afferma che i nuovi criminali del web sono soggetti tendenzialmente non violenti che nella solitudine di un computer, commettono azioni delittuose che non riuscirebbero mai a compiere al di fuori del Cyberspazio. Lo schermo diventa una sorta di protezione che influenza anche alcuni meccanismi del pensiero quali per esempio la percezione dell’illegalità del comportamento, la stima dei rischi di essere scoperti e la percezione del danno procurato alla vittima.

Sempre Marco Strano distingue due tipi di hackers: quello formato da una classe di età dai 30 ai 45 anni, ossia coloro che hanno cominciato da piccoli con i primi computer, che “sognano ancora ideali di ‘etica dell’hacking’ ma hanno quasi completamente abbandonato le frequentazioni pericolose del mondo digitale underground” (Marco Strano, “La psicologia degli hackers”,

ICT security 2003, documento on-line sul sito www.criminologia.org): l'altro gruppo è rappresentato da adolescenti che utilizzano tecniche di hacking più che altro per farsi vedere dagli altri e per dimostrare che anche loro ci sanno fare con il computer ma “molti di loro hanno più paura della mamma che della Polizia Postale” (Strano,2003).

Le ricerche condotte in Italia per configurare il personaggio “Hacker” sono state principalmente divise in due filoni:

1. studio sulle caratteristiche psicologiche, che ha portato alla costruzione del seguente profilo:
 - soggetto tendenzialmente non-violento;
 - soggetto con elevata capacità di pianificazione del comportamento per sfruttare le opportunità dell'informatica;
 - soggetto in possesso di minori strumenti psicologici di contenimento dell'ansia per l'assenza di un contatto diretto con la scena del crimine e con la vittima;
 - soggetto con la tendenza ad operare in solitudine;
 - soggetto con tendenza ad acquisire il know how criminale in ambito informatico;
 - soggetto con minore tendenza ad autopercepirsi come un soggetto criminale.

2. Un'altra serie di studi ha portato in evidenza la distorta percezione del crimine da parte dell'autore dello stesso. Si ha una diversa percezione rispetto un “normale” criminale in:
 - percezione dell'illegalità del comportamento;
 - stima dei rischi di essere scoperto;
 - stima dei rischi di essere denunciato;

- percezione del danno procurato alla vittima;
- valutazione della possibilità della sanzione sociale e legale. (Strano, “Manuale di criminologia clinica”, See, Firenze, 2003, pag 380-381)

Sempre in ambito criminologico, la dottoressa Stefania Ducci – criminologa e consulente presso l’UNICRI (United Nations Interregional Crime and Justice Research Institute) – struttura il seguente profilo degli hackers:

- quoziente intellettivo al di sopra della media ed eccellenti abilità tecniche;
- sono più che altro adolescenti brillanti che tendono a considerare scarso il loro sistema educativo;
- in prevalenza provengono da famiglie problematiche;
- hanno una spiccata avversione verso le autorità e i simboli che la rappresentano;
- hanno quella che possiamo definire “dipendenza da hacking”.⁷⁰

Facendo un po’ di ordine tra tutte le cose scritte fino ad ora si scopre che un hacker è colui che, sperimentando, ha portato l’innovazione nel campo informatico; colui che entra abusivamente all’interno di sistemi informatici; crea virus e toglie la protezione rendendo gratuiti programmi altrimenti a pagamento.

La confusione è ancora molta soprattutto perché in Italia manca il retroterra informatico presente negli Stati Uniti e per questo, mentre al di là dell’oceano non sempre si condannano le azioni compiute dagli hackers, nel

⁷⁰ L’intervento della Dottoressa Stefania Ducci si può leggere sul n° 9 della rivista “Hackers & C”, 2004, Piscopo Editore;

nostro paese si tende a caratterizzare in maniera negativa il personaggio in questione. Nella metà degli anni 80 il personal computer è ormai un “oggetto” conosciuto da molti e pubblicizzato sui mezzi di comunicazione. Questo porta un cambiamento nella concezione dell’informatica da parte degli addetti ai lavori: se prima si programmava per passione, ora nell’era di “Pac-Man” lo si fa prevalentemente per i soldi e al laboratorio statunitense si sostituisce il negozio di appassionati di informatica spuntato quasi per caso. Questa è l’atmosfera che arriva in Italia insieme ai primi “computer giocattolo”⁷¹ come il Commodore 64 e lo Spectrum i quali permettevano, oltre ad un’ottima esperienza videoludica, i primi tentativi di programmazione: gli odierni appassionati di informatica italiani, presumibilmente, hanno avuto tutti le stesse origini tra cassette, cartucce e manuali introvabili e incompleti.

Il “linguaggio macchina”, imparato soprattutto perché permetteva il cracking delle protezioni dei videogiochi per avere, così, qualche risorsa da scambiare, fu il primo passo nel mondo sconosciuto dei computer. Questo quadro di hacking, nato tra la fine degli anni 70 e l’inizio degli anni 80, è quello più rilevante fino al 1986 anno ufficiale di nascita del “Videotel”, una proto-internet italiana. Questo nuovo sistema fu la palestra per molti ragazzi impegnati tutta la notte nella ricerca di ingressi gratuiti nel servizio. Con un po’ di ingegneria sociale⁷² si riuscivano a carpire le password di grandi aziende alle quali venivano addebitate tutte le chiamate.

In questo periodo arrivano i primi contatti con BBS stranieri, soprattutto “ALTOS” in Germania nella quale si poteva trovare il meglio del panorama

⁷¹ Definiti così perché anche se buone macchine per la programmazione furono usate prevalentemente per giocare.

⁷² Per una definizione si veda il paragrafo 1.2. o il glossario.

hacker europeo: si poteva cercare⁷³ un particolare videogioco, un sistema operativo o un qualsiasi altro programma dal quale era stata eliminata la protezione.

Si trovavano anche le “mosche bianche” che si cimentavano nel tentativo di entrare in qualche computer super-protetto come quelli del governo americano.

La visione dell’hacker si divideva in due:

1. da una parte l’immagine che gli addetti ai lavori o i neofiti della rete avevano del personaggio ossia una sorta di “Guru” informatico a cui chiedere informazioni e farsi raccontare avventure nel cyberspazio;
2. dall’altra era la nuova frontiera della criminalità con scambio di materiale protetto da copyright e pornografia⁷⁴.

In una sorta di adattamento delle teorie esposte da Dick Hebdige nel suo “Sottocultura – il fascino di uno stile innaturale”, si può affermare che, dopo un periodo di “libertà” nel quale la sottocultura hacker italiana era praticamente ignorata soprattutto dai mezzi di comunicazione, ci fù il momento dell’integrazione ideologica da parte della cultura dominante⁷⁵.

Come già Tom Tatum fece negli USA nel 1982 creando lo Show televisivo “Wizard vs Wizard” nel quale sette hackers si sfidavano ai videogiochi, anche in Italia l’interesse dei media si basa principalmente sull’aspetto, si passi il termine, “circense” della questione. Alla fine degli anni 80, sulla

⁷³ E il più delle volte si trovava.

⁷⁴ Usando un gergo da “Guerre Stellari” si può affermare che alla prima definizione appartengono gli hackers “puri” mentre alla seconda fanno parte i cosiddetti “Dark Side hacker”.

scia del successo del film “WarGames”⁷⁶, in tv cominciano a circolare servizi sulla genialità di determinati ragazzi e sulla pericolosità delle loro azioni con un computer. Il tutto con lo scopo di esorcizzare l’eventuale voglia di “distruggere il mondo” innestata nei ragazzi dal suddetto film.

Accanto all’aspetto di massa rappresentato dagli show televisivi o dagli articoli sui giornali, se ne sviluppa un altro più “nascosto” rappresentato dalle comunità virtuali. Le più importanti nascono a Roma (Agorà e MCLink) e a Milano, dove la rete “Galactica” fu la prima che permise una connessione full-time alla neonata Internet ad un prezzo bassissimo per i tempi⁷⁷.

L’ingresso in Italia della tecnologia “Fidonet” permise, oltre che connessioni veloci anche con computer piuttosto lenti, grazie al concetto di “Matrix” creato da Tom Jennings lo scambio di e-mail sulle BBS collegate.

Ciò permise un aumento quantitativo e qualitativo delle connessioni alla rete: più persone rappresentavano più temi da affrontare e su cui discutere.

Unica pecca la policy troppo rigida che pretendeva, ad esempio, il controllo da parte dei sysop⁷⁸ del contenuto dei messaggi scambiati all’interno della BBS, rigorosamente non crittografati. Riassumendo:

- Il sysop è responsabile delle azioni dei suoi utenti;
- Il sysop è responsabile dei contenuti dei messaggi che passano dal suo nodo;

⁷⁵ Come detto questo è un adattamento personale della teoria esposta in: Dick Hebdige, “Sottocultura – il fascino di uno stile innaturale”, Milano, Costa & Nolan, 2000, pp 101-107.

⁷⁶ Nel film un ragazzo, che potremmo definire hacker, con il suo computer, inconsapevolmente, rischia di causare una guerra termo-nucleare. Il film è divenuto presto un “cult” movie tra gli appassionati di informatica. “Wargames” di John Badham, MGM, 1983.

⁷⁷ 200.000 lire. Era il 1988.

⁷⁸ I sysop erano coloro che amministravano la BBS.

- Il sysop ha il diritto di vedere la posta dei suoi utenti;
- La crittografia è vietata;
- Argomenti e contenuti critici, specie se espressi con linguaggio “seccante”, non possono trovare posto nelle aree Fidonet. (Chiccarelli e Monti, 1997, pag 99).

Accanto a questa politica riguardante i messaggi, c'è quella che affronta il problema della privacy⁷⁹:

- Non siamo in grado di garantirla;
- Che intende farlo se ne assume tutti gli oneri;
- Considerando che alcuni Stati hanno una normativa specifica che tutela la riservatezza dei messaggi, valutate se è il caso di assumersi la responsabilità di occuparsene. (Chiccarelli e Monti, 1997, pag 98).

Queste regole portarono alla chiusura dell'area “Cybernet” nella quale si discuteva liberamente di Hacking, phreaking e tecnologia in generale. Da una costola della suddetta area di discussione nacque “Decoder”⁸⁰, il centro italiano più importante per la discussione sui temi “caldi” dell'informatica: è da gruppi come questo che iniziarono i primi hacking alla rete con i furti, ad esempi, dei primi anni 90 del famoso “numba”⁸¹ (storpiatura dell'inglese “number”) che permetteva la connessione gratuita a spese dell'allora SIP.

L'Hacking in Italia era questo: prendere numeri di telefono per l'accesso telefonico gratuito ad Internet e farlo circolare liberamente, scambiare

⁷⁹ Mettendo in risalto, così, il fatto che non è un problema dei giorni nostri ma veniva affrontato anche prima dello sviluppo di massa di Internet

⁸⁰ Gruppo storico di informatici che diedero vita anche ad una rivista “Decoder”. Attualmente gestiscono la casa editrice milanese “Shake”.

⁸¹ 167-12837. Dato principalmente ad organi di stampa ma finito su moltissime BBS.

giochi e programmi sulle varie BBS e, qualche volta, provare l'ebbrezza di "bucare"⁸² qualche sito, magari istituzionale.

Soprattutto se giovani, gli hackers hanno una falsa percezione delle azioni da loro compiute: grazie alla mediazione del computer che si frappone tra loro e la vittima, si può affermare che la sensazione che si ha è quella di videogiocare. In molte ricerche sulla personalità "Hacker" si sono riscontrati tratti tipici come l'introversione e la volontà di perseguire un'ideale, "danneggiare il sistema informatico per mostrarlo/mostrarmi che sono in grado di farlo e per aumentare il livello di autostima" (Strano, 2003). Sempre nell'ambito dei tratti tipici della personalità, si riscontra la maggior parte delle volte, la volontà di essere considerati all'interno della comunità hacker.

Mancando, ieri come oggi, una legislazione precisa sull'argomento informatico, ci si sentiva liberi di muoversi nel cyberspazio italiano. Nei primi anni 90, ad esempio, si potevano acquistare per poche lire nelle edicole, cassette per il Commodore 64, contenenti videogiochi che, se comprati nei negozi specializzati, sarebbero costati molto di più.

Il discorso affrontato nel primo capitolo di questo lavoro sull'importanza di avere regole precise torna e, in questo caso, si evince l'ulteriore considerazione che una situazione di confusione legislativa può portare qualcuno a sentirsi al di sopra della legge.

⁸² Ossia riuscire a cambiare faccia ai siti Internet.

3.2 Dalle reti alla Rete

Poco tempo dopo l'uscita in Italia di "Giro di vite contro gli hackers" di Bruce Sterling, nel nostro paese comincia l'operazione "Hardware 1": "la più vasta operazione di polizia mai condotta nei confronti della telematica amatoriale"⁸³ (Chiccarelli e Monti, 1997, pag 114).

Il libro dello scrittore di fantascienza texano narra gli eventi dell'operazione "Sundevil"⁸⁴ degli anni 1990 – 1991 durante la quale, negli Stati Uniti, ci furono una serie di sequestri di materiale informatico, irruzioni nelle case di ragazzi e, si può affermare, fu l'inizio della rappresentazione dell'hacker "cattivo".

A differenza del caso statunitense dove l'attenzione delle forze dell'ordine fu concentrata in particolare sul gruppo "Legion of Doom", in Italia ci fu un'indagine su praticamente tutto l'ambiente telematico. L'operazione "Hardware I" giunse in un periodo di mutazioni storiche nell'ambiente informatico: si stava passando dalla BBS ad Internet o, per dirla come molti protagonisti di allora, da un concetto libero di rete ad uno prettamente commerciale.

Fino a quel momento l'informatica si concentrava sull'aumento dell'efficienza del PC, permettendo "viaggi" nelle BBS anche con elaboratori vecchi di qualche anno. Con l'avvento della Rete con la "R" maiuscola le cose cambiano radicalmente e comincia la corsa sfrenata all'ultimo ritrovato della tecnologia: molti software, compresi i browser per navigare nella rete, non funzionano se non si ha una macchina recente.

⁸³ Quando gli giunse la notizia, Sterling commentò: "Whoopee. This ought to do wonders for sales of my Italian law-and-disorder opus, Giro di Vite contro gli hackers".

⁸⁴ Si veda il capitolo 2.

L'originario concetto di cultura informatica come "libera circolazione delle idee" diventa "remunerativa circolazione di hardware".

Non solo.

Se un esile tentativo di alfabetizzazione informatica era stato fatto dai "pionieri" italiani con manuali scaricati nottetempo da BBS straniere o, molte volte, scritti da soli, dal 1994, anno dell'operazione "Hardware 1" e del "Netbang", ossia l'aumento esponenziale delle connessioni ad Internet, si passa ad una conoscenza che si ferma a concetti basilari buoni soltanto per usare determinati sistemi operativi e software di base: "è come se Gutenberg fosse vissuto per stampare giornali di pettegolezzi"(Gubitosa, "Oltre Internet", 2001, documento on-line).

In questa atmosfera di cambiamento l'undici maggio 1994 dalle procure di Torino e Pesaro scatta l'operazione di polizia di cui sopra. Dal capoluogo piemontese l'indagine parte grazie alla Guardia di Finanza che, dopo essersi collegata a numerose BBS ed aver intrattenuto rapporti con molti frequentatori delle bacheche virtuali, individua dodici BBS "pirata" nelle quali veniva scambiato materiale protetto da copyright.

Discorso diverso da Pesaro dove vengono effettuati sequestri a tappeto sospettando l'esistenza di una vera e propria rete di duplicazione e vendita di software protetto. Molti protagonisti di quelle giornate ricordano il sequestro non solo del computer e di materiale informatico ma anche dei tappetini del mouse, facendo intendere come la materia informatica era ancora da scoprire anche per le forze dell'ordine.

Bruce Sterling, tentando un paragone tra l'operazione "Sundevil" americana e l' "Hardware I" italiana, disse: "Nel maggio 1994 la polizia ha sferrato un

attacco contro i BBS italiani con uno spiegamento di forze che era almeno il doppio di quelle impiegate nella “Operation Sundevil” negli Stati Uniti – probabilmente cinque volte più grande. Questa è la più massiccia operazione di sequestri di servizi telematici nella storia mondiale. La Polizia italiana non è stata la prima a organizzare un attacco su larga scala contro i servizi di rete, ma lo ha fatto con più energia e violenza di chiunque altro al mondo.” (Bruce Sterling in “1994, 2004...’1984’ la storia continua” di Giancarlo Livraghi, 2004, www.interlex.it).

Il caos susseguente questa ondata di perquisizioni e sequestri provocò prevalentemente due effetti: i pirati informatici si nascosero aspettando che la tempesta fosse passata; molti gestori di BBS per paura⁸⁵ chiusero i loro nodi, a volte con dichiarazioni sconcertanti come: “Vi terrò informati sulla vicenda per quanto mi sarà possibile e fino a quando sarò in grado di farlo...credetemi da come si stanno mettendo le cose temo che presto giungerà anche la mia ora”.

Tra questi anche Giorgio Rutigliano, ovvero colui che portò la rete Fidonet in Italia.

I titoli dei giornali di quei giorni passavano da un "Caccia ai pirati dell'informatica"⁸⁶ (“La Repubblica” del 13 maggio 1994) a "Scoperta gang di pirati informatici"⁸⁷ (“La Stampa” del 19/5/94), portando un certo panico nel cittadino comune non ancora informatizzato, il quale poteva leggere: “(...)E dietro il culto di un hobby, praticato a livelli professionali, l’ipotesi

⁸⁵ Molti gestori non erano ragazzi ma padri di famiglia.

⁸⁶ Articolo a cura di Claudio Gerino.

⁸⁷ In particolare su “La Stampa” si poteva leggere: “All’anagrafe risultano impiegati di banca, disoccupati, studenti. In realtà sono “hackers”, “pirati informatici”, esperti di software in grado di soffiare ai produttori con sofisticati mezzi telematici, costosi

di un traffico internazionale di tecnologie avanzate” (“Stroncato un traffico di floppy e computer” di Giorgio D’Aquino, “Avvenire” del 15 maggio 1994).

Di contro alcuni organi di stampa davano risalto ai protagonisti dell’accaduto: “Il Manifesto” del 21 maggio 1994 titolava "The Italian Crackdown" e all’interno dell’articolo Ermanno "Gomma" Guarneri, fondatore del gruppo “Decoder” e della casa editrice milanese “Shake”, spiegava come si stava evolvendo la questione dando un quadro piuttosto pessimista “Quello a cui si assiste e' una sorta di supplizio di tantalo: ormai ogni responsabile di BBS aspetta il suo turno per la perquisizione, il sequestro e l'incriminazione.”

L’eco dell’operazione “Hardware I” arriva anche all’estero con articoli su giornali e pagine web sull’argomento: l’articolo sul “Time” del 13 giugno 1994 "Nabbing the pirates of cyberspace", a firma Philyp Elmer-Dewitt, inquadrava l’evento in un’ottica “orwelliana”, dando anche una motivazione politica affermando che “It was the most dramatic move yet in a determined -- and some say increasingly desperate -- effort by governments around the world to curb the spread of software piracy.(...) But government actions to stem the losses may be causing more problems than they solve. The Italian campaign, which began just as the newly elected right-wing government of media tycoon Silvio Berlusconi took office, hit largely left-leaning bulletin boards. And it is seen by some Italians as an ill-disguised attempt to suppress free speech on a troublesome new medium.” ; l’Electronic Frontier Foundation, l’associazione nata a difesa dei diritti digitali dopo l’operazione

programmi informatici di contabilità e videoscrittura, gestione aziendale, sistemi operativi e videogames.”

“Sundevil” americana, per voce di Stanton McCandlish affermò: "This is a prime example of what happens when ignorant law enforcement butts heads with the online world. This is why getting police and other agencies up to speed, not to mention updating the law, is so important."⁸⁸

La situazione diventò ancora più grave quando all’inizio di giugno 1994 venne colpita l’associazione pacifista “Peacelink”⁸⁹. Il “collegamento di pace” (libera traduzione della parola “peacelink”) nasce nel 1991 da un’idea di Alessandro Marescotti e Marino Marinelli. Nucleo centrale dell’associazione era, ed è, la discussione su temi quali la solidarietà, il volontariato e, soprattutto, il pacifismo. Mentre in Italia si stava sperimentando la rete Videotel, Peacelink offriva gratuitamente servizi per navigare nella rete con mezzi tecnologici più evoluti rispetto a quelli tradizionali usati dalla SIP. Con il lavoro di Giovanni Pugliese, uno dei primi amministratori della rete telematica Fidonet, l’associazione pacifista, nel 1992, divenne una rete autonoma⁹⁰. Peacelink fu un importante centro di solidarietà durante la guerra in Iraq del 1991 e nella missione di pace a Sarajevo nel 1992 e 1993: “PeaceLink non svolgeva alcuna attività sospetta ma un’azione di promozione della solidarietà alla luce del sole” (Alessandro Marescotti, documento on-line sul decennale dell’associazione “PeaceLink”, www.peacelink.it, 2001).

Il controllo della Finanza avvenne sul computer di Giovanni Pugliese nel quale venne trovata una copia non registrata di un software permettendo, in questo modo, il sequestro e la relativa chiusura della bacheca virtuale “per avere a fini di lucro detenuto a scopo commerciale programmi per

⁸⁸ Da “Wired Magazine” 2.08 dell’agosto 1994, pagina 29. Articolo “Hacker Crackdowns, italian style” di David Pescovitz.

⁸⁹ www.peacelink.it

elaboratore abusivamente duplicati” (Alessandro Marescotti, “Condannato per detenzione di word”, documento on-line, www.peacelink.it). L’errore grave fu quello di espandere l’accusa da Giovanni Pugliese all’intera rete PeaceLink: il programma sotto accusa era inserito nel computer di Pugliese⁹¹ e non all’interno della rete la quale, quindi, non poteva essere un centro di smistamento di software copiato illegalmente.

Durissime furono le reazioni da parte sia degli utenti dell’associazione che da vari schieramenti politici dai quali partirono numerose interrogazioni parlamentari: sorgeva, ragionevolmente, il dubbio che fosse stata colpita “PeaceLink” con un banale pretesto informatico. Il processo si concluse con una piena assoluzione ma i fatti di “Peacelink” rappresentarono il punto di chiusura per la telematica conosciuta fino ad allora.

Il “Crackdown”⁹² italiano portò alla formazione dell’ “ALCEI”, Associazione per la libertà nella comunicazione elettronica interattiva⁹³. L’associazione nacque, così come l’americana “Electronic Frontier Foundation” dopo l’operazione “Sundevil” descritta nel secondo capitolo, con l’obiettivo di tutelare i diritti del nuovo “individuo digitale” che si stava formando grazie alle nuove infrastrutture informatiche.

L’operazione “Hardware I” svelò alcuni lati dell’informatica italiana: da una parte ci si accorse che il personal computer si stava imponendo come nuovo mezzo di comunicazione con tutti i pro, scambio in tempo reale di messaggi e, con Internet che espandeva il suo raggio di azione, possibilità

⁹⁰ Nel 1991 la rete PeaceLink era giocoforza appoggiata su Fidonet. Dal 1992 divenne una rete autonoma soprattutto per motivi di policy (par 3.1).

⁹¹ Il software era anche installato così da non permettere lo scambio.

⁹² In un unico vocabolo si racchiude il significato di disfatta, crollo.

praticamente infinite di raccogliere qualsiasi tipo di informazione, e i contro, ossia la questione di come limitare un mezzo di comunicazione potenzialmente illimitato; dall'altra parte la tendenza a pensare che il personal computer potesse essere usato solamente da ragazzini dediti solamente ai videogiochi, era stata soppiantata dal fatto che, nel 1994, erano pochissimi gli adolescenti on-line mentre erano molti i professionisti del settore con una doppia "vita tecnologica" che li vedeva di giorno a programmare presso le aziende informatiche e di sera immersi nella telematica amatoriale.

3.3 Evoluzioni

Con l'ingresso in Italia di Internet, e del servizio commerciale Video On Line⁹⁴ cambia il ruolo della rete: si tende a dare più importanza alla forma e non al contenuto.

Con Internet molti si inventano "provider" approfittando dell'improvvisa voglia di cyberspazio. Trovandosi quasi sempre in difficoltà e volendo fare sempre più affari, questi avventori furono "costretti" ad assumere quelli che fino a poco tempo prima venivano additati come criminali: gli hackers. Questi ultimi si ritrovarono ad essere pagati per fare quello che gli piaceva di più ed inoltre potevano usare computer potenti per sperimentare: l'hobby preferito si trasforma in lavoro e se prima l'impegno giornaliero era per entrare in qualche sito, ora lo scopo del lavoro era l'esatto contrario.

Negli anni successivi alle operazioni di Polizia⁹⁵ sono nate numerose riviste on-line dedicate interamente all'underground informatico come "Newbies"

⁹³ www.alcei.it

⁹⁴ Grazie all'imprenditore sardo Nicola Grauso.

e “The Black Page”, nelle quali, oltre a trovare racconti interessanti di notti passate davanti al computer nel tentativo di entrare in qualche database, si trovavano articoli del genere: “con questo articolo cercherò di insegnarvi a crackare un programma, in particolare attaccheremo e sproteggeremo 3D Mark 99 Pro.”(Newbies, n°3), seguito dal solito avviso che in qualche modo tenta di de-responsabilizzare l’autore dell’articolo: “PREMETTO INNANZITUTTO CHE NON MI ASSUMO NESSUNA RESPONSABILITA' SULL'USO CHE FARETE DI QUESTO ARTICOLO”⁹⁶.

Il bisogno di ritrovarsi dopo la dispersione causata dal Crackdown portò alla organizzazione degli “Hack-IT”, ossia delle riunioni annuali nelle quali in pochi giorni si poteva assistere a seminari, lezioni di programmazione e discussioni sull’hacking con uno spirito molto simile all’americano “Homebrew”⁹⁷. Anche se molti, ultimamente, si sono lamentati per l’organizzazione di questi avvenimenti dedicati troppo al lato spettacolare dell’hacking, bisogna dire che tramite la visione di queste manifestazioni ci si accorge che la scena hacker italiana esiste ed è attiva.

Questo si evince anche dall’analisi dei dati del “Rapporto 2004 sulle segnalazioni ricevute”⁹⁸, documento redatto dal CERT-IT, Computer Emergency Response Team Italiano⁹⁹.

⁹⁵ Dopo la già citata “Hardware I” ci furono altre tra cui “Gift sex” incentrata sulla pedo-pornografia.

⁹⁶ Questo tipo di avviso è presente nella maggior parte delle “dichiarazioni” dei gruppi di Crackers. Quello che si trova più spesso è “If you like this software, buy it” (se ti piace questo software, compralo).

⁹⁷ Cap 2.1.

⁹⁸ Che raccoglie i dati sulle segnalazioni del 2003.

⁹⁹ <http://cert-it.dico.unimi.it>

Il Cert-It, gruppo di ricerca nato nel 1994 nel Dipartimento di Informatica e Comunicazione dell'Università degli studi di Milano, opera nel settore della sicurezza dei sistemi informatici. Con il rapporto annuale c'è la possibilità di avere informazioni molto dettagliate sulla natura degli attacchi e sulla qualità della sicurezza informatica; dall'altra parte c'è l'ambito della ricerca che permette di studiare metodi sempre innovativi nel campo della difesa dei sistemi.

Nel rapporto del 2004 si nota come l'attacco più usato dagli hackers nostrani è il cosiddetto "Computer fingerprinting" (554 casi) ossia tutte quelle azioni usate per avere informazioni sul computer obiettivo dell'attacco; mentre al secondo posto si trovano i tentativi di intrusione non autorizzata all'interno di sistemi informatici.

I dati riguardanti la distribuzione degli attaccanti e la distribuzione delle vittime ci fanno notare come il numero più alto degli attacchi proviene da telecomitalia.it (530 segnalazioni), ma bisogna sottolineare che il dato potrebbe essere falsato dal fatto che difficilmente un hacker attacca direttamente dal proprio computer perché tende a "rimbalzare" da vari sistemi precedentemente compromessi; le vittime sono, la maggior parte delle volte, i domini .it (997 casi).

Unendo a questi dati quelli del "Symantec Internet Security Threat Report"¹⁰⁰ della Symantec corporation, creatrice di numerosi software per la difesa del proprio computer come il famosissimo Norton Antivirus, si può affermare che i pericoli per i sistemi sono aumentati: il numero degli attacchi è cresciuto del 19% rispetto al 2002, la maggior parte dei quali

¹⁰⁰ Del 16 ottobre 2003, www.symantec.com.

compiuti con worm¹⁰¹; nella sola prima metà del 2003 sono stati individuati 994 nuovi virus; i casi di infezione per l'uso di software peer-to-peer¹⁰² e di messaggistica istantanea sono aumentati del 400% rispetto al 2002.

Accanto a questi dati sconcertanti bisogna affermare che sta aumentando in Italia, anche se molto lentamente, la consapevolezza da parte delle aziende del problema della sicurezza informatica. Secondo l'indagine "Ernst & Young – Global information security survey 2004" nel nostro paese sono in aumento sia gli strumenti per difendersi¹⁰³, sia il budget dedicato alla sicurezza.

L'interesse verso il fenomeno "Hacker" è cresciuto sia in strutture direttamente coinvolte nell'argomento come possono essere le aziende (informatiche e non), sia nell'ambito della comunicazione di massa. A titolo di esempio si è notato negli ultimi anni un considerevole aumento di riviste dedicate all'argomento alcune delle quali trattano la questione in maniera qualitativamente valida, mentre altre sfiorano solamente il tema "Hacker" lasciando la maggior parte dello spazio ai cosiddetti "tutorial"¹⁰⁴ su come diventare velocemente un "Kevin Mitnick".

Emblematico è, poi, l'aumento delle pagine web riguardanti l'argomento: digitando "Hacker" sul motore di ricerca "Google"¹⁰⁵ compaiono circa 387.000 pagine in italiano, che vanno da quelle di ambito professionale o di ricerca come www.dvara.net o www.bismark.it, a quelle di raccolta di

¹⁰¹ Ved. Glossario.

¹⁰² Ved. Glossario.

¹⁰³ Anche se spesso questo servizio è dato in appalto creando un fenomeno di decentralizzazione del settore della sicurezza informatica che potrebbe causare un minor controllo da parte dell'azienda centrale.

¹⁰⁴ Guide molto dettagliate.

¹⁰⁵ Ad oggi il motore di ricerca più usato.

software per un corso accelerato di hacking; eliminando il filtro di ricerca della lingua italiana si hanno circa 14.800.000 pagine web disponibili.

Il cambiamento del personaggio “Hacker” è stato affrontato anche nell’intervista a Raoul Chiesa - uno dei primi hacker (etici) italiani¹⁰⁶ ed oggi impegnato sul fronte della sicurezza informatica con la sua “@Mediaservice.net”¹⁰⁷ - il quale si dice “convinto dell’importanza di diffondere cultura in e sulla Rete, tramite una continua e sempre maggiore *informazione su tutto quello che gravita intorno ad essa*, con un occhio di riguardo alla vulnerabilità dei sistemi informatici ed alle continue evoluzioni tecnologiche, anche segno del cambiamento dei tempi.”¹⁰⁸

3.4 Intervista a Raoul Chiesa

Hacker, esperto di informatica, Lamer, Cracker, Hacker etico: come si possono distinguere oggi, considerando le potenzialità messe a disposizione dalla rete?

I fattori distintivi delle differenti figure esistenti nel mondo dell’hacking sono principalmente due: capacità tecniche (skill) e motivazione all’attacco.

Infatti, se da un lato un “Ethical Hacker” può avere uno skill estremamente elevato, dall’altro non compirà mai azioni criminose: questo fa sì che un “Ethical Hacker” non diventerà mai, ovviamente, un “Cracker”.

Viceversa, un “Lamer” è dotato di pochissime capacità tecniche, e non potrà mai compiere azioni né criminali (di un certo livello), nè tantomeno attacchi ad elevato contenuto tecnologico.

¹⁰⁶ Conosciuto come “Nobody”

¹⁰⁷ <http://@mediaservice.net>

¹⁰⁸ Dal “Curriculum Vitae” di Raoul Chiesa. Documento pubblico di “@Mediaservice.net”.

Questo, a mio avviso, è il solo metodo per distinguere le diverse tipologie di attaccanti: perché attaccano e come attaccano un “target”, un obiettivo.

Se l’hacker è considerato il “paladino” delle libertà informatiche, perché molti si pongono il problema di come frenare lo spirito e la voglia di ricerca? (rapporto hacker-leggi).

Ti posso rispondere che tutto ciò sta avvenendo, principalmente, per ignoranza sul fronte politico.

Prendiamo le recenti legislazioni antiterrorismo, tanto in territorio nord-americano quanto europeo: sono leggi che, di fatto, restringono (di molto) le possibilità di ricerca nel campo dell’I.T. A questo proposito ti consiglio due speech davvero interessanti, tenuti rispettivamente dal ricercatore Stefano “Raistlin” Zanero quando era nell’associazione Italian Black Hats (www.blackhats.it, “ethical hacking, unethical laws”) e dalla D.ssa Java Baloo (“Lawful interception of IP traffic: the european context”, www.blackhat.com).

Tornando alla tua domanda, le motivazioni sono due anche in questo caso: da una parte i mass-media, i quali in un ventennio hanno sradicato l’originale significato del termine hacker (così come ancora riportato oggi dal Jargon File) sino a farne una figura criminale; dall’altra parte troviamo invece i governi, gli utenti e le aziende che, “giustamente”, ritengono sia necessario fermare le azioni criminali degli “hacker”, e quindi accettano la stesura di nuove leggi restrittive, per “garantire la nostra sicurezza”. E’ un po’ come le telecamere a circuito chiuso nelle città: danno fastidio, certo, per la nostra privacy, ma se uno pensa che “e’ per il nostro bene e la nostra sicurezza”, allora tutto si accetta...

Di mio posso soltanto ricordare a questi legislatori come le maggiori scoperte di (in)sicurezza, negli ultimo vent’anni, siano state fatte proprio

grazie agli hacker: etici, professionisti come Kevin Mitnick e Kevin Poulsen o ragazzini alla Maphia Boy, queste sono le persone che hanno portato a galla insicurezze croniche le quali, senza di loro, non si sarebbero mai scoperte.

In Italia esiste, o è esistita, una scena hacker? Se sì, con quali caratteristiche precipue?

Certo, come in tutto il mondo, anche in Italia è esistita – ed esiste – una scena hacker, Con le sue particolarità e connotazioni, sia temporali che sociali.

La scena hacker italiana nasce durante la prima metà degli anni '80: il primo gruppo hacker di cui si ha notizia si chiamava “DTE 222”, dal nome del DNIC X.25 (prefisso internazionale di rete dati) italiano, “ITAPAC”.

La seconda ondata avviene tra il 1985 ed il 1994 (Pier's Group, il Videotel, le messaggerie e le BBS), mentre la terza “era” la si ebbe quando, anche in Italia, arrivò Internet, grazie a VOL (Video on-line) nel 1995.

Dal 1998/99 ad oggi siamo giunti alla quarta generazione, per non dire quinta: gli Script Kiddies hanno iniziato ad apparire (senza Internet, ciò sarebbe stato impossibile ed avremmo avuto solo i c.d. “lamer”), gli attacchi automatizzati sono divenuti uno standard, la globalizzazione ha fatto sì che Internet fosse presente ovunque.

Sul supplemento “@lpha” de “Il Sole 24 ore” del 9 settembre 2004, accanto ad un enorme “Barricatevi”, si poteva leggere “Ad agosto gli hackers hanno scatenato un’offensiva senza precedenti: investire in sicurezza è ormai d’obbligo”. Ma bisogna davvero avere così tanto timore degli hackers oppure la stampa crea un’ enfasi inutile? Come

trovi il rapporto stampa-hacker e tra hackers e mezzi di comunicazione di massa in generale?

Nell'agosto del 2004 non vi è stata alcuna "offensiva senza precedenti", vuoi anche perché chi produce Virus o Worm, o invia Spam, non è sicuramente "hacker", bensì un semplice criminale che utilizza la tecnologia per raggiungere i suoi scopi.

Quindi, nuovamente, torniamo alle già citate esagerazioni della stampa, ad un utilizzo quantomeno terroristico da parte della stampa stessa verso quello che "non è ben conosciuto".

Mi chiedo spesso perché i giornali non parlino mai degli hackers (etici) che scoprono vulnerabilità per il bene comune, di quelli che si accorgono di errori madornali nei software, applicazioni e trattamento dei dati personali...così come non si legge mai dell'utilizzo criminale che fanno i veri criminali della tecnologia..non ho mai letto articoli sulla mafia che usa la cifratura...come mai ?

Secondo te, è vero che oggi la maggior parte degli hackers ha perso lo spirito dei primi tempi e siede comodamente su poltrone da "Amministratore di sistema"? E' possibile fin da oggi tracciare una storia della metamorfosi degli hackers?

E' una domanda che si sente spesso, e non sono completamente d'accordo: anche in questo caso fare affermazioni del genere può divenire fuorviante, se si vuole analizzare seriamente un fenomeno così particolare come l'hacking, nel quale gli aspetti tecnologici, economici e sociali si mischiano incredibilmente.

Banalmente, questo "mistero" non è affatto ciò che sembra a primo acchito: nella vita di qualunque persona, in qualunque professione, c'è una crescita

personale, una maturità che si va ad acquisire durante il tempo, gli anni, maturando e diventando adulti.

Gli hacker non fanno altro che seguire questo iter: ritengo che una persona sarebbe davvero idiota se continuasse a comportarsi a 30 anni come si comportava a 15..... rendo l'idea ?

Quindi, se da un lato il violare un VAX/VMS a 15 anni mi permetteva di imparare il sistema operativo VMS e la security in ambienti mainframe, oggi gli OpenVMS li sottopongo a test di intrusione - autorizzato e pagato da un'azienda – proprio per verificarne le insicurezze. E' la stessa cosa che facevo 15 anni fa? Tecnicamente sì. Ma la sostanziale differenza è proprio nel modo in cui lo si fa: oggi è una professione, se non c'è autorizzazione e liberatoria non si procede, e così via.

In ultimo, abbiamo poi un fattore evolutivo e di "brain-input": da teenager, gli hacker acquisiscono moli di informazioni enormi, "lavorando" con orari, ritmi, stili e vite sociali davvero assurde; sono cose che si fanno, appunto, nell'adolescenza, ma difficilmente una persona arrivata ai 25, 28 o 30 anni ha ancora la forza fisica e mentale, il tempo materiale e soprattutto l'elasticità per continuare ad agire così.

Lo spirito hacker quindi resta, ma viene accompagnato ad un'evoluzione personale, un'avvenuta maturità, un modo diverso e forse più intelligente di ascoltare, imparare, acquisire know-how, fare ricerca, unire la propria passione al proprio lavoro.

Dall'intervista vengono fuori molti spunti interessanti, a partire dall'importante distinzione tra capacità tecniche, proprie degli hackers più "anziani" che hanno avuto la possibilità di arricchire le proprie conoscenze con la prima informatica, e l'analisi di come un obiettivo viene colpito.

I temi esposti nel primo capitolo del presente lavoro si ripresentano nella risposta alla seconda domanda nella quale ci si accorge di una certa perplessità da parte di Raoul Chiesa nei confronti di provvedimenti presi per la sicurezza non solo informatica. L'esempio delle telecamere rende in pieno l'idea di come sia molto difficile riuscire a separare il contesto della sicurezza dei cittadini e quello della protezione della privacy degli stessi da parte dei legislatori¹⁰⁹.

In tutto questo all'hacker viene riconosciuto il merito di aver fatto evolvere il campo delle tecnologie grazie alle sue scoperte e si sottolinea il fatto di come, la maggior parte delle volte, non ci sia la giusta riconoscenza. Questo perché si tende ad avere una scarsa conoscenza del fenomeno in questione e, di conseguenza, si dà più risalto ad "invasioni" di virus nella rete.

La situazione hacker italiana viene divisa in generazioni a seconda della tecnologia posseduta: oggi, con l'espansione globale di internet, siamo arrivati alla quarta, probabilmente la più "comoda" dal punto di vista tecnologico e di know-how in quanto, proprio grazie al cyberspazio, si possono trovare infinite risorse con una facilità sconosciuta alle precedenti generazioni.

¹⁰⁹ Si veda il capitolo 1, paragrafo 1.2.

Il nucleo dell'intervento di Raoul Chiesa sta nel discorso "evolutivo" dell'hacker: se lo spirito hacker si accosta ad una maturazione personale, sia tecnica che morale, allora si rimane "Hacker" anche se, magari, si è a capo di un'azienda informatica.

Fondamentale è, dunque, cercare di far evolvere quello che era una passione o un hobby, in una professione, cercando, però, di mantenere intatta l'etica hacker originaria¹¹⁰.

¹¹⁰ Questa posizione è molto vicina a quella esposta in Himanen P., 2001, "Etica Hacker", Milano, Feltrinelli.

CONCLUSIONI

Scrivere sulle nuove tecnologie è sempre complicato. Si ha la difficoltà di trovare le caratteristiche di elementi in continua evoluzione, come ad esempio il cyberspazio, non-luogo venuto alla luce soltanto pochi anni fa ma che ha preso sempre più importanza nell'ambito della comunicazione di massa, il quale è destinato ad essere il nostro campo d'azione per il futuro: lavoro, rapporti sociali e raccolta delle informazioni passeranno inesorabilmente attraverso i cavi telefonici.

In questo nuovo quadro è normale che si sviluppi una curiosità verso tutte le potenzialità del nuovo mezzo in questione. Nel presente lavoro si è descritta la figura affascinante dell'hacker, curioso per eccellenza, il quale si pone come protagonista nello sviluppo del cyberspazio. Cosa succede, però, se la curiosità innata dello "smanettone" si trasforma in intrusione in banche dati di grandi società o in modifiche non autorizzate su vari siti internet?

Qui sta il centro dei tre capitoli affrontati in precedenza: riuscire a capire quali vie segua la curiosità – o anche la voglia di imparare – per trasformarsi talvolta in crimine.

Se in un primo momento la domanda può sembrare troppo "estrema" – magari perché tutti abbiamo un pizzico di curiosità – dopo l'analisi dei vari aneddoti inseriti nel presente lavoro e, soprattutto, dei casi "Sundevil" e "Hardware I" ci si rende conto di come un dubbio venga fuori.

Possiamo davvero lasciare circolare liberamente personaggi come Kevin Mitnick, capace di penetrare praticamente in qualsiasi sistema informatico, giustificandolo solamente come curioso?

Ma d'altra parte, grazie proprio a questo tipo di persone, le maggiori falle di sicurezza dei sistemi informatici sono uscite fuori.

Come evidenziato nelle pagine precedenti, la ragione, probabilmente, sta nel mezzo. Con le distinzioni che nell'ambiente underground informatico sono venute fuori con gli anni si è voluto proteggere quello che di buono era stato fatto dalla comunità hacker – infatti la divisione hacker/cracker è venuta fuori proprio dai pionieri dei computer per non essere scambiati con chi “distruggeva” sistemi informatici - e, indirettamente, si è trovata una risposta alla domanda che permea questo lavoro: la curiosità si trasforma in crimine quando si è consapevoli di tale mutazione.

Un hacker etico, ad esempio, è consapevole di non creare danni entrando in una rete per trovare eventuali bachi, così come un cracker è consapevole dei danni che porterà il virus su cui sta lavorando.

La curiosità può essere la stessa, ma le conseguenze sono totalmente differenti.

Per provare a rispondere completamente alla questione bisogna tenere conto che gli elementi in gioco sono molti altri. Tra questi troviamo: la caratterizzazione sociale delle nuove tecnologie, l'uso del termine “hacker” da parte dei mezzi di comunicazione di massa e, ultimo ma non meno importante, la questione legislativa.

L'hacker, come si è visto, ha, al contrario del sistema legislativo, la dote di adeguarsi immediatamente alle nuove tecnologie, anzi, in molti casi, fa da anticipatore. Ed è, si pensa, proprio questa dote a far sì che il protagonista di questo lavoro sia trattato nella maggior parte dei casi con un certo timore.

Proprio questo timore porta ad una chiusura nell'ambito della legislazione in campo informatico. Una soluzione al problema può essere quella proposta da Nicholas Negroponte nel suo *Essere digitali*, ossia una mediazione tra individuo, in questo caso l'utente, e la nuova tecnologia: provare a capire dove si potrebbe arrivare usando in maniera adeguata i mezzi a nostra disposizione evitandone uno scorretto.

Sviluppare una curiosità, che non sfoci nell'illegalità, verso la tecnologia che ci circonda.

Questo processo dovrà comprendere sia i produttori di tecnologia che gli individui-utenti ma, soprattutto, coloro che devono pensare all'integrazione della tecnologia all'interno della società.

Ad esempio, bisognerebbe evitare, in futuro, di proporre brevetti per il software che limitano la libera programmazione, e, magari, sviluppare programmi per la comunicazione *in e sulla* rete per far capire a fondo tutte le potenzialità del mezzo di comunicazione.

In questa nuova situazione l'hacker, inteso come "esperto tecnologico", può davvero diventare un punto di riferimento per la comprensione della tecnologia e un alleato prezioso nella comprensione della comunicazione attraverso il cyberspazio.

Il rischio è quello di avere, in futuro, un aumento impressionante di nuove tecnologie accompagnato da un altrettanto elevata incomprendimento delle stesse.

RINGRAZIAMENTI

Un ringraziamento particolare va al Dottor Maione che mi ha dato la spinta a scrivere; al Dottor Di Lallo, inesauribile fonte di notizie nel campo della criminologia informatica; allo staff di Radio Mania, senza il quale molte cose non sarebbero state scritte; a Veruska, grazie alla quale le prime lettere di questo lavoro sono state scritte; a Simona, grazie alla quale sono state scritte le ultime.

Chiaramente un sincero ringraziamento va alla mia famiglia che mi ha sopportato durante tutto il periodo di scrittura.

Infine ringrazio Marco e Massimo Ceccarelli per l'inestimabile supporto.

BIBLIOGRAFIA

Carola Freschi A. e Leopardi L., 1998, “Una ragnatela sulla trasformazione”, City Lights Italia;

Chiccarelli S. e Monti A., 1997, “Spaghetti Hacker”, Milano, Apogeo;

DeFleur M. L. e Ball-Rokeach S. J., 1995, “Teorie delle comunicazioni di massa”, Bologna, Il Mulino;

Di Bona C., Ockman S., Stone M., 1999, “Open sources - voci dalla rivoluzione open source”, Milano, Apogeo;

Di Corinto A. e Tozzi T., 2002, “Hacktivism, la libertà nelle maglie della rete”, Roma, Manifestolibri;

Durkheim E., 1971, “La divisione del lavoro sociale”, Edizioni di Comunità, Milano, in Fallace R e Wolf A., 2000, “La teoria sociologica contemporanea”, Il mulino, Bologna;

Fallace R., Wolf A., 2000, “La teoria sociologica contemporanea”, Il mulino, Bologna;

Gibson W., 2003, “Neuromante”, Milano, Collezione Urania – Mondadori;

Hebdige D., 1979, “Sottocultura, il fascino di uno stile innaturale”, Milano, Costa & Nolan;

Himanen P., 2001, “Etica Hacker”, Milano, Feltrinelli;

Leary T., 1995, “Caos e cibercultura”, Apogeo-Urra;

- Lèvy P., 2002, “L’intelligenza collettiva. Per un’antropologia del cyberspazio”, Milano, Feltrinelli;
- Levy S., 2003, “HACKERS Gli eroi della rivoluzione informatica”, Milano, Shake ed.;
- Miconi A. (a cura di), 2000, “Introduzione alla mediologia”, Roma, Luca Sossella editore;
- Mitnick K. D. in collaborazione con Simon W. L., 2003, “L’arte dell’inganno, i consigli dell’Hacker più famoso del Mondo”, Milano, Feltrinelli;
- Orwell G., 2004, “1984”, Milano, Mondadori;
- Raymond E. S., 1999, “Breve storia sugli hacker”, Milano, Apogeo;
- Ricci Bitti P.E. e Zani B., 1983, “La comunicazione come processo sociale”, Bologna, Il Mulino;
- Scelsi R., 1994, “Cyberpunk”, Milano, Shake ed.;
- Scelsi R., 1994, “No Copyright”, Milano, Shake ed.;
- Stallman R., 2003, “Software libero, pensiero libero”, Ed. Stampa Alternativa/Nuovi Equilibri;
- Stephenson N., 1995, “Snow Crash”, Milano, Shake ed.;
- Sterling B., 2003, “Giro di vite contro gli Hackers”, Milano, Shake ed.;
- Stoll Clifford, 2000, “The Cuckoo’s egg. Tracking a spy through the maze of computer espionage”, Sperling & Kupfer;

Strano M., 2003, “Manuale di criminologia clinica”, Firenze, SEE;

Torvalds L. e Diamond D., 2001, “Rivoluzionario per caso”, Milano, Garzanti;

Williams S., 2002, “Codice Libero” , Milano, Apogeo;

Wolf M., 2000, “Gli effetti sociali dei Media” , Milano, Bompiani;

WEBGRAFIA

Agostini Y. e Chiesa R., “Storia ed etica Hacker”, dalla conferenza webb.it, Padova 6 Luglio 2002;

Associazione “Italian Black Hats” , “Ethical Hacking”, www.dvara.net;

Bernadotti F., “Hacker’s Programming Book”, www.bernadotti.it ;

Bernadotti F., “Storia Hacker italiana”, www.bernadotti.it ;

Berners-Lee, 16/04/1998, “Internet devasta la privacy”, www.repubblica.it;

Chiesa R., “Cosa Kevin David Mitnick non potrà fare nella sua vita: praticamente tutto...”, www.internos.it;

Chiesa R., “Il difficile rapporto tra hacking e marketing”, www.internos.it;

Chiesa R., “Le 10 regole dell’hacking”, www.internos.it;

Chiesa R., “Legalità, non legalità”, www.internos.it;

Chiesa R., “Who is who : Hackers chi sono? “, www.internos.it ;

CIRM, 2003, “Gli italiani lo sanno: siamo già tutti a rischio”
www.raiuno.rai.it/static/immagine/superquarkdossiersondaggio31.pdf;

EUROBAROMETRO, settembre 2003-dicembre 2003, “Data Protection”,
www.cambio.unifi.it, laboratorio di ricerca sulle trasformazioni sociali dell’Università degli studi di Firenze;

Gubitosa C., “Italian Crackdown”, www.apogeonline.com;

Gubitosa C., “La vera storia di Internet”, www.apogeonline.com;

Gubitosa C., “Oltre Internet”, www.apogeonline.com;

Livraghi G., 2004, “1994, 2004...’1984’ la storia continua”,
www.interlex.it;

Marescotti, A., “Condannato per detenzione di word”, www.peacelink.it;

McKenziem, 2001, “Hacker Manifesto 2.0”, www.dvara.net;

Raymond E. S., 16 luglio 2003, “How To Become A Hacker”, rev 1.20,
www.dvara.net;

Raymond E. S., 24 agosto 2000, “The Cathedral and the Bazaar”,
www.dvara.net;

Raymond E. S., 18 giugno 1998, “The Hacker Dictionary (Jargon File)”,
versione 1.90, www.dvara.net;

Rinaldi A. e Florida Atlantic University, 1998, “Netiquette”,
<http://wise.fau.edu/netiquette/net/index.htm>;

Strano M., 2003, “La psicologia degli hackers - ICT security 2003”,
www.criminologia.org;

Symantec corporation, 16 ottobre 2003, “Symantec Internet Security Threat
Report”, www.symantec.com;

The Mentor, “Hacker Manifesto”, da www.dvara.net.

DOCUMENTI VARI

CENSIS, 2004, “XXXVIII – Rapporto sulla situazione sociale del paese”, Roma;

CERT-IT, 2004, “Rapporto 2004 sulle segnalazioni ricevute”, Milano;

“@lpha”, 9 settembre 2004, supplemento di approfondimento scientifico de “Il Sole 24 ore”;

D’Aquino G., 15 maggio 1994, “Stroncato un traffico di floppy e computer”, Avvenire;

Elmer-Dewitt P., 13 giugno 1994, "Nabbing the pirates of cyberspace", Time;

Guarnieri E., 21 maggio 1994, “The italian crackdown”, Il Manifesto;

La Posta L., 14 febbraio 2003, “Hackers usati come parafulmine”, Il Sole 24 ore;

Microsoft Corporation, 2002, “EULA”;

Mola G., 27 febbraio 1999, “Anarchici o truffatori – la vera storia degli hackers”, La Repubblica;

Pescovitz D., agosto 1994, “Hacker Crackdowns, italian style”, Wired Magazine 2.08;

Rivista “Decoder”, 1995, Shake ed.;

Rivista “Hackers & C”, 2004, Piscopo Editore;

Rivista on-line “Newbies”;

Rivista on-line “The Black page”;

SITI VISITATI

www.kevinmitnick.com

www.spaghetthacker.it

www.puntoinformatico.it

www.dvara.net

www.apogeonline.com

www.storiainformatica.it

www.garzantilinguistica.it

www.apogeonline.com

www.alcei.it

www.clusit.it

www.privacy.it

www.p2pforum.it

www.fastsharing.it

www.2600.org

GLOSSARIO

Avatar: immagine che tende a configurarsi come la rappresentazione digitale dell'io mentale del soggetto.

BBS: "Bulletin Board System". Una sorta di bacheca virtuale nella quale si scambiavano files e messaggi. La "madre" dell'odierna Internet.

Cracker: secondo lo "Jargon File", redatto originariamente da Eric S. Raymond ma divenuto ben presto documento pubblico, Cracker è colui che rompe la sicurezza dei sistemi informatici. Il termine fu coniato dagli hackers per impedire la confusione di termini usata dalla stampa.

Cyberpunk: filone fantascientifico "figlio" delle nuove tecnologie, in particolare della rete, contraddistinto da "una visione ultratecnologica del futuro, un'azione veloce, una costruzione serrata e un disprezzo per tutto quello che è lento e noioso". (Michael Swanwick citato in "Il cyberpunk come movimento", documento on-line, www.fantascienza.com). Tra gli autori più importanti si possono citare: Bruce Sterling, autore della prima raccolta del genere cyberpunk "Mirrorshade" (Milano, Mondadori, 2003); William Gibson, autore del "Neuromante", (Milano, Mondadori, 2003) considerato il primo libro del filone; Patricia K. Cardigan; Neal Stephenson, autore di "Snow Crash" (Milano, Shake ed., 1995), considerato post-cyberpunk.

Cyberspazio: 1. la matrice o "information-space" che si apre durante una connessione con elettrodi installati nel corpo umano; 2. una valida alternativa al mondo reale così come suggerito, ad esempio, dal film "Matrix". Tale rappresentazione fu molto usata durante gli anni del netbang, ossia dell'aumento esponenziale delle connessioni ad Internet; 3. la situazione in cui si trova un hacker durante una sessione di hacking. Tentando di unire le diverse definizioni si può affermare che il Cyberspazio è un non-luogo, in quanto non esistente fisicamente, nel quale domina la comunicazione orizzontale, non gerarchica e interattiva in cui non c'è una divisione netta tra emittente e destinatario del messaggio.

Dialer: software creato per connettere il computer ad una particolare linea telefonica.

Download: operazione che permette di "scaricare" sul proprio computer dei dati presenti nella rete.

Firewall: software usato per la protezione del computer da eventuali intrusioni.

Free Software: concetto nato negli anni 70 grazie a Richard Stallman e al suo programma “Emacs”. La dicitura “Free” sta per libero e non gratuito, come molti interpretarono nei primi anni di diffusione, caratterizzando un tipo di software che permetta la visione e la modifica del codice.

Hacker: negli anni 50 e 60 all’interno del Mit contraddistingueva colui che riusciva in qualche impresa tecnologica molto difficile. Con l’andare avanti del tempo il sostantivo ha acquisito una diversa connotazione, positiva o negativa, a seconda del contesto usato. Un Hacker è un esperto informatico che si muove con disinvoltura all’interno della rete, questa sua capacità lo porta anche ad essere indicato come il principale “male” dell’informatica.

Ingegneria sociale: 1. una modalità particolarmente amata nel mondo degli Hacker che sfruttano l’impreparazione e l’ingenuità degli utenti per ottenere informazioni riservate. Creando un indirizzo di posta elettronica, scelto in modo tale da trarre in inganno il ricevente, possono inviare delle e-mail che sembrano arrivare dal provider stesso in cui chiedono di modificare la password di accesso in uso e di comunicarla immediatamente tramite posta elettronica. Gli utenti che lo faranno consegneranno la chiave di accesso ai malintenzionati di turno (definizione tratta dal documento on-line “I consigli della Polizia di Stato a tutti i navigatori”, www.poliziadistato.it); 2. “Uso del proprio ascendente e delle capacità di persuasione per ingannare gli altri.” (Mitnick, 2003, pag. 3).

Internet: la rete che collega milioni di computer in tutto il mondo.

Lamer: nel gergo Hacker, colui che usa software già programmato, senza studiarlo, per commettere illeciti sulla rete.

Link: collegamento ipertestuale contenuto all’interno delle pagine web.

Linux: sistema operativo alternativo al più famoso “Microsoft Windows” creato nel 1991 da Linus Torvalds e divenuto un esempio per la programmazione open-source.

Log, files di -: registrano tutti gli eventi, anomali e non, che si verificano all’interno di un personal computer.

Matrix: 1. tecnologia creata da Tom Jennings la quale permetteva lo scambio di e-mail sulle BBS; 2. nella recente trilogia cinematografica “Matrix” - fratelli Wachowski, Warner Bros, 1999/2004 – figurava un’estrema rappresentazione del cyberspazio.

Netbang: periodo all’inizio degli anni 90 nel quale ci fu un sensibile aumento di connessioni ad Internet.

Netiquette: documento nato nella seconda metà degli anni 90 dalla collaborazione dei primi gestori della neo-nata Internet nel quale si possono leggere le regole da seguire per un buon uso di Internet.

Neuromante: libro di William Gibson uscito nel 1984. Fu un testo rivoluzionario in quanto si parlava di cyberspazio e di reti neurali, concetti sviluppati anni dopo l'uscita del romanzo.

Open Source: si definisce tale un programma il cui codice è visibile e modificabile.

P2P (peer-to-peer): si dice di rete locale in cui ognuno dei computer collegati ha al pari di tutti gli altri accesso alle risorse comuni senza che vi sia un'unità di controllo dedicata come server. (definizione da: www.garzantilinguistica.it).

Phreaker: "Crackatore" di telefoni. Comparsi nei primi anni di hacking, sperimentavano qualsiasi uso del telefono cercando in qualche modo di effettuare chiamate gratuite.

Provider: società adibita a fornire il servizio di connessione Internet.

Reverse engineering: tecnica che permette di rendere leggibile (aprire, o come si dice in termini informatici, "decompilare") il codice di un programma chiuso ("compilato").

Server: computer utilizzati per il salvataggio di dati e gestione di alcune funzioni tra le quali, ad esempio, la posta elettronica.

Spamming: ricezione di posta indesiderata. Seppur non rappresenti un problema dal punto di vista della sicurezza informatica, si configura come una violazione della privacy.

Spyware: software con lo scopo di comunicare allo sviluppatore le abitudini di navigazione del proprietario del pc nel quale il programma è installato. Negli ultimi anni la diffusione di tale software è aumentata in modo esponenziale.

Trojan Horse: (Cavalli di Troia) software che si nascondono in dati innocui per poi installarsi nel sistema. Vengono usati per spiare e rubare dati sensibili come le password di sistema.

Virus: sono il tipo di software dannoso più famoso. Hanno la capacità di autoreplicarsi e, alcuni, quella di nascondersi anche al più evoluto anti-virus. Anche se la maggior parte dei virus crea problemi, ne esistono alcuni che non comportano nessun danno al pc. Il primo è stato programmato da Elk Cloner nel 1982 per Apple II.

Worm: forma molto diffusa di codice maligno. Questo programma è in grado di riprodursi all'interno del computer causando, molto spesso, danni rilevanti. Per propagarsi usa sia la posta elettronica che altri strumenti di rete. Nel 1988 lo studente americano Robert Morris provoca il blocco quasi totale delle reti con il primo worm.