Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea in Scienze di Internet

IDENTITA', PRESTIGIO ED ETICA:

analisi antropologica delle motivazioni e delle soddisfazioni degli Hackers

Tesi di Laurea in Economia dell'informazione

Relatore:
Chiar.mo Prof.
Diego Lanzi

Presentata da:
Alessandro Vignoli
Mat. 0000213482

I

2009-2010

Indice

Sviluppo di Internet e origini dell'Hacking

1.1 Internet, fasi storiche.

La rete Internet nasce negli anni cinquanta, nell'ambito dei dipartimenti per la difesa e nelle grandi università americane, istituiti con ingenti somme di denaro a disposizione, che hanno contribuito in modo decisivo allo sviluppo del cyberspazio (o spazio virtuale).

Sin dall'inizio della Rete l'applicazione maggiormente diffusa tra gli utenti è senza dubbio la posta elettronica, sviluppata negli anni settanta da Ray Tomlinson, programmatore della *BBN*[1].
Tutte le innovazioni tecnologiche legate ad Internet che lo portano ad essere il primo mezzo di comunicazione mondiale, sono, almeno all'inizio della storia, il risultato di processi diretti allo sviluppo ed alla conoscenza, non al lucro.
Internet non nasce nel mondo dell'impresa e l'obiettivo che guida i ricercatori che lo hanno creato è lo sviluppo e la condivisione della conoscenza.
Proprio da questo spirito di libertà e condivisione, alcuni operatori traggono le loro tesi per garantire facilità di acceso e possibilità di sviluppo della rete, senza dover incorrere nelle limitazioni del diritto d'autore e del copyright, da loro considerato come il vero freno all'ingegno umano.

Per cercare di capire fino in fondo che tipo di obiettivi siano all'origine del fenomeno, occorre considerare che il primo nucleo di progettisti di ARPANET (la principale fonte di quella che in seguito è diventata Internet) proveniva principalmente dal Massachussetts Institute of Technology *(MIT)* di Cambridge e più in dettaglio da una società *spin-off* del MIT.
Questi ricercatori godevano di un'ampia autonomia finanziaria ed organizzativa e soprattutto non erano influenzati da imprenditori dediti solo al profitto, avevano quindi la possibilità di lavorare in un luogo sicuro e senza vincoli da parte dello

1. Bolt Beranek and Newman - società di consulenza informatica statunitense, ora denominata BBN Technologies si occupa di ricerca e sviluppo. La sede centrale è a Cambridge, Massachusetts (USA). E' nota per aver elaborato il packet switching (compresi ARPANET e Internet).

Stato o di privati, cosa che avrebbe potuto soffocare la loro creatività, tutelati da risorse pubbliche e ricerche *Mission-orienteted,* in un ambiente non soffocante per la libertà di pensiero e d'innovazione.

In sostanza ARPANET non deriva da un programma di ricerca privata, non nasce, come un prodotto commerciale da vendere a potenziali consumatori, ma si sviluppa nell'ambito del mondo accademico e militare.

Le fasi di sviluppo di Internet si possono sintetizzare come segue.

Nel 1960, all'interno della *RAND corporation*[2], Paul Baran inizia il primo lavoro di ricerca scientifica sulla commutazione di pacchetto. Per i suoi studi sulle rete di trasmissione dati, Baran si ispira alla rete più complessa in assoluto: il cervello umano. Dallo studio approfondito delle reti neurali ricava un modello che battezza col nome di "rete distribuita" (distributed network), basato sulla molteplicità di collegamenti. La duplicazione e la sovrabbondanza di connessioni del cervello umano permette di rimpiazzare facilmente una parte danneggiata con una nuova connessione realizzata dai neuroni rimasti intatti.

Un'altra idea rivoluzionaria di Baran è quella di frazionare i messaggi in diverse unità elementari di informazione, ciascuna in grado di seguire un percorso differente all'interno della rete.

In un suo memorandum, dal titolo "*On Distributed Communications Networks*" si legge che: " ... è tempo di cominciare a pensare ad una nuova e non ancora esistente rete pubblica, un impianto di comunicazione (…) progettato specificamente per la trasmissione di dati digitali tra un vasto insieme di utenti."

Le proposte di Baran incontrano lo scetticismo della comunità scientifica, che non ritiene il progetto tecnicamente realizzabile. Per cinque anni Paul Baran realizza dei dettagliatissimi memorandum scientifici, con i quali vengono confutate una ad una tutte le obiezioni e le critiche mosse al suo progetto.

Nel 1969 un *network* di computer messo in piedi dalla Advanced Rsearch

2. è un think tank statunitense. Il nome deriva dalla contrazione di "research and development". Fondata nel 1946 con il supporto finanziario del Dipartimento della Difesa statunitense, attualmente impiega più di 1500 ricercatori presso le sedi di Santa Monica, Washington e Pittsburgh. Dal 1992 è attiva in Europa attraverso la controllata RAND Europe.
Tra i suoi principali successi, la RAND Corporation annovera l'applicazione della teoria dei giochi per la decisione di differenti opzioni, metodologie per anticipare possibili sviluppi futuri attraverso scenari e DELPHI e la definizione teorica della commutazione di pacchetto.

Projects Agency (ARPA) da origine ad Internet. L'ARPA viene creata dal dipartimento della difesa degli Stati uniti allo scopo di mobilitare risorse di ricerca, in particolare del mondo universitario, verso la costruzione di una superiorità tecnologica militare sull'Unione Sovietica subito dopo il lancio del primo Sputnik nel 1957.

ARPANET è soltanto un programma minore uscito da uno dei dipartimenti dell'ARPA, l'Information Processing Techniques Office (IPTO), insediato nel 1962 sulla base di un'unità preesistente.

Lo scopo di questo dipartimento, così come definito dal suo primo direttore, *Joseph Licklider*[3], uno psicologo trasformatosi in scienziato informatico al MIT, è quello di stimolare la ricerca sull'utilizzo interattivo del computer.

Nasce così l'idea di un *network* interattivo informatico, che costituisca un sistema di comunicazione militare invulnerabile all'attacco nucleare. Nella realizzazione di tale *network,* l'IPTO, su proposta della stessa RAND Corporation al dipartimento della difesa, si basa proprio sulla rivoluzionaria tecnologia di trasmissione delle telecomunicazioni, sviluppata da Paul Baran: la "commutazione a pacchetto".

Successivamente per rendere possibile la connessione di ARPANET con gli altri *computer network*, a cominciare da quelli gestiti da ARPA, come PRNET e SATNET, viene introdotto il concetto di: "*network* di *network*".

Nel 1973, due scienziati informatici, Robert Kahn, di ARPA, e Vincent Cerf, della Stanford University, delineano l'architettura fondamentale di Internet.

Nel 1978 Cerf, Postel e Crocker, tre scienziati della University of Southern California, hanno l'idea di aggiungere al protocollo di comunicazione TCP (Transfert Control Protocol) il protocollo IP (l'Internet Protocol) mettendo a punto il protocollo TCP/IP, ancora oggi lo standard con cui opera Internet.

Nel 1984, la National Science Foundation (NSF) mette a punto una propria rete di comunicazioni via computer (NSFNET) e, nel 1988 comincia a utilizzare ARPA-INTERNET, come sua dorsale.

Nello stesso periodo, dalla filosofia nata attorno al sistema operativo *UNIX*[4]

3. Joseph Carl Robnett Licklider (March 11, 1915 – June 26, 1990),conosciuto semplicemente come J.C.R. or "Lick" era uno scienziato informatico americano, considerato una delle più importanti figure nella scienza e nella storia dei computer.

4. è un sistema operativo portabile per computer inizialmente sviluppato da un gruppo di ricerca dei

scaturisce: l' "*open source moviment*": un tentativo di tenere aperto l'accesso a tutte a tutte le informazioni relative ai software.

Nel 1984, Richard Stallman, un programmatore della MIT, fonda la Free Software Foundation (FSF), proponendo di sostituire il "copyright" con il "copyleft".

Mettendo in pratica i principi dell'FSF, nel 1991 Linus Torvalds, studente ventiduenne dell'università di Helsinki, sviluppa un nuovo sistema operativo basato su UNIX, chiamato Linux e lo distribuisce gratuitamente su Internet, chiedendo agli altri di migliorarlo e pubblicare a loro volta sulla rete le modifiche introdotti. Sulla scia di queste nuove filosofie, nascono in questo periodo gruppi dediti allo sviluppo del software cooperativo basato sull'*open source.*

Nel 1990 IBM, MCI e *Merit Network*[5] crearono un'organizzazione senza fini di lucro chiamata *Advanced Network and Services* (ans) che ha la missione di gestire e commercializzare i servizi della NSFNET oltre che di potenziare, assieme a Merit Network, la dorsale già esistente. Nel gennaio 1991 entra in gioco un altro contendente, *Sprint*[6], a cui viene affidato il compito di sviluppare le connessioni con le reti della ricerca in Europa, e successivamente con l'Asia, attraverso la *International Connections Manager*.

Già nel 1992 gran parte delle istituzioni accademiche e di ricerca americane sono collegate a NSFNET e la comunicazione con le reti governative veniva garantita dalla presenza di speciali nodi di scambio *(Federal Internet Exchange)* sulle due coste: fix-East e fix-West. La connessione con l'Europa e con l'Asia era invece garantita da Sprint (http://www.sprint.com).

Così, entro la metà degli anni novanta, Internet è privatizzata, consentendo alla sua architettura aperta l'arricchimento di tutte le reti di computer collegati in ogni parte del mondo. Il *World Wide Web* (cui spesso ci si riferisce

laboratori AT&T e Bell Labs, fra i quali c'erano inizialmente anche Ken Thompson e Dennis Ritchie.

5. la Merit Network Inc.è una organizzazione no profit, di proprietà degli stessi membri, situata a Ann Arbor, Michigan, che offre servizi di rete e corsi di alta qualità a diverse organizzazioni tra cui K-12, governo ed altre organizzazioni no profit.
Nella sua storia Merit ha sperimentato nuove tecnologie di rete e, dal 1987 fino all'aprile 1995, è riuscita a rielaborare la spina dorsale della National Science Foundation Network (NSFNET) in collaborazione con la National Science Foundation, ANS, IBM, MCI e lo stato del Michigan.

6. la Merit Network Inc.è una organizzazione no profit, di proprietà degli stessi membri, situata a Ann Arbor, Michigan, che offre servizi di rete e corsi di alta qualità a diverse organizzazioni tra cui K-12, governo ed altre organizzazioni no profit.
Nella sua storia Merit ha sperimentato nuove tecnologie di rete e, dal 1987 fino all'aprile 1995, è riuscita a rielaborare la spina dorsale della National Science Foundation Network (NSFNET) in collaborazione con la National Science Foundation, ANS, IBM, MCI e lo stato del Michigan.

semplicemente con *Web* o con l'acronimo *WWW*) è stata cronologicamente l'ultima funzionalità di Internet a essere sviluppata.

Il successo della "ragnatela mondiale" è stato tale che attualmente, per la maggior parte degli utenti (e dei mass-media), essa coincide con la rete stessa. Sebbene questa convinzione non sia tecnicamente corretta, è sicuro che gran parte del 'fenomeno Internet' sia dovuto proprio alla diffusione del Web.

L'impulso decisivo alla sua diffusione, infatti, viene proprio agli inizi del 1993, quando Marc Andressen ed Eric Bina, ricercatori presso il *National Center for Supercomputing Applications* (NCSA) dell'Università dell'Illinois, realizzano la prima interfaccia grafica multi-piattaforma per l'accesso ai documenti pubblicati su World Wide Web (BROWSER): Mosaic.

La semplicità di uso di Mosaic e le caratteristiche innovative dell'architettura informativa del Web, nel giro di pochissimi mesi, conquistano tutti gli utenti della rete, dando inizio a un processo di espansione tecnologica senza pari nel passato. Attualmente il numero di documenti presenti sul Web è stimato nell'ordine dei miliardi, e in centinaia di milioni sono gli utenti che quotidianamente ne fanno uso.

Parlando di World Wide Web, ci troviamo nella situazione di Achille nel ben noto paradosso di Zenone: nuovi servizi e nuove fonti di informazioni nascono in continuazione e qualsiasi enumerazione sarebbe incompleta non appena terminata.

1.2 Gli studenti del MIT, i primi Hacker

Intrinsecamente legata allo sviluppo della rete è la storia degli hackers, che ha inizio nell'inverno del 1958 proprio presso il *MIT* di Cambridge, il quartiere universitario di Boston, in un club studentesco di modellismo ferroviario: il Tech Model Railroad Club, all'interno del quale era sorto il comitato "*Signal & Power" (S&P)* che si occupava del funzionamento del circuito elettrico del modellino.

Si trattava di studenti brillanti ed intelligenti che iniziarono in questo modo ad occuparsi di informatica. Il termine ***hacker,*** inizialmente*,* indicava semplicemente gli scherzi organizzati dagli studenti (come ad esempio il rivestire d'alluminio la

cupola che dominava l'università). Successivamente, per merito degli stessi membri del club, il termine venne esteso al settore dell'informatica per passare a indicare un programmatore abile e preparato; infine, nel gergo mediatico, è spesso erroneamente interpretato come sinonimo di criminale informatico o cracker.

Nel 1959 al MIT fu istituito il primo corso di informatica, rivolto allo studio dei linguaggi di programmazione, al quale alcuni membri del *S&P* si iscrissero e dopo essere rimasti affascinati dagli elaboratori, i primi computer consegnati all'Istituto dalla *Digital* a seguito della loro dismissione da parte dell'esercito americano, perché fossero utilizzati per fini di ricerca e sperimentazione. Si trattava dell' IBM 704.

Nonostante l'accesso a tali apparecchiature (del valore di diverse migliaia di dollari) fosse all'epoca permesso solo a professori e ricercatori, i membri del *S&P* riuscirono ad ottenere l'autorizzazione ad utilizzarli liberamente durante le ore di lezione. Questo grazie all'abilità dimostrata nell'uso dei linguaggi di programmazione, nella fattispecie LIPS.

Le eccezionali doti degli hacker del MIT ebbero presto il sopravvento sui piani di studio, dimostrando, peraltro, quanto vario potesse essere anche a quell'epoca l'uso di un elaboratore.

L'obiettivo principale dei ragazzi del MIT era quello di realizzare programmi migliori utilizzando il minor numero di istruzioni possibile, in considerazione della scarsità delle risorse di sistema e dell'altissimo costo delle espansioni.

Come specificato nel paragrafo precedente, si ricorda che la logica secondo cui questo gruppo lavorava non era però legata, come oggi solitamente avviene a ragioni di profitto, bensì al puro interesse scientifico e alla sete di conoscenza.

Un altro fattore che ha reso possibile un rapido sviluppo è che all'epoca (negli anni '50), non era stata ancora formalizzata alcuna tutela del diritto d'autore per il software. I programmi realizzati dagli hacker e dai loro professori erano, quindi, a disposizione di chiunque volesse studiarli e migliorarli.

In questo modo, ciascun programmatore, anziché sprecare tempo prezioso poteva concentrarsi sui miglioramenti da apportare. Ogni programma costituiva una sfida ad ottenere risultati migliori. L'obiettivo dell'ottimizzazione e il pieno

sfruttamento delle risorse disponibili, nonché gli eccezionali risultati ottenuti, convinsero i protagonisti di quella prima rivoluzione informatica che il libero accesso alle informazioni, la disponibilità della tecnologia, l'uso dei computer, potessero davvero consentire di migliorare la società.
Si stava così costruendo, in maniera del tutto spontanea, un corpo organico di concetti, convinzioni e costumi che ha portato allo sviluppo dell'etica Hacker, tutt'ora priva di un vero e proprio manifesto.

Negli anni '60 e '70 l'attenzione degli hacker si spostò sull'hardware. Era il periodo degli *homebrewer,* soggetti dediti allo studio delle apparecchiature che compongono gli elaboratori, allo scopo di rendere accessibili non solo le informazioni ma anche la tecnologia. Questa è quindi una fase di sperimentazione sulle componenti dei sistemi informatici.
Spingere un elaboratore alle sue massime potenzialità, assemblare schede e processori allo scopo di trarne il miglior risultato possibile, costituì il secondo passo nella storia dell'hacking, mentre la competizione a realizzare il miglior software aveva animato il primo glorioso periodo del MIT.

Un decennio dopo Steve Jobs e Steve Wozniak, due famosi hackers membri dell'*Homebrew Computer Club*[7], in un garage, diedero vita al primo *personal computer* della storia, che rese famosa in tutto il mondo la *Apple (Appl*e computer incorporated), da loro stessi fondata proprio allo scopo di rendere la tecnologia del pc disponibile per tutti.
Gli anni ottanta saranno ricordati come *l'età dell'oro dell'hacking*.
Gli eccezionali programmatori formatisi nei periodi precedenti e i linguaggi di programmazione sviluppati nel corso degli anni, consentirono la realizzazione di software di altissimo livello, anche grazie alla tecnologia che, evolvendosi, ha dato vita al personal computer in grado di gestire i colori e l'audio. E' in questo periodo che negli Stati Uniti e in Europa nacquero i primi contrasti per la tutela dei diritti d'autore legati alla produzione di programmi per elaboratori.

7. la prima riunione del leggendario Homebrew Computer Club si svolse nel marzo del 1975 nel garage di uno dei membri a Menlo Park, contea di San Mateo (Silicon Valley). I membri del club Homebrew erano degli appassionati di elettronica, sebbene molti fossero ingegneri elettronici o avessero comunque un'esperienza come programmatori.

L'informatica e la telematica hanno così conquistato il diritto di essere riconosciute come discipline autonome e sono state ufficialmente inserite nei piani di studio delle scuole. La tecnologia a basso costo ha favorito la diffusione dei computer nelle famiglie e quindi la formazione di una cultura informatica, soprattutto tra i giovani. I personal computer collegati in rete hanno sostituito, anche nelle aziende di medie e grandi dimensioni, i vecchi sistemi di elaborazione basati su server centrale e terminali dislocati negli uffici, favorendo la produttività individuale.

Le reti telematiche sono divenute realtà ed internet ne rappresenta la massima espressione. L'hacking è una cultura che conta migliaia di adepti in tutto il mondo.

Fu, dunque, dagli anni ottanta in poi che i mass-media scoprirono il fenomeno sociale dell'hacking, una realtà purtroppo spesso associata al problema della criminalità informatica e, in particolare, alla figura del "malicious hacker" o "dark side hacker", soggetto dedito all'assalto dei sistemi informatici e telematici allo scopo di arrecare danni o di trarne un vantaggio economico.

In effetti, azioni di questo tipo si sono realmente verificate e continuano tutt'ora a esistere e ad essere un problema da regolare, ma rappresentano veri e propri casi di criminalità informatica che con l'hacking vero e proprio non hanno nessun legame.

1.1 L'Hacking in Italia

Il fenomeno hacker in Europa, ma soprattutto in Italia, ha uno sviluppo completamente diverso rispetto da quello che ha avuto negli USA.

Basti pensare che la tecnologia e la cultura *hacker* arrivano in Italia dagli USA a distanza di trent'anni e contrariamente a quanto è accaduto in altri paesi, per i quali l'approccio è stato chiaramente di ispirazione statunitense, assume connotati del tutto atipici e assolutamente propri.

Nel nostro Paese il fenomeno nacque (per poi ricollegarsi, dopo aver raggiunto una sua maturità, al corrispondente fenomeno americano) per il medesimo bisogno di conoscenza, per la stessa curiosità che aveva ispirato i giovani

hacker del MIT.

Favorito dal lancio dei primi computer a basso costo, prodotti dalla *Commodore*[8] *e dalla Sinclair*[9]*,* l'hacking si sviluppò in Italia vent'anni dopo l'esperienza americana, coinvolgendo centinaia di giovani che, quasi naturalmente e molto velocemente, divennero esperti d'informatica.

Questa nuova tendenza si scontrò quasi subito con delle norme decisamente datate, inadeguate alle esigenze dello sviluppo tecnologico, alle quali fecero seguito interventi legislativi che, nell'intento di portare la normativa al passo con i tempi, finirono per sanzionare condotte della cui rilevanza penale si ha ragione di dubitare. Il mondo dell'hacking italiano, come avvenuto già in passato per gli hacker statunitensi, si scontrò per la prima volta con le forze dell'ordine e la magistratura.

Gli alti costi delle connessioni telefoniche, infatti, spinsero gli hacker italiani, soprannominati *"smanettoni*", a procurarsi l'accesso ai sistemi chiamati *outdial*[10] o alla rete *Itapac*[11]*,* in entrambi i casi con l'addebito dei costi, rispettivamente, a carico delle aziende proprietarie o della Sip (oggi Telecom*).*

Oltre a questa pratica, che certamente non favorì l'instaurazione di buoni rapporti tra la comunità informatica italiana e le forze dell'ordine, la crescente diffusione delle *BBS*[12] preoccupò i servizi segreti, che iniziano ad interessarsi alle comunità telematiche temendo l'utilizzo a scopo eversivo, o comunque criminale, dei nuovi strumenti di comunicazione.

Gli smanettoni erano costretti ad operare da soli, scambiandosi informazioni per vie più o meno ufficiali. Questo li portò ad aumentare più lentamente le proprie conoscenze, dato che la diffusione era forzatamente clandestina, in un contesto

8. Commodore International Ltd., comunemente nota come Commodore, è stata una società multinazionale di informatica con quartier generale a West Chester in Pennsylvania (Stati Uniti) e sede legale nelle Bahamas. La società, all'epoca celebre in tutto il mondo per i suoi computer, commercializzava i propri prodotti con il brand "Commodore". Celebre anche il suo logo: la lettera "C" affiancata da una bandierina.

9. Il Sinclair ZX Spectrum, prodotto a partire dal 1982 dall'inglese Sinclair Research Ltd di Clive Sinclair, è un microcomputer originariamente dotato di microprocessore Z80 a 8-bit, linguaggio BASIC di 16 kB in ROM, 16 kB di RAM espandibili a 48 kB e una caratteristica tastiera in lattice con 40 tasti multifunzione.

10. un internet outdial è un modem che può essere connesso a Internet e poi usato per comporre un numero telefonico. Gli outdial normali chiamano solo i numeri locali, ma un outdial globale, GOD, è capace di chiamare sulle lunghe distanze.

11. ITAPAC è una rete a commutazione di pacchetto, basata su protocollo X25, nata nel 1986 per iniziativa della SIP e della ASST. Molto utilizzata all'inizio degli anni '90, oggi è pressoché sparita anche se continua ad essere utilizzata da alcuni bancomat e POS, oltre a qualche vecchio mainframe.

12. acronimo per Bullettin Board System: sistema a bacheca per informazioni. Indica uno o più computer collegati tramite modem ad una banca dati.

diverso sarebbe potuta esser meno faticosa e approssimata. Ignorati dalle università i giovani hacker italiani andavano sviluppando caratteristiche simili ai colleghi statunitensi, ma diverse da quelle dei primi Hacker del MIT, vale a dire l'intolleranza e la poca fiducia verso il mondo accademico-istituzionale.

Alla luce di quanto detto è giusto identificare i nostri primi pionier dell'informatica come seguaci dell'etica hacker, oppure è meglio chiamarli in maniera differente?

Anche se il fenomeno italiano nasce, come quello americano, con le stessa finalità di conoscenza e curiosità, le divergenze tra i due mondi sono abissali.

Sia come livello di preparazione sia come modo di operare il divario tra hacker italiani e americani inizia a ridursi solo negli ultimi anni.

In Italia nel 1986 vi erano tre BBS, legati a queste sorsero i primi club di hacker, il più famoso dei quali era il DTE di Milano. Nello stesso anno nacque il *videotel*[13] intorno al quale nacquero le prime "comunità virtuali" così, nonostante la quasi totale mancanza di contatti con i colleghi statunitensi, gli smanettoni iniziarono ad identificarsi in una serie di concetti che ricalcavano le stesse richieste che il movimento americano aveva effettuato negli anni '70: la libertà d'informazione, la lotta alle corporazioni e la volontà di esplorare, che nascevano dal comune denominatore del cyberspazio.

Nel giro di pochi anni fiorirono scuole private di programmazione e di informatica. Le istituzioni non erano in grado di far fronte alle esigenze degli "smanettoni", ma a partire dagli anni '80 nacquero le prime scuole private di programmatore *BASIC*[14] e vennero istituiti corsi di diploma di ragioniere e di perito programmatore e di perito informatico; tuttavia mancavano ancora attrezzature ed adeguate risorse umane competenti.

13. il Videotel è stato il videotex della SIP - Società Italiana per l'Esercizio delle Telecomunicazioni, l'ex monopolista telefonico italiano oggi confluito in Telecom Italia.

14. in informatica il BASIC (acronimo dell'inglese "Beginner's All purpose Symbolic Instruction Code", in italiano "codice di istruzioni simboliche di uso generale per principianti") è un linguaggio di programmazione ad alto livello sviluppato a partire dal 1963 nell'Università di Dartmouth (Dartmouth College) per il calcolatore GE-225.

Il profilo dell'Hacker

2.1 Diverse definizioni

Secondo Steven Levy (giornalista americano specializzato in tecnologia e computer), l'hacker pratica "*l'esplorazione intellettuale a ruota libera delle più alte e profonde potenzialità dei sistemi di computer, o la decisione di rendere l'accesso alle informazioni quanto più libera e aperta possibile. Ciò implica la sentita convinzione che nei computer si possa ritrovare la bellezza, che la forma estetica di un programma perfetto possa liberare mente e spirito*".

È evidente che la traduzione italiana di "pirata informatico" non solo sia peggiorativa, ma porti alla distorsione del significato originale. Ne deriva l'identificazione degli hacker come persone curiose ed appassionate al mondo dell'informatica, che mettono a disposizione le loro conoscenze per creare programmi gratuiti utilizzabili da chiunque, spesso fondamentali nel mondo delle telecomunicazioni.

Qui sopra è riportata una delle tante descrizioni di Hacker oggi a disposizione. Come si è detto precedentemente quello dell'informatica è un campo molto recente, in continua evoluzione, di conseguenza è molto difficile delineare in maniera univoca le figure che lo popolano, in primis quella dell'Hacker.

La letteratura sul computer crime presenta oltre 20 mila definizioni del termine hacker dimostrando che su tale figura esistono diversi atteggiamenti e connotazioni più o meno criminali.

Il *Webster Online Dictionary a*lla voce hacker riporta tra i vari significati: "*Esperto della programmazione e nella risoluzione di problemi con un computer"* e *"Persona che guadagna illegalmente l'accesso e qualche volta manomette le informazioni di un sistema informatico*".

Una nozione abbastanza fedele è disponibile nel *Jargon File*[15], reperibile on line all'indirizzo *http://www.catb.org/-esr/jargon.*

15. Il Jargon File è un documento originariamente redatto da Raphael Finkel della Stanford University e attualmente mantenuto da Eric S. Raymond, uno dei massimi esponenti della cultura hacker nel mondo. Esso è essenzialmente un vocabolario del gergo usato dagli hacker e dai professionisti dell'IT, ma contiene anche definizioni e regole di buona educazione da rispettare in rete (netiquette).

Tramite internet è possibile accedere a questo file ipertestuale, messo a disposizione di tutti gli utenti della rete, il documento è nato nel 1975 a Stanford e viene periodicamente aggiornato, per cui ne sono disponibili numerose versioni. *Raymond*[16] mantiene attualmente questo file.

La descrizione dell'Hacker nel file avviene per punti.

1) Una persona che ama esplorare i dettagli dei sistemi programmabili e i modi in cui estenderne le capacità, al contrario del resto della comunità che utilizza internet solo per lo stretto necessario.

2) Chi programma entusiasticamente, se non in maniera ossessiva, o che preferisce programmare al posto di disquisire sulla programmazione.

3) Una persona in grado di apprezzare l'abilità nell'attività di Hacking.

4) Una persona che impara a programmare presto e bene.

5) un esperto di un particolare programma , o chi per diversi motivi ci lavora quotidianamente, fino a conoscere detto programma fin nelle sue parti più remote.

6) Un appassionato o un esperto di qualunque materia.

7) Chi ama raccogliere la sfida intellettuale di superare le limitazioni con creatività.

Si tratta di una vera e propria élite, i cui componenti sono ben disposti ad accogliere nuovi membri meritevoli, garantendo così un continuo riciclo di persone e di idee. Gli unici requisiti per entrare a far parte della comunità sono l'abilità ed il riconoscimento di quest'ultima da parte degli altri membri: infatti si parla di una comunità basata unicamente sulla meritocrazia, in cui i titoli e le esperienze lavorative non hanno valore e ciò che fa la differenza è il lavoro concreto.

Secondo alcuni autorevoli autori: "la caratteristica che più appare emergere dalla complessa struttura psicologica degli hacker è il sentimento

16. Eric Steven Raymond (4 Dicembre 1957), spesso chiamato ESR, è un programmatore di computer, autore e esperto di open source. Il suo nome diventò famoso tra gli hacker quando iniziò la manutenzione del "Jargon File" nel 1990. Dopo la pubblicazione nel 1997 di "The Cathedral and the Bazaar", Raymond diventò, un interlocutore per il movimento open source.

d'onnipotenza che ad essi deriva dal rapporto instaurato col computer. Il controllo pressoché completo dell'hardware."

Le molteplici possibilità d'utilizzo del termine hacker sono state sintetizzate da diversi autori, anche all'interno della stessa categoria esistono distinzioni.

Ira Winkler[17] li suddivide in tre categorie: i geni, gli sviluppatori e gli altri. I *geni* sono individui particolarmente intelligenti e capaci di intervenire su natura e funzionamento dei sistemi informatici e telematici al punto di essere in grado di contribuire all'evoluzione della scienza e della tecnologia. Gli *sviluppatori* migliorano gli strumenti di lavoro esistenti o ne creano di nuovi.

Gli *altri* si limitano a sfruttare l'evoluzione tecnologica e scientifica che deriva dagli strumenti di lavoro per i fini più disparati.

Il problema è che chiunque abbia un buon bagaglio culturale nel campo dell'informatica e della telematica è in grado di utilizzare tali strumenti in modo sovversivo per trarne un ingiusto profitto o per arrecare danno. Ad ogni modo il termine hacker è utilizzato correttamente solo se indica le prime due categorie di individui: i geni e gli sviluppatori.

Un'altra distinzione è stata costruita da *Marco Strano*[18] che individua:

1. "Hacker tradizionale", che è colui il quale agisce spinto dal gusto per la sfida e per dimostrare a sé e agli altri la perizia acquisita in campo informatico.
2. "Hacker distruttivo vandalico", che sparge virus con l'intento di comunicare la sua rabbia contro il sistema.
3. "Hacker distruttivo professionista", che agisce spinto dalla logica lucrativa.
4. "Hacker spia", che opera veri e propri furti di informazioni su commissione.
5. "Hacker antagonista", che agisce spinto da motivazioni di lotta alla strumentalizzazione commerciale o alla politica delle informazioni.
6. "Hacker terrorista", che usa le tecniche dell'hacking con lo scopo di destabilizzazione sociale all'interno della comunicazione istituzionale.

17. presidente and figura attiva del CEO, Winkler è riconosciuto come una dei maggiori esperti di Internet Security, spionaggio industriale e informatica legata al crimine, nel mondo. E' uno specialista del *penetration testing*, dove si infiltra nelle reti delle compagnie, sia tecnicamente che fisicamente, per trovare e riparare le debolezze del sistema.

18. Marco Strano, Psicologo e Criminologo è considerato uno dei maggiori esperti del mondo di Psicologia investigativa e criminal profiling.

E' anche necessario precisare che nel Jargon file il termine hacker tende a connotare l'appartenenza ad una comunità globale; ciò implica che questi aderisce in qualche modo a principi condivisi da altri, un'etica appunto, anche se la caratteristica che contraddistingue in ogni caso il vero hacker è la curiosità unita ad un'intelligenza brillante, dinamica al di sopra della norma, capace di liberarsi da ogni condizionamento e prediligendo argomenti scientifici. Oltre alla curiosità, i principali elementi tra loro strettamente connessi, che da sempre hanno accomunato gli hacker sono: il principio dell'*hands-on*, la creatività, la ricerca della perfezione, la sfida nel superare i limiti, la ricerca del consenso meritocratico, un atteggiamento anti-autoritario e anti-burocratico e, soprattutto, la convinzione che la libera informazione sia il presupposto necessario per il progresso della società.

Del resto gli hacker ritengono che comprendere il funzionamento delle cose permetta di dominarle, di acquistare potere su di esse e trovare, in fondo, in questo potere, una soddisfazione assoluta. Solo intervenendo fisicamente sulle cose è possibile conoscerne la logica più intrinseca e verificarne le intuizioni che possono migliorarle.

Perennemente alla ricerca delle debolezze, dei limiti dell'oggetto di indagine, l'*hacker* sfida sé stesso tentando di superarli.

2.1.1. Luoghi comuni e disinformazione

Alla luce di quanto descritto, ci si domanda perché comunemente quando si parla degli hacker si pensa a persone senza scrupoli capaci d'infettare i nostri computer, e mettere a rischio il nostro diritto alla *privacy.*

La causa è da rilevare nel difficile rapporto tra filosofia hacker e mezzi di comunicazione di massa.

Nel maggio del 2000 i mass media hanno scatenato un nuovo allarme commentando la diffusione del virus *I love you*. La natura del virus, non fu così pericolosa come i media avevano sbandierato ai quattro venti, in quanto gli appositi antivirus fermarono il propagarsi dell'infezione sul nascere, ma la notizia rimbalzò all'interno di giornali e telegiornali, mettendo in moto una fobia

generale fra gli operatori inesperti facendo acquistare loro antivirus a costo esorbitanti. Alla diffusione della notizia, non ci fu un adeguato modo per tutelarsi, magari intervistando un esperto in materia, in grado di rassicurare gli operatori, e di spiegare loro come potevano tutelarsi dal *virus.*

In questa situazione, come in molte altre, gli *hacker* sono stati messi sotto accusa, e anche questa volta l'impulso di dare la notizia si è rivelata una forma di disinformazione.

Lo scambio di notizie gioca oggi un ruolo determinante in ogni settore della società. La televisione, la radio e i giornali sono i mezzi di comunicazione che l'uomo utilizza quotidianamente per tenersi informato su cosa accade nel mondo.

Occorre però chiedersi se gli attuali strumenti siano in grado di informare in maniera oggettiva e, soprattutto, se chi scrive ha conoscenza di ciò che è chiamato a descrivere.

L'eccesso di informazione, e la scarsa competenza in una materia così nuova e sempre piena di innovazioni si traduce in uno svantaggio per la collettività, che non solo rimane disinformata, ma spesso ha una distorta concezione di cosa effettivamente accade.

Questo problema riguarda pienamente la figura dell'*hacker*, descritto continuamente dai mezzi di comunicazione di massa come criminale "informatico". La criminalità informatica, al contrario è costituita, salvo rare eccezioni, molto più semplicemente, da frange tecnologicamente avanzate della criminalità organizzata e della delinquenza comune.

Gli *hacker* vengono citati a sproposito dai mass media in più di un'occasione ed equiparati ai *cracker* e *phreaker,* dai quali, invece, si differenziano in modo sostanziale.

I media tradizionali, hanno iniziato una paradossale gara alla criminalizzazione di Internet e degli *hacker*, riuscendo a terrorizzare l'utente medio della "rete". Secondo la "teoria del discorso" di *Foucault*[19] questo sarebbe un tipico caso in cui discorsi dei media hanno contribuito a costruire la realtà di un fenomeno,

19. Paul Michel Foucault (Poitiers, 15 ottobre 1926 – Parigi, 25 giugno 1984) è stato uno storico e filosofo francese. Filosofo, archeologo dei saperi, saggista letterario, professore al Collège de France, tra i grandi pensatori del XX secolo.

producendo, nel caso dell'hacking, le definizioni più diffuse del tecnocriminale.
Si può affermare, al riguardo, che l'esperienza e l'identità della comunità hacker sono state filtrate dai mezzi di comunicazione e dalle istituzioni creando una rappresentazione senz'altro fuorviante, tanto da etichettarli come gruppi socialmente devianti e pericolosi, poiché trascendono le norme e i valori legalmente e moralmente accettati.
Le forze dell'ordine (Polizia di Stato, Guardia di Finanza, e Arma dei Carabinieri) cercano continuamente di far fronte a questa disinformazione, un esempio è rappresentato dalla creazione di reparti *ad hoc* per perseguire i cc.dd. *cracker* ed assicurare alla giustizia i veri criminali "informatici".
Il termine *cracker*, non riconosciuto dai *mass media* tradizionali, indica il lato oscuro (*dark side*) dell'h*acker.* Il termine è nato per identificare colui che "cracka", cioè colui che riesce a sbloccare sistemi protetti o a copiare illegalmente software commerciali, violandone le chiavi di protezione e/o di registrazione.
Il Jargon file afferma che i cracker sono soggetti che distruggono la sicurezza di un sistema; di fatto essi sono "pirati informatici", cioè "criminali informatici".
Ciò che accomuna gli *hacker* e i *cracker* sono solo le abilità e le conoscenze informatiche, ciò che li differenzia è il modo di usare tali qualità: mentre i primi cercano di contribuire al progresso della comunità scientifica, mediante lo studio ed il dibattito, senza sfociare mai in crimini o in danneggiamenti, i secondi, al contrario, hanno finalità esclusivamente illegali.

Gli *hacker* veri e propri, dunque, non agiscono con l'intenzione di compiere reati informatici, né normalmente li compiono; vanno perciò distinti dai *cracker*, ossia coloro che agiscono allo scopo di violare sistemi informatici, per acquisire informazioni riservate o per puro vandalismo.
Essi sono pertanto ben lontani dalla c.d. *etica hacker*, i cui caratteri fondamentali risiedono in primo luogo nella convinzione che la condivisione della conoscenza sia una bene essenziale e che la condivisione della propria esperienza, programmando codici liberamente modificabili e facilitando l'accesso alle relative informazioni, costituisca un vero e proprio obbligo morale.

In secondo luogo, alcuni affermano la rispondenza a tale etica, dunque la liceità, del *system–cracking*, purché non vengano commessi furti, atti di vandalismo o di lesione della privacy.

Se il principio della condivisione delle esperienze e delle informazioni è generalmente accettato dagli *hacker*, altrettanto non può tuttavia dirsi del secondo, ritenuto totalmente illecito da alcuni. Ne consegue che la generalizzata criminalizzazione di questi, esprime una mancata conoscenza del fenomeno perché essi sono ben distinti dai cracker.

Altro punto focale che distingue le due figure sta nella "firma", mentre i primi spesso rivendicano le loro azioni; i secondi cercano di eliminare le tracce del proprio passaggio o della propria presenza all'amministratore di sistema.

Nel mondo dell'informatica sfortunatamente è assai difficile identificare il confine tra la legalità e l'illegalità, in quanto ben pochi sono a conoscenza delle norme poste a tutela dei sistemi informatici e telematici e del software. Uno dei punti fondamentali su cui l'etica hacker si basa è proprio la libertà di "utilizzo" del software.

Oltre agli *hacker* e ai *cracker*, altri soggetti capaci di alterare i sistemi informatici e telematici sono i p*hreaker*, anch'essi derivano dalla cultura *hacker*, ma il loro scopo è quello di sabotare ed utilizzare abusivamente i sistemi telefonici ed a tal fine ricercano e sperimentano continuamente nuove tecniche. I *phreaker* sono divenuti famosi negli anni '60, prima che internet diventasse uno dei principali mezzi di comunicazione, grazie al *blue box*[20]*,* che garantiva connessioni a costi irrisori. Anche in Italia si è sviluppato il fenomeno dei *phreaker*, utilizzando lo stesso sistema del *blue box,* fenomeno scemato nel 1992, quando Telecom su sollecitazione di altre compagnie telefoniche, ha adottato il nuovo protocollo CCIS per il monitoraggio delle linee, basato oggi su frequenze non trasportabili su linee telefoniche standard.

20. La blue box (in inglese scatola blu) è uno dei primi strumenti storicamente usati negli Stati Uniti e in altri Paesi per il phreaking; si tratta di un dispositivo elettronico che emette segnali sonori (toni) di frequenza pura o risultanti dalla sovrapposizione di due sottotoni di frequenza distinta.
Il nome dell'oggetto deriva dal colore del primo apparato di questo tipo confiscato dagli addetti alla sicurezza della società telefonica Bell.

I motivi che spingono alcuni programmatori a realizzare virus informatici o a sabotare programmi, sono, infatti, di varia natura, dal lucro alla semplice soddisfazione personale. Chi si prodiga nella creazione di questi programmi è detto "*virus writer*"; spesso sono semplici ragazzi che vogliono attirare solo attirare l'attenzione, mentre altre volte sono veri e propri programmatori professionisti assoldati da aziende produttrici di software antivirus.

2.1.2. Come gli Hacker vedono se stessi

Come si è visto molto spesso gli hacker vengono etichettati nei modi più bizzarri, spesso anche in forma dispregiativa, come fossero dei criminali, il cui profilo sarebbe assimilabile a quello di un individuo depresso, incapace di avere rapporti con il resto della società e con i propri coetanei e capace di atti criminali.

Al contrario per la propria comunità, un *hacker* si considera un soggetto appassionato di computer, che li conosce nei minimi particolari, sempre aggiornato, e soprattutto non si autodefinisce "hacker", perché sono gli altri a identificarlo.

Gli *hacker* ritengono ignoranti i mass media e la popolazione, nel senso che non sono in grado di riconoscere con esattezza cosa sia l'*hacking* e cosa significhi per loro. Sono anche ben consci del fatto che per colpa di pubbliche amministrazioni e media, la maggior parte della gente abbia un'idea sbagliata del loro "ruolo", vedendoli come figure negative e fuorilegge.

Essi si sentono ingiustamente odiati e non si ritengono in alcun modo una minaccia per l'economia e per il benessere del paese, bensì una risorsa, poiché consci di essere molto abili e preparati nella loro materia.

Gli *hacker* si definiscono difensori di basilari diritti umani, e considerano criminali coloro che vogliono censurare l'informazione bloccando la libera ricerca del sapere e della conoscenza.

A questo proposito si riporta di seguito un passaggio del manifesto hacker "The coscience of a hacker":

"Noi esploriamo…e voi ci chiamate criminali.
Noi cerchiamo la coscienza…e voi ci chiamate criminali.
Noi esistiamo senza colore della pelle, senza nazionalità,
senza pregiudizi religiosi…
e voi ci chiamate criminali.
Ma soprattutto, noi cerchiamo conoscenza…
Ed è per questo che ci chiamate criminali…
Guardatevi, avete paura di noi. Mobilitate risorse enormi
per prenderci.
Voi costruite bombe atomiche, voi fate la guerra, voi
uccidete, imbrogliate e ci mentire e tentate di farci credere
che è per il nostro bene, eppure siamo noi criminali.
Si, sono un criminale. Il mio crimine è sapere quello che
voi non vorreste dire, desiderare di sapere tutto ciò che la
mia natura di essere umano mi dà il pieno e inalienabile
diritto di conoscere.
Il mio crimine è quello di giudicare la gente
in base a quello che pensa e dice,non per come appare.
Il mio crimine è di essere più furbo di voi,
una cosa che non potrete mai perdonarmi. […]"

2.4 Modus operandi

In che cosa consiste esattamente l'attività di Hacking.

Entrando nel vivo nelle tecniche d'attacco hacker, possiamo anticipare che non esiste un'unica modalità d'azione, ma ogni qual volta un'operazione si conclude con successo c'è sempre la firma di chi ha operato, come rivendicazione di ciò che è stato compiuto.

Il *War dialling*[21] è una tecnica molto usata come prima fase di un attacco comune tra gli hacker di un certo livello tecnico, questa consiste in un processo

21. War dialing o wardialing è un tecnica che usa il modem per fare scansioni automatiche di elenchi telefonici componendo ogni numero nel codice di un'area localizzata, per cercare computer, Bulletin board systems e fax. I cracker in genere cercano password si accesso.

con il quale il computer viene istruito attraverso degli script ad effettuare telefonate seguendo una lista di numeri prefissati, fino a quando non rispondono un modem o un altro computer. In questo caso il programma provvede al *routing* delle telefonate, garantendo la supervisione di queste ultime, l'identità del cliente ed i loro numeri di telefono, in questo modo si consente all'hacker di effettuare telefonate sia nazionali che internazionali.

Altro metodo d'attacco è il: *Ping-of-Death Attack*[22] effettutato contro i Web Server. Il termine PING (*Packet Internet Groper*) si riferisce ad un metodo che consente di determinare se un *host* è presente su di un network e se opera periodicamente.

Per effettuare un *ping* viene impiegato un protocollo chiamato: *Internet Control Messagge Protocol* (ICMP), in grado di effettuare scansioni per testare una connessione o per localizzare gli accessi ai network.

I network, infatti, utilizzano i messaggi ICMP per individuare e localizzare problemi tecnici (come ad esempio un router che non riesce a trasmettere pacchetti di dati alla stessa velocità con cui li riceve).

Inviando ad un server una quantità innumerevole di pacchetti in un breve lasso di tempo, può accadere che il server non sia più in grado di rispondere a tutte le richieste, "andando in *crash"* ed impedendo agli utenti di accedere alle sue informazioni.

Con alcuni strumenti gli *hacker* sono in grado di mappare interi *network* di *computer* (perfino Internet), effettuando scansioni verso le porte dei *network*, alla ricerca di vulnerabilità e, una volta trovate, pianificano attacchi mirati.

Come spiegato nel capitolo precedente, un elemento fondamentale che divide gli *hacker* dai *cracker* e da chi commette reati informatici è, oltre alle finalità, la firma cioè la propria "orma", ovviamente anonima, c.d. handle, questa fa parte del modus operandi, e viene lasciata dopo aver concluso un'operazione. Per fare un esempio, quando un hacker o un gruppo fa un *web defacement*, lascia la propria firma inserendo il *nickname* nella home page attaccata, così nel sito apparirà il nome di chi ha *bucato* il web. Molto spesso, oltre al nome

22. ping of death (abbreviato POD) è un tipo di attacco su un computer, che comprende l'invio di ping deformati o contenenti virus. Un ping di solito è 56 byte (or 84 byte se si considera l'IP); storicamente molti sistemi informatici non potevano trattenere un pacchetto di ping maggiore di 65,535 byte. Inviare un ping di questa taglia poteva mandare in tilt il computer.

dell'artefice è possibile trovare anche dei messaggi, spesso di tipo politico-sociale, che gli hacker lasciano per sensibilizzare l'opinione pubblica su notizie non trattate dai media.

Come operano gli Hacker, da soli o in gruppo

Gli *hacker* più abili agiscono da soli, a causa del rischio di essere scoperti quando si agisce in gruppo, credendo che all'interno del gruppo ci sia sempre un anello debole.

Sono costretti, quindi, a tenere segreta la loro attività online, rilevandola solo ad alcune persone fidate, senza entrare mai nello specifico. Ciò non toglie, comunque, che gli *hacker* solitari possano operare in gruppo in via del tutto sporadica, per particolari progetti o per stringere legami con altri esponenti del mondo underground, con cui parlare e per scambiare le proprie esperienze.

E' da sottolineare come nel corso degli anni il diritto sostanziale in materia di *computer crime* abbia determinato una sensibile modifica dell'etica hacker, costringendo il passaggio da una comunità aperta ed amichevole ad un circolo chiuso e ristretto.

Gli *hacker* oggi sono più isolati, più restii a condividere le informazioni in loro possesso e molto più attenti a dare confidenza a chi non conoscono. Persistono, tuttavia, alcune comunità *underground* frequentate da *hacker*. Chi agisce in gruppo sono di solito gli adolescenti, che si avvicinano all*'hacking* per ragioni tecniche informatiche o, più semplicemente, perché attirati dal fascino del mondo underground.

Sentirsi parte di una comunità è importante nella realizzazione della propria identità personale, in quanto si può imparare più velocemente e sentirsi più protetti con l'aiuto di esperti. Questi gruppi sono sorretti da regole precise, la cui violazione determina l'espulsione del trasgressore.

Regole principali sono: l'obbligo di condividere tutte le informazioni di cui si è venuto a conoscenza durante un'incursione informatica ed il divieto di divulgarle all'esterno del gruppo. Si può venire espulsi, comunque, anche qualora non si dia un contributo attivo alle attività del gruppo.

Nei gruppi più sofisticati i membri non si incontrano di persona e in pochi conoscono il vero nome, l'età e la località di origine degli altri membri. E'

possibile, inoltre, che i gruppi si uniscano per discutere o confermare dei teoremi, spesso mettendo in pratica ciò che si afferma, facendo si che un'ampia discussione sia un motore per lo sviluppo.

2.5 Obiettivi e motivazioni

I *target* principali degli attacchi informatici, in particolare per azioni di *hacking*, sono i sistemi o i siti di enti governativi, in particolare militari, e quelli delle grandi corporazioni, soprattutto finanziarie, aziende di telecomunicazioni, o aziende che limitano con il loro *copyright* la diffusione di nuovi sistemi operativi. E' evidente come la scelta degli obiettivi da colpire cambi con l'aumentare delle abilità tecniche del soggetto, a causa delle maggiori difficoltà che l'attacco comporta.

L'obiettivo degli attacchi ad un sito governativo o militare, oppure di importanti società multinazionali, è quello di attirare l'attenzione dei *mass media* sul loro operato e di veicolare un messaggio di tipo politico o sociale.

A tal fine, accanto all'intrusione nel sistema informatico o telematico, possono essere attuate operazioni di *web defacing*, per far capire all'azienda colpita di essere nel mirino e che c'è il rischio di essere attaccati di nuovo se non si modifica la propria politica.

I mass media come già spiegato, fraintendono generalmente l'obiettivo degli *hacker*, indicando l'intrusione e il *web defacing* come gli unici scopi e tralasciando completamente il messaggio sociale o politico.

Altri gruppi *hacker* hanno, invece, il fine di sensibilizzare l'opinione pubblica sul problema della sicurezza informatica e sugli abusi che le grandi aziende perpetuano nei confronti degli utenti, monitorandoli e limitandole nell'esercizio delle proprie libertà.

2.6 Ambiguità nel rapporto con amministrazioni e istituzioni

Tra gli hacker e gli amministratori di un sistema informatico e telematico si crea spesso un rapporto di competizione, ma al contempo di collaborazione.

Una volta scoperte nuove vulnerabilità in un sistema, l'*hacker* può scegliere di tenere l'informazione per se, o per il gruppo d'appartenenza, ma anche di informare l'amministratore.

Ci sono poi strade di compromesso, come aspettare che l'amministratore abbia riparato i "buchi" nel sistema prima di divulgare la notizia.

I veri *hacker* di solito optano per quest'ultima possibilità, per evitare attacchi al sistema danneggiato e permettere all'amministratore di individuare gli errori e correggere i difetti.

La posta elettronica è il mezzo di contatto preferito dagli *hacker,* che via e-mail indicano agli amministratori quali sono i *bug* individuati ed i metodi utilizzati per compromettere il sistema.

Vi sono però alcuni che scrivono dei veri e propri rapporti per gli altri membri dell'underground, in cui elencano le vulnerabilità con le loro note. L'intento è quello di sottolineare come sarebbe facile per gli amministratori rimuovere i difetti rilevati e mantenere il sistema sicuro, perciò se un sistema viene attaccato la colpa non può che essere dell'amministratore negligente.

Secondo alcuni *hacker,* tuttavia, questa "funzione di servizio pubblico" non sarebbe assolutamente apprezzabile, ritenendo che ci siano modi più appropriati per migliorare la sicurezza della rete, come ad esempio il sistema di criptografia, sistemi di firewall e maggior sicurezza nelle comunicazioni.

Per quanto attiene, invece, il rapporto tra *hacker* ed istituzioni, sia nazionali che internazionali, questo è spesso di sfida nei confronti dei soggetti incaricati della vigilanza e del controllo (forze dell'ordine, enti di vigilanza), considerati di scarsa capacità tecnica ed incapaci di comprendere il mondo dell'*hacking,* con l'unico fine di limitare le libertà personali e lo sviluppo tecnologico attraverso una gestione monopolistica del mercato (si pensi ad esempio alle compagnie telefoniche o televisive).

Per le comunità hacker, quindi, il rapporto sostanziale tra governo e cittadini deve essere non di tipo gerarchico e autoritario (così detto rapporto verticale), bensì paritario (rapporto di tipo orizzontale) ed è estremamente importante monitorare il lavoro delle istituzioni, divulgare informazioni sui loro affari e, se possibile, bloccarle con i mezzi e le capacità informatiche dell'*hacking*.

Uno dei principi fondamentali dell'etica *hacker* consiste proprio nel dubitare dell'autorità, promuovendo il decentramento.
Principio che sottintende ad una profonda sfiducia nei confronti delle istituzioni, degli amministratori ed anche delle multinazionali specializzate nel commercio di strumenti informatici, che favorirebbero l'imbrigliamento delle menti più fervide, con il conseguente blocco del progresso.

Le conseguenze di questo ambiguo atteggiamento sulle pubbliche istituzioni, ha portato all'elaborazione di misure di sicurezza e strumenti più o meno efficaci di difesa e "studio" dell'Hacker.

Etica Hacker: norme e valori

3.1 I princìpi

Come si evince dall'analisi della sua figura, l'hacker è per natura indisciplinato, tendenzialmente anarchico, restio ad adeguarsi a qualsiasi tipo di regola, in contrasto con ogni tipo di dogma e di dottrina prestabiliti e preconfezionati.
Per questo mal si adatta a qualsiasi struttura gerarchica e all'organizzazione del lavoro, che non consente di pensare ed agire liberamente.
Si già accennato che nella filosofia degli hacker, le misure di sicurezza poste a protezione dei sistemi informativi costituiscono solo un ostacolo da rimuovere rapidamente, un limite imposto. Mentre non è hacker colui che assalta i sistemi per finalità tipiche della criminalità comune ed organizzata, chi si introduce in un sistema per danneggiarlo o per provocarne il malfunzionamento con l'intenzione di trarne un ingiusto profitto: tale filosofia di comportamento è in netto contrasto con la filosofia dell'hacking.
Alla base del loro comportamento sta il principio secondo cui i sistemi informatici possono concretamente contribuire al miglioramento della società, grazie alla capacità di diffondere le informazioni in modo capillare e veloce.
Queste sono considerate patrimonio dell'umanità, al pari dell'aria, dell'acqua, delle risorse naturali e quindi, dove vengano frenate dai governi al solo fine di ottenere il controllo della collettività, non per migliorarne le condizioni di vita ma per esercitare su di essa il potere, devono essere recuperate e diffuse. I sistemi protetti da misure di sicurezza sono violati non per non perché vengano bloccati o danneggiati, ma affinché siano recuperate e diffuse le informazioni riservate in essi contenute.
Dice Raymond (tra i redattori dello Jergon File): "Chiunque possa darti degli ordini, può fermati dal risolvere problemi dai quali sei affascinato ... Gli autoritari prosperano sulla censura e sulla segretezza. Essi distruggono la cooperazione volontaria e lo scambio di informazioni. L'unica 'cooperazione' che piace è quella di cui hanno il controllo".

S. Levy[23]: "L'ultima cosa di cui c'è bisogno è la burocrazia. Questa, che sia industriale, governativa o universitaria, è un sistema imperfetto ed è pericolosa perché inconciliabile con lo spirito di ricerca dei veri hacker. I burocrati si nascondono dietro regole arbitrarie: si appellano a quelle norme per rafforzare il proprio potere e percepiscono l'impulso costruttivo degli hacker come una "minaccia".

L'etica degli hacker è il collante di questa controcultura: si tratta, di un sistema di valori profondi non scritta o codificata, mai oggetto di dibattito, implicitamente accettata: una specie di manifesto programmatico di tutti gli hacker caratterizzato dallo spirito libertario e tipicamente contro-culturale degli anni '60.

Ovviamente ogni comunità culturale è mediata e modulata dal contesto storico-sociale, è per questo che l'etica Hacker dei primi anni si differenzia su alcuni punti da quella attuale, che deve fare i conti con nuove problematiche.

Tale ideologia parla di un'audace simbiosi fra uomo e macchina di cui gli hacker sono divulgatori, con il fine di alfabetizzare le masse alla nuova tecnologia informatica.

Per gli hacker del MIT la pratica dell'hacking era incentrata su sei principi fondamentali:

1) L'accesso ai computer deve essere illimitato e completo. L'imperativo è *hands on* (metterci su le mani): gli hacker, infatti, credono nella possibilità di imparare smontando le cose, osservando come funzionano e usando questa conoscenza per creare cose nuove.

2) Tutta l'informazione deve essere libera*.* Ogni controllo proprietario su di essa è negativo. Dovere etico degli hacker è la condivisione del proprio sapere e della propria esperienza con la comunità d'appartenenza, separata dal resto della società. Nell'underground tutto circola liberamente e rapidamente sia che si tratti di materiale coperto da copyright o meno: secondo questa ideologia il copyright è, infatti, un concetto ormai superato nella futura società dell'informazione. L'arte dell'*hackeraggio* per esplorazione e divertimento è

23. Steven Levy (nato nel 1951) è un giornalista americano che ha scritto diversi libri su computer, tecnologia, crittografia, sicurezza informatica e privacy.

eticamente corretta fino al momento in cui non siano commessi intenzionalmente furti, atti di vandalismo, distruzione di privacy, danno ai sistemi informatici: è contro l'etica alterare i dati che non siano quelli necessari per eliminare le proprie tracce, evitando così d'essere identificati.

3) Dubitare dell'autorità. Promuovere il decentramento. La burocrazia è politicamente inconciliabile con lo spirito di ricerca costruttiva e innovativa degli hacker, il quale incoraggia l'esplorazione e sollecita il libero flusso delle informazioni. L'utopia degli hacker, come sintetizza Levy, è portare i "computer alle masse, i computer come giradischi, livellando le ineguaglianze di classe, la tecnologia non più come strumento di potere nelle mani delle classi egemoni".

4) Gli hacker dovranno essere giudicati per il loro operato e non sulla base di falsi criteri quali ceto, età, etnia e posizione sociale. La comunità hacker ha un atteggiamento meritocratico: non si cura dell'apparenza mentre è attenta al potenziale dell'individuo nel far progredire lo stato generale dell'hackeraggio e nel creare programmi innovativi degni d'ammirazione. La stratificazione di status si basa quindi sulla conoscenza, l'abilità e l'estro digitale.

5) Con un computer si può fare arte. Emerge una certa estetica dello stile di programmazione. Nei computer si può ritrovare la bellezza e la fine estetica di un programma perfetto che, spinto al massimo delle sue potenzialità, può liberare la mente e lo spirito: ogni programma dovrebbe essere ammirevole e progettato per espandere le possibilità dell'utenza. Il computer è l'estensione illimitata della propria immaginazione personale.

6) I computer possono cambiare la vita in meglio. Gli hacker hanno profonda fede nel computer come strumento di liberazione e di trasformazione della realtà. La controcultura hacker è un movimento che per diffondere i propri principi si avvale della tradizionale stampa cartacea underground.

Esistono numerosi giornali e riviste specializzate o di "nicchia" di cui gli hacker sono produttori.

Sanno ovviamente sfruttare i più potenti mezzi di distribuzione elettronica che presentano maggiori vantaggi come l'istantaneità e, soprattutto, la circolazione delle informazioni in tempo reale.

Un altro elemento forte che accomuna gli hacker è il ***gergo*** che rappresenta un legame simbolico, l'integrazione tra valori e stili di vita del gruppo.
Gli hacker condividono un linguaggio comune che è il vero e proprio sedimento della cultura hacker Americano-Inglese: esso costituisce perciò il mezzo privilegiato di comunicazione istituzionale di tale controcultura sia al suo interno che verso l'esterno. Tale linguaggio, che è un sistema di segni deliberatamente opaco e allusivo, è determinante nella formazione dell'identità socio-culturale, una specie di marchio di unicità; è come una finestra sulla cultura hacker che ne riflette la costante evoluzione.

Il linguaggio informale tipico della cultura hacker è una potente arma di esclusione dalla comunità, ma anche di aggregazione qualora sia d'ausilio come collante ideologico. Questo gergo colorito è sorprendentemente ricco di implicazioni, variazioni e sfumature che partono dalla lingua inglese.

I princìpi indicati trovano applicazioni in diversi ambiti della vita degli Hacker

3.1.1 Etica del Lavoro

L'etica hacker può essere considerata sul campo "professionale" come un "rapporto entusiastico nei confronti del lavoro".
L'etica hacker del lavoro viene utilizzata in un'accezione che trascende il mondo dell'informatica, basandosi sul principio secondo cui l'attività degli hacker deve essere motivata non dal denaro ma dalla "passione" e dal desiderio di creare qualcosa che la "comunità dei pari" possa ritenere di valore.
La "passione" infatti è intesa da Raymond come un'attività interessante, stimolante e piacevole. Per essere hacker, l'alta tecnologia non è assolutamente necessaria, l'essere hacker ha a che fare con l'abilità e con la passione per ciò che si fa. Al contrario *Max Weber*[24] nel saggio "L'etica protestante del capitalismo" colloca il concetto di "lavoro" come dovere alla base dello spirito capitalistico che si diffuse all'inizio del Sedicesimo secolo.

24. Maximilian Carl Emil Weber (Erfurt, 21 aprile 1864 – Monaco di Baviera, 14 giugno 1920) è stato un economista, sociologo, filosofo e storico tedesco.
È considerato uno dei padri fondatori dello studio moderno della sociologia e della pubblica amministrazione.

Il lavoro viene considerato da Weber come un dovere che l'individuo deve sentire nei confronti della sua attività professionale intesa come valorizzazione della propria forza lavoro o del suo possesso materiale (capitale).

Quanto esposto è agli antipodi dell'etica hacker del lavoro che trae origini dall'accademia di Platone che enfatizzava la passione per la ricerca intellettuale,. Secondo Weber l'etica del lavoro ha origine nei monasteri grazie alla diffusione della regola benedettina che richiedeva a tutti i monaci di considerare il lavoro loro assegnato come un dovere, nel rispetto del principio secondo cui "l'ozio è il nemico dell'anima".

Secondo questo principio non ha importanza tanto la natura del lavoro, ma piuttosto che questo sia svolto e portato correttamente a compimento. Il lavoro in questa accezione è la cosa più importante della vita. Nei casi più estremi si manifesta come una "dipendenza" che conduce al completo rifiuto degli altri ed all'esaltazione del senso di responsabilità che in alcuni casi si manifesta addirittura con il senso di colpa del lavoratore, nel caso in cui egli, impossibilitato a svolgere la propria attività per motivi di salute, sia costretto a rimanere a casa.

L'etica protestante del lavoro, che continua a dominare tutt'oggi la società, non viene messa in discussione dalla *network society*, ma il fenomeno dell'hacking propone uno spirito alternativo, che mette in dubbio il pensiero corrente.

Non per nulla le prime frange di studenti che hanno avviato il fenomeno dell'hacking negli anni sessanta sembrano avere la loro discendenza, come movimento underground, dagli Yippy, componenti dello Youth International Party, cioè un movimento anarchico hippie: la matrice ideologica e politica di questo "partito", nato per contestare la guerra in Vietnam, comportava una vivace, a tratti surrealistica, polemica sui valori borghesi come proprietà privata, tabù sessuali e abitudini socio-culturali.

3.1.2 Etica del Tempo e del Denaro

Secondo Weber, inoltre, il concetto di lavoro è strettamente connesso con quello di *tempo.*

Lo spirito del capitalismo, infatti, sorge da quel particolare atteggiamento nei confronti del tempo sintetizzato dal famoso slogan di *Benjamin Franklin*[25] "Il tempo è denaro". Del resto quella basata sulle tecnologie dell'informazione (Information Tecnology) è un'economia della velocità basata sull'ottimizzazione ed organizzazione del tempo che consente di fare arrivare le innovazioni scientifiche ai consumatori prima che lo faccia la concorrenza.

La risposta hacker al problema del tempo, sia in termini pragmatici che etici, invece, è di tutt'altro tenore.

In termini pragmatici si può affermare che la creatività, intesa come fonte essenziale della produttività dell'economia dell'informazione, mal si concilia con le condizioni di fretta costante che l'azienda spesso impone al lavoratore per il raggiungimento degli obiettivi prefissati.

Infatti affinché si abbia un sistema produttivo che permetta lo sviluppo di una vera opportunità per il ritmo creativo, è necessario che per la realizzazione dei programmi non siamo stabiliti termini brevissimi. Tutto ciò, sicuramente, mortificherebbe la possibilità di creare "cose interessanti" a detrimento della produttività stessa. Del resto anche *Les Earnest*[26], del laboratorio di intelligenza artificiale dell'università di Stanford, ha offerto un compendio della risposta hacker al problema dell'impiego del tempo che può essere così sintetizzato: "Noi cerchiamo di giudicare la gente non da quanto tempo spreca, ma dagli obiettivi che raggiunge in periodi di tempo abbastanza lunghi…".

Passando ad analizzare i termini etici della questione tempo, vista dal mondo hacker, non si può non partire dalla considerazione secondo cui nella cultura della supervisione dell'orario di lavoro, la maggior parte degli esseri umani finisce per essere condannata all'obbedienza.

Una cultura del genere è stata sempre rifiutata dagli hacker, i quali in nome del rispetto del lavoratore, ma soprattutto dell'individuo in quanto tale, hanno osteggiato costantemente ogni atteggiamento autoritario di qualsiasi impresa o

25. Benjamin Franklin (Boston, 17 gennaio 1706 – Filadelfia, 17 aprile 1790) è stato uno scienziato e politico statunitense. Fu uno dei Padri fondatori degli Stati Uniti nonché un genio poliedrico; svolse attività di giornalista, pubblicista, autore, filantropo, abolizionista, diplomatico, inventore, politico e fu tra i protagonisti della Rivoluzione americana. Era, inoltre, appassionato di meteorologia e anatomia.

26. Lester Donald Earnest nacque negli USA il 30 dicembre 1930. Iniziò la sua carriera come programmatore di computer nel 1954 come ufficiale della U.S. Navy Aviation Electronics e come responsabile del Digital Computer Project al Naval Air Development Center, Johnsville, Pennsylvania.

agenzia governativa.

L'etica hacker, di fronte alla riduzione del valore individuale e della libertà in nome del lavoro, si basa non sul principio "il tempo è denaro" ma piuttosto nel principio "la vita è mia" e va vissuta ora. In altre parole, la vita non è fatta solo di lavoro ma anche di altre passioni alle quali l'individuo deve dare importanza per la realizzazione delle sue più intime aspirazioni.

L'etica hacker e quella protestante differiscono radicalmente anche in ordine alla concezione del *denaro*. Basti pensare all'Open Source Movement e alla Free Software Foundation.

Per Weber, lo spirito capitalistico pone come *summum bonum*, ossia come bene supremo, il "guadagnare denaro, sempre più denaro".

Questo, al pari del lavoro, è visto come fine a sé stante e la *new economy* è tutta protesa al suo accumulo.

Si tratta di un valore cui la società attuale non sembra riuscire a rinunciare e che, al contrario, ne rafforza l'importanza.

Analogamente, anche l'idea di proprietà, estesa all'informazione, ne risulta potenziata: le aziende realizzano i loro profitti cercando di possedere le informazioni tramite brevetti, marchi di fabbrica, accordi di non divulgazione e altri mezzi.

In contrasto con l'etica del denaro protestante, negli hacker si riscontra la convinzione che "la condivisione delle competenze sia per loro un dovere etico". Se storicamente il precursore del controllo sul libero flusso delle informazioni è il monastero, i precedenti storici dell'etica hacker sono l'accademia e l'etica scientifica. Gli scienziati, infatti, mettono a disposizione il loro lavoro affinché altri lo usino, lo testino e lo sviluppino ulteriormente; la loro ricerca è basata sull'idea di un processo aperto e autoregolato.

Infatti, solo grazie ad una critica fornita dall'intera comunità scientifica, le teorie possono essere sviluppate collettivamente e i difetti percepiti possono essere gradualmente eliminati.

Basandosi su questi principi etici molti hacker distribuiscono apertamente i risultati della loro creatività affinché altri li testino e li sviluppino ulteriormente.

Un esempio è Linux, il sistema informatico operativo a 32 bit per personal computer, creato da un gruppo di hacker che hanno usato il loro tempo libero per lavorare insieme al progetto. Per assicurare il carattere aperto, cioè il libero accesso agli utenti, Linus Torvalds ha usato su Linux il concetto di "copyleft", una forma di concessione sviluppata nel progetto Les Earnest di *Stallman*[27], il quale garantisce che tutti gli sviluppi siano disponibili ad altri affinché ne facciano liberamente uso.

Gli hacker, quindi, riconoscono nel denaro una necessità per la sopravvivenza e motivano la propria attività con gli obiettivi del valore sociale e dell'apertura.

Volontà e desiderio di ogni hacker è creare qualcosa di valore per la comunità secondo uno sviluppo che procede attraverso la condivisione delle idee e delle informazioni.

Non è il denaro, ma la gratificazione che deriva dal riconoscimento dei propri pari a spingere gli individui a sviluppare programmi da offrire liberamente.

La vita si compone di relazioni sociali e racchiude in sé un prioritario bisogno di appartenenza, quindi la semplice accettazione da parte della comunità non è sufficiente: occorre conquistarne il rispetto dimostrando le proprie capacità sul campo.

La soddisfazione personale poggia, in altri termini, sulla consapevolezza meritocratica di far parte di un tutto. Per rappresentare la filosofia di apertura e di socializzazione delle informazioni Raymond si serve del modello del *bazar* contrapponendolo a quello della *cattedrale.*

La cattedrale è definita come un modello in cui una persona o un gruppo di persone molto ristretto progetta e tutti gli altri vedranno i risultati definitivi. Nel bazar l'ideazione è aperta a tutti e fin dall'inizio le idee sono messe a disposizione degli altri.

I vantaggi sono rilevanti: quando le idee vengono diffuse in fase iniziale possono essere oggetto di aggiunte o critiche da parte di altri, mentre quando la cattedrale viene presentata nella sua forma definitiva le sue fondamenta non possono essere cambiate. Si tratta di un processo di condivisione nel quale i partecipanti si avvicinano verso nuovi miglioramenti.

27. Richard Matthew Stallman (New York, 16 marzo 1953) è un programmatore, hacker e attivista statunitense. È uno dei principali esponenti del movimento del software libero.

3.1.3 Etica del Network

Oltre all'etica del lavoro e del tempo, secondo *Himanen*[28], esiste un significativo terzo livello dell'etica hacker definibile "netica" o etica del network.

Con questa espressione ci si riferisce al modo di rapportarsi degli hacker alle reti della network society, in un'accezione più ampia rispetto alla *netiquette* intesa come libertà di espressione e libero accesso alla rete. Per gli hacker la libertà di espressione e la privacy sono stati ideali importanti e la rete si è sviluppata coerentemente su questi principi.

Vivere secondo i tre livelli etici del lavoro, del denaro e del network permette il conseguimento del più alto rispetto della comunità hacker.

Se un hacker riesce ad onorare anche un ultimo valore, ovvero la creatività, l'uso immaginativo delle proprie capacità, il continuo sorprendente superarsi e il donare al mondo un nuovo e consistente contributo, ottiene una vera e propria consacrazione. I soggetti che raggiungono questi livelli rappresentano dei veri e propri mentori, garanti della cultura hacker, capaci di dare buoni consigli, d'insegnare la *filosofia di vita hacker.*

Spesso le risposte che essi danno non sono esaurienti, ma dirette a forzare l'allievo a credere in se stesso e a trovare da solo le risposte. Solo indicando gli spunti e fornendo piccoli segreti la curiosità dell'allievo si tiene alta e lo si spinge a lavorare da solo, senza troppi aiuti, senza perdere lo spirito *hacker* della ricerca.

Questo non vuol dire che il mentore lascia carta bianca ai suoi allievi, tutt'altro, esso si sente responsabile delle loro azioni e spesso li protegge dai pericoli della rete.

Il mentore è, quindi, una figura cardine della collettività hacker, non si diventa tali solo perché si è acquisito un titolo, ma per decisione di altri *hacker* in base alle proprie capacità meritocratiche.

28. Il professor Himanen Pekka è uno dei ricercatori più conosciuto al mondo dell'era dell'informazione, i cui lavori sono stati pubblicati in 20 lingue dall'Asia all'America. La sua opera più famosa è senz'altro The Hacker Ethic (2001).

3.2 L'evoluzione dell'etica hacker, generazioni a confronto

Steven Mizrach, antropologo dell'università della Florida, afferma che negli anni si sia sviluppata una nuova etica *hacker*, che si distacca da quella dei giovani studenti del MIT.

Ciò sembra dovuto al fatto che gli *hacker* sono sempre più numerosi e più distanti, di quanto erano gli hacker degli anni sessanta.

Il punto fondamentale in cui le due etiche si differenziano riguarda l'opportunità di divulgare immediatamente e totalmente i dettagli di una vulnerabilità di un sistema. In base alla nuova etica, avvertire l'amministratore del sistema della vulnerabilità trovata può portare ad un'immediata risoluzione del problema. In questo modo non si cerca di sfidare l'amministratore, che di solito è un appartenente alla comunità hacker, ma di informarlo di una vulnerabilità del suo sistema e contestualmente consigliargli il modo in cui risolvere il problema. Solamente qualora il problema non dovesse essere risolto, allora il *bug* verrà divulgato e reso pubblico in Rete.

Il rispetto dell'operatore, quindi, diviene più importate della "condivisione"a tutti i membri della comunità, ormai numerosissimi rispetto ai primi anni.

Legislazione e criminalità informatica

4.1 Situazione attuale

Con lo sviluppo delle nuove tecnologie nel campo dell'informatica e della telematica sono aumentate le opportunità di crescita e di confronto in campo sociale, economico, politico, culturale e scientifico, dove si sono visti ridisegnare gli scenari della vita quotidiana. Le nuove tecnologie, oltre a determinare cambiamenti in tutti i settori di rilevante interesse sociale hanno provocato profonde innovazioni anche nel diritto mettendo in discussione istituti come la giurisdizione, la competenza territoriale ed alcuni principi consolidati, come quello della responsabilità penale: tutto ciò è riconducibile alla nascita di nuove figure e di atti illeciti contro il patrimonio e contro le libertà individuali. L'*hacking* in senso stretto consiste in un accesso non autorizzato ad un sistema informatico, che potrebbe configurare la commissione di un reato.

I c.d. reati informatici possono essere commessi con e senza l'utilizzo del computer. Il danneggiamento volontario, la frode, la ricettazione, il furto, la frode bancaria, lo spionaggio militare o industriale sono tutti reati normalmente commessi senza l'uso del mezzo informatico e telematico, ma ai quali le nuove tecnologie hanno dato nuova sostanza.

Diversi sono i reati strettamente connessi all'*hacking* che però non implicano l'utilizzo dell'informatica, per esempio: il furto per rubare documenti contenenti username e password, qui entra in gioco anche il problema della privacy; in questi casi si è ben lontani dall'etica *hacker*, ma si è in presenza di veri e propri criminali, incuranti dei danni che posso creare nella rete e all'intera comunità.

4.1.1 Definizione di *computer crime*

I reati posso essere di diverso genere e gravità, ma in ogni caso tali condotte hanno convenzionalmente assunto la denominazione di *computer crimes*

essendo accomunate dall'uso degli elaboratori elettronici.

Il *computer crime* si realizza in tutti quei casi in cui il computer si interpone tra l'autore del crimine e la vittima e nel caso in cui rappresenti lo strumento principale per eseguire una determinata azione criminale, alterando la percezione della gravità dell'atto, la percezione della vittima, la stima dei rischi di essere scoperto e catturato.

Il computer, per tali ragioni è stato definito come uno strumento "prone to measure", proprio per sottolineare la sua capacità di divenire oggetto o mezzo per la commissione di reati eterogenei.

Alla luce di tale premesse va sottolineato che le ricerche sul computer crime si focalizzano sullo studio delle variabili percettive e del comportamento dell'individuo indotte dalla tecnologia digitale, soprattutto quando tale tecnologia media una relazione tra autore di un crimine e vittima.

Secondo un'ottica prettamente psicologica di indagine della problematica in esame, l'impatto dell'informatica con il sistema sociale ha imposto dei processi adattivi da parte degli individui anche in ambito criminale ed ha alterato il modo di percepire la realtà, compresi i crimini.

Si può affermare che l'impatto della information tecnology sull'uomo agisce su tre diverse dimensioni: sociale, organizzativa e individuale.

La prima, quella sociale, è strettamente legata all'aumento dell'allarme politico-istituzionale e alla produzione di un corpo normativo specifico.

La seconda dimensione, concernente l'organizzazione, è riferibile alla necessità, da parte delle aziende e delle istituzioni, di affrontare il problema del cyberspazio come proprietà privata, essendo esso divenuto luogo di concentrazione di interessi economici ed elevati investimenti, oltre che spazio di interconnessione tra i vari comparti della Pubblica Amministrazione.

La terza dimensione del fenomeno, quella individuale, è legata all'impatto dell'informatica sugli schemi cognitivi degli individui ed alla sua induzione ad alterazioni percettive che possono interferire, a vario titolo, sui livelli di consapevolezza dei delinquenti durante le loro azioni criminali.

Da un'analisi specifica della dimensione "sociale" del fenomeno si ricava che la minaccia criminale nel mondo virtuale non è assimilabile a quella tradizionale

strettamente radicata sul territorio ed ivi localizzata, ma assume una connotazione transnazionale, svincolata dai confini dei singoli Stati.
Le tradizionali condotte criminali che trovano la loro naturale espansione nella realtà virtuale si affiancano ad una serie di comportamenti che oscillano tra il lecito e l'illecito e che sono dannosi e lesivi di interessi universalmente riconosciuti e meritevoli di tutela.
In breve, con l'avvento dell'informatica e di Internet si è assistito alla modifica delle forme criminali tradizionali in forme criminali che agiscono all'interno dei nuovi sistemi di comunicazione digitale.

Tra i più importanti e gravi fenomeni di criminalità informatica si possono distinguere:la cyberpedofilia (scambio di pedopornografia); il cyberterrorismo; la diffusione di virus informatici; le truffe telematiche via e-mail; *netstrike*[29]; violazione della privacy di aziende; diffusione di informazioni illegali online (violenza, razzismo, esplosivi, droghe, sette sataniche).
La caratteristica peculiare di tali illeciti è la distanza tra i cybercriminali e le loro vittime potenziali.
La condotta delittuosa può concretizzarsi in più azioni svolte in tempi diversi o contemporaneamente, da uno più soggetti, in luoghi diversi o in uno spazio virtuale.
Le vittime possono essere colpite immediatamente a distanza di tempo in uno o più luoghi.
Lo scenario del computer crime si articola sostanzialmente attraverso tre fattori emergenti: utilizzo dell'informatica da parte di criminali professionisti che hanno colto le nuove opportunità offerte dalla tecnologia per incrementare i loro guadagni e per eludere con più facilità le strategie di contrasto da parte delle agenzie istituzionali; azioni eclatanti da parte di soggetti che compiono crimini come "funzione espressiva" (es. rubo con il computer per dimostrarmi quanto sono bravo) e non come "funzione strumentale" (rubo con il computer perché mi servono i soldi); azioni illegali svolte da soggetti di basso profilo criminale o completamente estranei al mondo del crimine che confondono, sottostimano o addirittura ignorano la dimensione dissociale e antigiuridica di comportamenti

eseguiti in ambiente digitale (per esempio adolescenti che utilizzano l'hacking per soddisfare la loro voglia di trasgressione e di distruzione).

La spiegazione del crimine tecno-mediato e la definizione della responsabilità e dei livelli di consapevolezza ad esso correlati, implicano la necessità di un esame dell'influenza della dimensione digitale sulla modalità percettiva e valutativa del soggetto nelle varie fasi dell'azione illegale.

Poiché spesso il cybercrime altera la percezione, la distinzione e la valutazione degli effetti provocati con il proprio comportamento ed attenua altresì la stima delle reali possibilità che il proprio crimine venga scoperto e sanzionato, si può ritenere che la mediazione di uno spazio virtuale in un crimine possa generare i seguenti fenomeni:

1) allargamento del numero dei possibili autori del reato rendendo adatti al crimine molti individui avulsi al mondo dell'illegalità;

2) creazione di una manifestazione di illegalità distribuita in larghe aree sociali;

3) diffusione di atteggiamenti di impunità su determinati crimini;

4) scarsa conoscenza delle leggi civili e penali in materia.

Un esempio concreto di bassa percezione e di scarsa valutazione degli effetti delle azioni illegali attraverso l'uso degli strumenti informatici, è ravvisabile nel comportamento di molti giovani hacker che considerano l'hacking soprattutto come un vezzo, un gioco o un sistema per dimostrare a sé ed agli altri la perizia acquisita in campo informatico, evidenziando profili criminologici abbastanza bassi.

Spesso il compimento di tali condotte illegali (come ad esempio l'utilizzo di internet per trasmettere virus, violare la privacy, rubare o sabotare informazioni preziose, organizzare frodi e manipolare mercati azionari) è giustificato non da un vantaggio per l'autore, in termini pragmatici, ma piuttosto dalla valenza comunicativa che tali azioni implicano nell'ambiente esterno e nei confronti di se stesso. Danneggiare un sistema informatico, diventa così uno strumento per dimostrare a sé ed agli altri che si è in grado di farlo, così da aumentare il livello di autostima.

Molte indagini statistiche di settore, del resto, hanno dimostrato che l'hacking può rappresentare per i giovani una forma di devianza, utilizzata per entrare in

comunicazione con il mondo degli adulti “a livello paritetico”, attraverso il canale criminale. L’essere considerati “importanti” potrebbe in tal modo rappresentare un elemento affascinante per alcuni soggetti che vivono particolari condizioni di disagio. Alla base di tale deviante modello esistenziale si collocano, il più delle volte, quelle difficoltà che gli adolescenti incontrano nel particolare e delicato momento della crescita nel quale le attese sono fortemente influenzate dai processi di socializzazione vissuti precedentemente e dal modo in cui essi interpretano le aspettative degli altri nei loro confronti.

Diverso è, invece, l’atteggiamento degli hacker “esperti” (i “veri hacker”) in ordine alla percezione e/o consapevolezza dell’azione criminale.

In tale categoria di soggetti predomina la convinzione di appartenere ad un’élite di “commandos” destinati a violare quelle regole non ritenute importanti in quanto dettate ed imposte da organizzazioni che controllano il mondo con il fine esclusivo di accrescere il proprio potere ed il proprio patrimonio.
Il principio cardine che regola l’azione degli hacker, del resto, è noto ed è bene ribadirlo: la conoscenza del computer è fondamentale per il miglioramento della vita dell’uomo ed ogni ostacolo alla libera diffusione della cultura informatica deve essere rimosso combattendo, fra l’altro, le multinazionali dell’informatica.
Si giustificano così le azioni lesive dell’immagine di sicurezza ed affidabilità dei software prodotti da tali aziende ed in tale ottica si può anche ritenere che la creatività dell’hacker si contrappone, prevalentemente, all’azione monopolistica e speculativa delle multinazionali.
Anche in tale contesto, tuttavia, le dinamiche di illegalità possono essere lo specchio di condizioni di disagio, esorcizzate attraverso azioni telematiche di disturbo e di danneggiamento che presentano, attualmente, contorni meno definiti rispetto a quelli del sistema socio-culturale convenzionale. Ciò nondimeno, le azioni di intrusione telematica, come già detto, rappresentano il più delle volte vere e proprie condotte criminali e come tali perseguibili da norme penali.

4.1.2 *Criminal Profiling*

Si è cercato a questo proposito di studiare la psiche degli *hacker ,* avvicinandosi al loro ambiente ed osservando i loro comportamenti.

In questo studio, una tecnica prestata all'informatica giuridica che ha riscosso molto successo per i risultati ottenuti è il *Criminal Profiling.*

Strumento utilizzato dagli investigatori per conoscere la psiche dei criminali, la loro personalità, abitudini di vita, status sociale, al fine di restringere il numero dei sospetti e arrivare ad una più rapida individuazione del responsabile.

Questa tecnica serve, oltre a tracciare un profilo psicologico dell'autore del reato, anche a collegare crimini correlati, per individuarne l'autore e fornire strategie d'interrogatorio.

L'*hacker* viene studiato come un soggetto seriale, cioè un soggetto che agisce in maniera costante, con uno specifico *modus operandi e firma.*

Con riferimento al *modus operandi* di un attacco informatico, gli *hacker* seguono condotte standardizzate con lo scopo di "bucare" un sistema per le più svariate motivazioni; le comuni tecniche di *Criminal Profiling* devono essere, quindi, rielaborate per adattarle alle peculiarità della materia.

Scopo dello studio è stabilire perché viene compiuto l'attacco e le caratteristiche di chi lo compie, cioè capire cosa è accaduto e come.

Un ruolo fondamentale è ricoperto dagli esperti di sicurezza informatica, che hanno il compito di dire "cosa" è realmente accaduto e "come" ciò è stato desunto dell'analisi della scena del crimine.

Nel caso di attacchi informatici, infatti, non c'è raccolta di DNA, ma di files in cui vengono registrate le attività compiute nell'ambito del sistema informatico o telematico.

Sulla base del *Criminal Profiling* è possibile affermare che gli *hacker* provengono dai ceti sociali medio-bassi. Un altro aspetto su cui ci si basa per tracciare il profilo di un hacker, è sicuramente il rapporto che questo ha con la società.

Gli psicologi e gli esperti di *Criminal Profiling* li etichettano come individui dalla personalità contorta, considerandole persone introverse ed antisociali, che si

sentono più a loro agio a rapportarsi tramite relazioni virtuali, che con modalità tradizionali.
Oggi, però, sempre più spesso, persone comuni tendono a stringere amicizie su *blog* e *chat*. Quindi, sfatando i sempre più numerosi luoghi comuni, è possibile affermare che sicuramente gli *hacker* hanno in genere una personalità eccentrica, ma sono comunque persone perfettamente normali.

4.2 Gli interventi legislativi contro i reati informatici

Appare opportuno soffermarsi ad analizzare brevemente il modo in cui gli ordinamenti giuridici hanno tentato di osteggiare il fenomeno della criminalità informatica, anche a livello penale, non solo per quanto riguarda la semplice regolamentazione, ed il loro atteggiamento di fronte all'esigenza di tutela di quegli interessi che ormai nello spazio virtuale rivestono la stessa importanza degli interessi riscontrabili nel mondo reale.

La necessità di un intervento legislativo in materia penale volto a reprimere comportamenti socialmente dannosi o pericolosi, legati alle nuove tecnologie informatiche, è stata avvertita con una certa apprensione fin dai primi anni ottanta da parte di numerosi Stati, sia europei (ad esempio Danimarca, Norvegia, Austria, Francia) che extraeuropei (Stati Uniti, Australia, Canada, Giappone).
Un rapido sguardo al panorama normativo internazionale mostra, quindi, come il legislatore italiano si sia mosso con un certo ritardo, avendo posto (o tentato di porre) rimedio alle lacune esistenti nell'ordinamento giuridico. Infatti solo alla fine del 1993 con la legge 23 dicembre n. 547 ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"), ha introdotto nell'ordinamento penale specifiche ipotesi di reato relative al computer crime, ampliando i poteri degli inquirenti nella fase di acquisizione delle prove, prevedendo intercettazioni informatiche e telematiche (art 266 bis c.p.).
Sul piano sostanziale, inoltre, sono state introdotte ipotesi di reato inerenti alla frode informatica (art. 640 ter c.p.), ai documenti informatici (art. 491 bis), al

sabotaggio telematico (art. 420 c.p.) al danneggiamento di sistemi informatici e telematici (art. 635 c.p.), all'accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.), all'intercettazione non autorizzata di comunicazioni informatiche o telematiche (art. 617 quater c.p.).

Sono state inoltre previste ipotesi di reato consistenti anche nella detenzione e diffusione abusiva di codici di accesso a sistemi informatici (art. 615 quater c.p.), nella diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies), nella violazione, sottrazione e soppressione di corrispondenza (art. 616 c.p.), nell'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche e telematiche (617 quinquies), o di falsificarne, alterarne o sopprimerne il contenuto (617 sexies) e infine, nella rivelazione del contenuto di documenti segreti o di comunicazioni e conversazioni (art. 621 e 623bis c.p.).

Prima della legge 23 dicembre n. 547 del 1993, in Italia, alcuni sporadici interventi settoriali avevano interessato, in maniera più o meno diretta, questa materia: è il caso della legge 18 maggio 1978 n. 191*,* con la quale era stato introdotto nel codice penale l'art. 420 che, nel sanzionare l'attentato ad impianti di pubblica utilità, menzionava espressamente anche gli impianti di elaborazione di dati (tale norma è stata integralmente sostituita dall'art. 2 della legge 547) .

Si può inoltre ricordare la legge 1º aprile 1981 n. 121*,* contenente il "Nuovo ordinamento dell'Amministrazione della Pubblica Sicurezza", istitutiva di un Centro di elaborazione dati presso il Ministero dell'Interno e rappresentativa della prima forma di tutela di dati archiviati in un sistema informatico.

Altre disposizioni relative a reati informatici sono state poi emanate solo negli anni novanta: così, ad esempio, l'art. 12 della legge 5 luglio 1991 n. 197, che punisce l'uso indebito di carte di credito, o l'art. 10 che tutela penalmente una serie di condotte definibili "pirateria informatica" (decreto aggiornato dal d. lgs. 205/96 ed in seguito modificato dalla legge n. 248 del 2000), fino ad arrivare ad atti normativi più recenti, a tutela della *privacy* e delle banche di dati, rappresentati dalla legge n. 675 del 1996 ("Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") e dal decreto legislativo n. 169 del 1999 ("Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche

di dati").

Per la tutela dei minori contro la pornografia infantile su Internet inoltre, è stata introdotta la legge 3 agosto 1998, n. 269, "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno dei minori, quali nuove forme di riduzione in schiavitù".

In tema di criminalità informatica, nonostante siano passati molti anni dalla sua entrata in vigore, la legge n. 547 del 1993 conserva un ruolo centrale.

Occorre ricordare come, tra le tante disposizioni penali che oggi presidiano l'uso delle tecnologie informatiche, assume un particolare rilievo la citata disciplina a tutela dei programmi per elaboratore.

Tale disciplina nelle sue previsioni penali, comunque, non può essere applicata a condotte realizzate da *hacker*, riferendosi espressamente a finalità di "lucro (oggi "profitto") incompatibili con l'etica hacker.

4.3 Diritto d'autore nell'era digitale

Tra le problematiche legate alle difficoltà di adattamento delle norme giuridiche ai reati informatici, un caso di particolare complessità è quello del diritto d'autore.

La legge sul diritto di autore, Legge n. 633 del 22 aprile 1941, tutela le opere dell'ingegno a carattere creativo purché siano originali.

Il concetto di "opera originale" è ben più ampio di quello di "opera d'arte" in senso stretto, in quanto prescinde da qualsiasi valutazione circa il valore artistico o di bellezza dell'opera.

Oggetto della tutela, quindi, non è tanto l'idea contenuta nell'opera di ingegno bensì il modo con cui questa viene espressa; non è l'argomento in sé bensì il modo e la forma con cui questo viene espresso. Al proprietario dell'opera vengomo riconosciuti sia una tutela morale come: diritto di paternità dell'opera; diritto all'integrità dell'opera, diritto alla pubblicazione (o di inedito), diritto di pentimento; sia una tutela patrimoniale, garantendo: diritto di riprodurre, di eseguire, di rappresentare, di diffondere, di distribuire, di noleggiare, di prestare, di elaborare o trasformare e modificare.

Un testo sulla storia di Roma, ad esempio, è tutelato non per le idee o le teorie in

esso espresse (che potrebbero anche essere trite e ritrite), ma in relazione all'originalità del modo con cui queste vengono esposte dall'autore.

Quasi tutto su Internet dovrebbe essere considerato protetto dal diritto d'autore o dal copyright nei paesi di common law.

Lo scopo del diritto d'autore è quello di promuovere l'espressione creativa o scientifica, dando l'incentivo per inventare nuove cose. Esso dà al titolare il diritto esplicito di decidere come può essere usato il suo lavoro. Solamente il creatore originale ha il diritto di autorizzare o rifiutare la riproduzione, la distribuzione, l'esecuzione, o la rappresentazione del suo lavoro. Solo lui può decidere se un altro può utilizzare il suo lavoro.

La tutela del diritto d'autore in in rete è particolarmente difficile.

Internet è una nuova forma di comunicazione che collega la gente del mondo intero e tutti possono accedervi, acquisendo ogni tipo di informazione disponibile. L'opinione errata, che la maggior parte delle persone abbia il potere di copiare qualsiasi cosa indistintamente, è dovuta all'estrema facilità con cui si possono riprodurre i *file*.

Nell'era digitale in cui viviamo si può copiare quasi tutto da Internet, dai grafici alla musica. Cliccando sul mouse è possibile trasferire un lavoro originale salvandolo sul proprio *hard drive*, ma non significa che sia sempre legale.

La tutela del diritto d'autore viene, dunque, messa in crisi dall'avvento delle nuove tecnologie, che permettono nuove forme d'accesso al sapere, come gli hacker da anni auspicano a gran voce sulla rete. Accanto a chi come gli *hacker* propugna il libero accesso alla conoscenza, c'è chi, al contrario, afferma il carattere privato della proprietà intellettuale a tutti i livelli.

Una disciplina equa dovrebbe cercare di accordare queste due posizioni così agli antipodi e tenere in considerazione il carattere immateriale delle nuove opere digitali, che non possono essere tutelate come le opere tradizionali.

Uno strumento volto al controllo di ciò che circola su di un computer, e che valuti se esso rispetti determinate condizioni legali è il DRM (*Digital Rights Management*, una serie di sistemi tecnologici mediante i quali i titolari di diritti d'autore possono esercitare ed amministrare tali diritti nell'ambiente digitale, grazie alla possibilità di rendere protetti, identificabili e tracciabili tutti gli usi in

rete di materiali adeguatamente “marchiati”) per la protezione degli oggetti culturali in formato digitale tutelati dal diritto d’autore o dal *copyright* (in particolar modo tutela i brani musicali).

L’esempio più noto di programma che integra un DRM è il software “i-Tunes” di Apple, questo permette di gestire i file musicali presenti su di un computer e garantisce l’accesso a *music store on line* di Apple, permettendo di scaricare legittimamente brani musicali a prezzi accessibili, garantendo, inoltre, la copia in un numero limitato di volte.

Lo stesso Linus Torvalds, importante esponente della FSF, ha dichiarato che certe forme di DRM non sono affatto malevole, ma possono servire a garantire maggior sicurezza per l’utente. Allo stesso modo anche Microsoft si è mossa verso il mondo *open source,* concedendo maggiori facoltà ai suoi utenti e ricevendo in questo modo anche un plauso dalla *Free Software Fondantion.*

Fenomeni di degenerazione legati all'Hacking

5.1 Disagio sociale e giovanile

Abbiamo visto nel capitolo precedente come le azioni di pirateria informatica, oggetto d'indagine in vari ambiti di ricerca (criminologia, psicologia, sociologia), risultano essere frutto di dinamiche complesse, strettamente legate ai processi di interazione dell'autore con le norme penali e sociali, con l'ambiente esterno, con le vittime e, in definitiva con il proprio sé.

Appare a questo punto opportuno soffermarsi a ricostruire analiticamente il percorso che porta gli hacker ad assumere un'identità deviante meritevole di interesse da parte delle scienze sociali.

Bisogna, naturalmente partire dal concetto di "devianza" per vedere in quali termini esso si può associare al fenomeno dell'hacking.

Il termine devianza (desviaciòn social, deviancy, déviance sociale, soziale Abweichung o Devianz) ha una lunga storia nella letteratura sociologica teorica ed empirica, il dizionario di sociologia dà la seguente definizione di devianza:

"Atto o comportamento o espressione, anche verbale, del membro riconosciuto di una collettività, che la maggioranza dei membri della collettività stessa giudica come uno scostamento o una violazione più o meno grave, sul piano pratico o su quello ideologico, di determinate norme o aspettazioni o credenze che essi giudicano legittime, o cui, di fatto, aderiscono e al quale tendono a reagire con intensità proporzionale al loro senso di offesa".

Gli elementi minimi e costitutivi di questa definizione, rilevanti dal punto di vista del sociologo sono:

a) un attore individuale o un gruppo;

b) un comportamento che si qualifica per la sua relativa eccezionalità nei confronti del quadro normativo generalmente accettato da una società- Stato nonché codificato dal diritto positivo e comunque, ben radicato nella cultura dominante del tempo.

Dunque due aspetti vanno sottolineati sul piano interpretativo: il comportamento

deviante è relativo all'azione di alcuni attori ed è storicizzato, vale a dire non risulta sempre identico nelle varie epoche e nei vari luoghi.

Si spiega così il fatto che le definizioni correnti nei manuali di sociologia e nelle enciclopedie di scienze sociali propongono, quasi sempre, un punto di vista sulla devianza nettamente relativistico, che riconduce l'attributo deviante ad una valutazione che si dà dell'azione piuttosto che ad una sua caratteristica effettiva.

In altri termini: il deviante è un attore che adotta un comportamento che tradisce, in vario modo e con conseguenze disparate, le aspettative che usualmente definiscono il senso della realtà quotidiana di un ambiente sociale con il quale il deviante interagisce. Per effetto dell'azione deviante una norma istituzionalizzata perde la sua efficacia o, in parole più povere, non fa più presa su quel soggetto particolare.

L'atto deviante, in genere, non resta però privo di conseguenze; di solito produce una reazione dalla forma diversificata che testimonia il bisogno insopprimibile di controllo sociale che qualsiasi organizzazione sociale in ogni tempo ed in ogni luogo deve manifestare se vuole esistere.

Questa reazione può essere letta come un'espressione "naturale" della struttura normativa della società, che pretende di ricucire la smagliatura aperta dalla devianza e di mantenere così la sua operatività.

Ove non ci sia una reazione della società, l'atto non può maturare la sua connotazione come atto deviante, se non astrattamente, in quanto non viene riconosciuto.

La norma agisce socialmente attraverso due canali: la legittimazione, vale a dire l'adesione "normale" alle aspettative di comportamento anche per merito di un processo di socializzazione ben riuscito, oppure con l'azione degli apparati di controllo che funzionano erogando sanzioni al fine di ripristinare lo stato di conformità antecedente all'atto deviante.

La definizione scientifica della devianza assume connotazioni diverse in riferimento all'impostazione teorica generale adottata da chi la studia. Il sociologo positivista, ad esempio, fa coincidere l'atto deviante con il rifiuto della norma codificata e si preoccupa di individuare le motivazioni che inducono alla devianza. In questo caso, dunque, l'azione deviante ha una sua marcata

specificità come oggetto di studio.

Il sociologo marxista tende, invece, a privilegiare un'impostazione secondo cui la devianza si connette a determinati ruoli definiti, naturalmente, dalla differente appartenenza di classe e dalla posizione che i soggetti occupano nel processo produttivo, matrice determinante della struttura della società e dunque anche radice ultima del comportamento deviante.

Ovviamente, a seconda dell'impostazione teorica prescelta, oppure in funzione di alcune scelte di valore predilette, ci si imbatte in una diversa classificazione degli atti devianti.

Usualmente tutti i testi di sociologia parlano di comportamento deviante quando fanno riferimento ad una molteplicità di comportamenti ascrivibili a diverse tipologie di individui:

a) Malati: tossicodipendenti, alcolisti, affetti da patologie legate a pratiche o stili di vita considerati sconvenienti, per i quali la qualifica di devianza assume la connotazione di patologia.

b) Diversi: omosessuali, handicappati fisici e psichici, che sono espressione della devianza come anormalità.

c) Ribelli:, le cui scelte di vita sono connotate come ricerca di alternative.

d) Delinquenti: trasgressori di norme del diritto che impersonano l'accezione di devianza come reato o crimine.

E' proprio la categoria dei "ribelli" (contestatori, innovatori rivoluzionari), che più delle altre, richiama immediatamente la figura degli hacker.

Non va dimenticato, infatti, che il termine hacker non contraddistingue semplicemente colui che irrompe nei computer, ma uno stile di vita e un modo di essere caratterizzato da una curiosità irrefrenabile e dalla voglia di venire in possesso di qualsiasi informazione. Nessuna barriera alla conoscenza, né autorità che si anteponga alla verità: questa è la loro ideologia.

Se a ciò aggiungiamo che la condotta degli hacker (o, quantomeno di una categoria di essi), è a volte contraddistinta dall'utilizzo della rete telematica per finalità illegali, o prive di apparenti giustificazioni morali, è del tutto evidente che il loro comportamento non può che essere qualificato come "deviante".

Nell'hacker, cioè, sono ben visibili gli elementi minimi e costitutivi presenti nella

definizione di devianza più sopra riportata: un attore individuale o un gruppo (c.d. banda) che, avvalendosi delle alte conoscenze informatiche, viola le regole o le norme attraverso il compimento di reati informatici, tradendo così le aspettative che i membri del sistema sociale ha nei suoi confronti.
Per tale motivo, il suo comportamento deviante, disfunzionale e pericoloso non può che essere valutato negativamente dalla società. Anche per gli hacker, quindi, è possibile parlare di due principali cause di devianza: un difetto di socializzazione, vale a dire una scarsa interiorizzazione di valori e norme, e tensioni psicologiche legate all'infanzia, in base alle quali viene meno l'adesione al sistema normativo.
Quest'ultimo aspetto, che suscita un particolare interesse tra gli esperti di sociologia della devianza, merita ulteriore approfondimento.

Come risulta dai numerosi esempi e dalle indicazioni disponibili sui siti, l'età in cui più probabilmente si sviluppa la tendenza alla criminalità informatica corrisponde a quella adolescenziale
La necessità di definirsi, espressa dagli hacker, nonchè il rifiuto delle regole, lo spirito di corporativismo in nome di un interesse comune e inoltre la tendenza ad adottare modalità irresponsabili "prive di coscienza sociale", sembrano rispecchiare le problematiche tipiche dello sviluppo. L'insieme delle relazioni all'interno delle quali vengono attuati i crimini informatici lascia inoltre spazio a considerazioni sui temi dell'aggressività, della trasgressione, dell'amore per il rischio e della socializzazione E' stato rilevato che la trasgressione è una caratteristica universale dell'adolescenza e che in essa si realizza la tendenza a mettere in discussione le regole educative e sociali.
Il punto difficile da superare per un ragazzo in questa fase è l'abbandono delle illusioni e l'assenza di regole precise, tipiche dell'infanzia e il riconoscimento delle regole sociali che lo circondano. Tale accettazione spesso è difficile e il rifiuto si manifesta con aggressività, chiusura, asocialità, che se vengono ben affrontate portano alla formazione di una propria identità.
Bisogna aiutare l'adolescente a rendersi consapevole del significato inconscio dei suoi comportamenti, affinché li possa orientare e controllare.

Egli deve abbandonare i sogni megalomaniaci che erano appartenuti all'infanzia, relegandoli alla fantasia e fronteggiando il senso di timore e di panico che ne deriva.

La difficoltà a portare a compimento questo difficile compito è il motivo per cui molti adolescenti cercano di rimanere indefinitamente in una fase transitoria, in una condizione che può essere definita "adolescenza prolungata".

In questa particolare fase il computer è paragonabile ad un oggetto o un luogo sicuro che qualcuno vorrebbe non lasciare mai, al pari di quegli oggetti (come la copertina di Linus) a cui i bambini fanno ricorso al momento dell'esplorazione del mondo oltre la culla, interpretati dapprima come inseparabili da sé e successivamente abbandonati pur mantenendone l'esperienza.

Inoltre la nozione di aggressività si associa all'intenzione di arrecare un danno a un'altra persona. L'atto aggressivo, quando non dipende da un disturbo della personalità, è la normale espressione della ribellione adolescenziale alle regole che hanno caratterizzato la dimensione educativa entro la quale il giovane è cresciuto.

In questo senso si può ipotizzare che gli hacker effettuino un tipo di aggressione che non da modo di doverne fronteggiare la realtà fisica.

La tendenza al crimine è stata invece riferita a una cattiva integrazione o, comunque, come risposta a particolari condizioni della struttura sociale di appartenenza. La soluzione talvolta operata dall'adolescente, che vive la frustrazione dell'ambiente come una minaccia alla propria individualità, è quella dell'affiliazione alle bande antisociali.

Questa affermazione sembra corrispondere alla modalità secondo cui le "bande di hacker" si uniscono sotto una bandiera comune giurandosi reciproca fedeltà e collaborazione.

Non bisogna dimenticare che molte delle incursioni più spettacolari sono state compiute in gruppo, ed induce a riflessione il pensare che si tratti di individui che in realtà non si sono mai visti e che forse abitano a migliaia di chilometri di distanza.

Il desiderio di eccellere è una possibile conseguenza della perdita dell'immagine idealizzata dei genitori e dell'importanza di innalzarsi, la necessità di condividere il

gergo e gli interessi con il gruppo dei pari, magari oltrepassando i limiti e diventando un eroe, essere tipi eccezionali.

Dalle illusioni su se stessi può emergere anche la megalomania, ed è questa che può anche spingere l'adolescente sulla strada della criminalità.

L'adolescenza è il periodo in cui è centrale la ricerca dell'identità e i mutamenti del corpo innescano una ridefinizione globale dell'esperienza. Le prese di posizione degli hacker presentano ricorrenti allusioni al disagio esistenziale e alla necessità di trovare una definizione di sé.

Nel mondo della Rete l'identità è solo un concetto, per via dell'impossibilità di dimostrare fisicamente la propria presenza; la scelta poi di celare anche quel poco di sé che è espresso nel nome, fa sì che l'unico modo per affermarsi sia quello di compiere qualche grande impresa, qualcosa per cui sia possibile essere considerato "un eroe".

La maschera dell'Io presentata in rete è solo un'alternativa alle molteplici maschere presenti e passate di cui l'individuo dispone e questo permette di capire perché un numero sempre maggiore di persone "avvii relazioni sociali senza mai incontrarsi nel senso più comune del termine". Ciò è ovviamente possibile grazie alle tecnologie che consentono una "comunicazione mediata".

L'identità, arricchita da "protesi comunicazionali", diviene qualcosa di fluttuante.

Gli hacker, possiamo dire, fanno ampio uso di "protesi tecnologiche" e di una tecnologia avanzata che usano per modificare se stessi e la configurazione delle loro macchine, insieme e separatamente; soprattutto utilizzano il computer per sviluppare forme di interazione sociale non ordinarie, nel corso delle quali la loro identità si modifica e nello stesso tempo, viene modificata. Il computer non è soltanto uno strumento, ma un teatro di esperienza sociale in cui il soggetto multiplo "è l'elemento socializzante all'interno della rete".

In conclusione, l'utilizzo della tecnologia, che amplia la dimensione corporea per mezzo delle macchine (in questo caso del computer) fonde la base biologica del corpo con quella tecnologica.

Occorre a questo punto analizzare i rimedi che si possono ipotizzare per ovviare a tali conseguenze dannose.

5.2 Interventi specifici: il progetto educativo-promozionale

Alla luce delle considerazioni sin qui svolte, gli spunti di riflessione per ritenere che alcuni hacker, nei casi in cui le caratteristiche di disagio sopra descritte siano particolarmente accentuate, siano da considerarsi dei soggetti che vivono una condizione di malessere e quindi di disagio da non sottovalutare.
E' opportuno domandarsi *come affrontano gli operatori sociali il fenomeno dell'hacking, inteso come nuova forma di devianza, anche in considerazione delle vaste proporzioni da esso assunte nell'odierna società del benessere.*

Purtroppo ad oggi non si riscontrano, nel settore del servizio sociale, interventi mirati all'assistenza ed al recupero dei giovani hacker.
Eppure aiutare un individuo a rendersi consapevole del significato inconscio dei suoi comportamenti devianti, affinché li possa orientare e controllare, dovrebbe rappresentare il compito principale affidato all'assistente sociale.
Una delle tante definizioni di servizio sociale lo ritiene come l'arte di svolgere servizi diversi per raggiungere il miglioramento della società, o anche come attività organizzata che tende a favorire un reciproco adattamento degli individui all'ambiente sociale.

Recuperare un giovane che impatta nel fenomeno del computer crime richiede una programmazione di interventi che vede impegnati ed interagenti vari soggetti: il minore, la famiglia, l'ambiente in cui vive, la scuola, i servizi sociali.
Gli interventi, in particolare quelli del servizio sociale, devono essere improntati in primo luogo su una dimensione preventiva ed educativa e, in secondo luogo, sulla costruzione di progetti che tengano conto dell'azione formativa da condurre sul territorio.
In campo sociale, per prevenzione si intende "un'azione sociale complessa orientata ad innovare le organizzazioni, le istituzioni ed i servizi, in modo che, rispondendo ai reali bisogni cittadini, costituiscano un tessuto non favorevole alla emersione di comportamenti distruttivi".
Questo ci porta a considerare e rilevare le due componenti interne della

prevenzione: una di limitazione dei fattori di rischio e l'altra, invece, di promozione del cambiamento.

Tuttavia non si può non rilevare che nel termine "prevenzione" si possono cogliere alcuni elementi di ambiguità che renderebbero auspicabile un suo superamento.

Per chiarire, non si attuerebbero azioni preventive se non si pensasse che i soggetti dell'intervento non fossero potenziali disadattati o devianti.

Lo stesso termine indica "essere prevenuto", ossia nutrire del pregiudizio. E' proprio questa la ragione per cui, con riferimento agli hacker, è decisamente meglio utilizzare il concetto di "promozione", cioè di creazione di un equilibrio.

Impostare progetti di interventi in ottica promozionale comporta, a differenza della prevenzione, di operare in ambito di "normalità" e non di "devianza", su tutti gli adolescenti o giovani e non solo su quelli che si sono resi protagonisti di atti di pirateria informatica.

Del resto gli hacker, per definizione, non compiono atti devianti; anzi come abbiamo avuto modo di osservare, la maggior parte di essi sono veri e propri attivisti che tematizzano atti sociali.

In tale contesto entra in gioco il ruolo dell'assistente sociale che deve discernere tra hacking inteso come patologia e hacking inteso come controcultura e, quindi, con una sua legittimità.

Tale fondamentale discernimento si reputa opportuno per gli operatori sociali affinché questi pongano la loro attenzione, in particolare, sulla dimensione educativa degli interventi, che si traducano in un'azione formativa da portare avanti nel contesto sociale giovanile.

Ciò per evitare che gli hacker vengano solo criminalizzati o visti come soggetti portatori di disagio.

Del resto prevenire il disagio adolescenziale è pressoché impossibile; bloccare, infatti, il disagio evolutivo equivarrebbe a fermare il processo di crescita dell'adolescente, mentre ostacolare il disagio socio-culturale comporterebbe un cambiamento globale del nostro sistema sociale, si possono però rendere queste fasi della vita, più costruttive e meno dannose per la personalità dell'individuo e per la società.

Tutto ciò premesso, considerato che per il giovane l'ambiente di sviluppo e di crescita culturale e morale, dopo la famiglia, è indubbiamente la scuola, un progetto di intervento in ottica promozionale potrebbe consistere nell'introduzione, proprio all'interno dell'istituzione scolastica, di corsi formativi ed educativi finalizzati ad un corretto utilizzo dei nuovi media e in particolare, di internet.

Ciò comporterebbe di volta in volta, da parte dei servizi sociali, l'organizzazione di incontri periodici dei giovani con sociologi specializzati in "media education" che affrontino temi come la dipendenza dal computer, etica e cultura hacker, e quant'altro serva a delineare il giusto rapporto tra giovani e telematica intesa anche come circuito in cui vengono scambiate le informazioni sulle tecniche di hacking.

Se lo spazio dedicato al problema dalle istituzioni scolastiche si dimostrasse insufficiente, il progetto educativo promozionale in questione si potrebbe pur sempre integrare con l'attività dei Centri di Aggregazione Giovanile (CAG), istituiti al fine di rispondere ai bisogni di educazione extra-scolastica.

Anche all'interno di questi centri (presso i quali vengono svolte o coordinate attività sociali, educative, culturali, ricreative, sportive per finalità di socializzazione e aggregazione dei giovani) si potrebbe istituire una sorta di laboratorio pedagogico per la ricerca di forme adeguate di approccio educativo all'utilizzo del web.

I CAG, con l'ausilio di interlocutori esterni (sociologi, esperti di informatica, psicologi, criminologi), potrebbero rappresentare luoghi di osservazione della dimensione comunicativa dell'azione degli hacker, così da offrire a coloro i quali vi partecipano, validi strumenti di relazione e di confronto con una realtà (quella virtuale) che potrebbe coinvolgerli in modo fuorviante ed antisociale.

Si pensi a un percorso formativo che tenga conto di come educare un ragazzo al giusto utilizzo di uno strumento di "semplice" comunicazione come la chat.

Nell'ambito di tali strutture, così come all'interno delle istituzioni scolastiche, si potrebbero realizzare modelli di valutazione che permettano una verifica continua del programma educativo e promozionale, tramite la somministrazione ai giovani di appositi questionari dai quali possa evincersi quale sia la considerazione da

essi raggiunta di fronte allo sviluppo tecnologico ed all'utilizzo dei nuovi media. Da tali verifiche il servizio sociale sarebbe in grado di monitorare costantemente il grado o la qualità delle conoscenze informatiche acquisite, anche nell'ambito degli incontri programmatici, nonché il rapporto dei giovani con il proprio computer e con la rete (per esempio per sapere il tempo che essi dedicano all'utilizzo del p.c. e per quali ragioni si connettono ad internet) e molte altre informazioni utili a mettere in luce quale sia la loro idea di etica hacker, di cracker, di crimine informatico o di che cosa voglia dire violare un sistema.

Dai dati raccolti, gli operatori, troverebbero sicuramente quegli elementi necessari per capire se il giovane che utilizza i nuovi strumenti telematici, abbia sviluppato (o se sia in grado di sviluppare) una capacità di interazione sociale o se, nel caso contrario, occorrono mirati e nuovi interventi per ricreare un equilibrio sereno all'interno della propria personalità, in grado di garantire un potenziamento delle capacità di socializzazione o di promozione dell'identità.

Naturalmente perché progetti di questo tipo si realizzino è indispensabile una massiccia attività formativa, e di sensibilizzazione istituzionale.

5.3 Abbandono dell'Hacking

Se si sta parlando di criminalità vera e propria legata all'Hacking, le misure di recupero sopra descritte vanno osservate e applicate in modo che automaticamente venga interrotta (forzatamente) l'attività dell'Hacker. Ci sono anche casi in cui tale attività viene lasciata volontariamente dall'individuo stesso.

Questo avviene, di solito, quando l'*hacker* ritiene che non valga più la pena rischiare, soprattutto perché frustrato e indignato dallo stato attuale del mondo underground, che non rispecchia più i propri valori. Si sta parlando chiaramente di persone non più adolescenti.

La maggior parte di essi in realtà abbandona solo temporaneamente, perché esposta ad un pericolo (ad esempio, sanno di essere controllati dalla polizia), o per riflettere sulla propria situazione personale, riprendendo la loro attività di *hacking* a pericolo scampato.

Alcuni, invece, continuano ad utilizzare le loro capacità nel "settore", lavorando

nel campo della sicurezza informatica, cambiando pelle da *black* a *white-head*, smettendo di combattere l'*establishment* ed entrando a farne parte per sconfiggere i suoi nemici, controllando e "pattugliando" il cyberspazio per il bene della comunità, sebbene ognuno a modo proprio, con regole non scritte.

Con questo processo di trasformazione, queste persone cercano anche di riscattare, in qualche modo, l'immagine negativa che l'opinione pubblica si è fatta degli *hacker*.

Occorre ricordare, infatti, che gli hacker hanno una naturale curiosità nei confronti della *computer security* e in generale nutrono un certo rispetto verso gli esperti del settore. Basti pensare al fatto che le abilità acquisite facendo *hacking* sono le stesse richieste per diventare un esperto di sicurezza informatica.

Intraprendere una carriera nel settore della sicurezza informatica rappresenta non solo un fattore di crescita umana e professionale, ma anche un modo per scaricare sul lavoro la propria ossessione o dipendenza dell'*hacking*.

Quella appena descritta rappresenta una fisiologica evoluzione di molti *hacker* verso l'età adulta.

Non mancano, però, i casi di chi, non avendo una preparazione professionale in materia, fatica a trovare un'attività diversa.

È corretto affermare che gli *hacker* non abbandonano mai del tutto il mondo dell'*hacking,* perché la loro curiosità verso l'informatica e i *network* informatici non muore mai, cambia solo la definizione, il senso che danno di volta in volta alla parola *hacker*.

Conclusioni

Scopo principale di questa tesi è stato quello di analizzare più da vicino il fenomeno dell'hacking, dalle origini alle sue attuali implicazioni sociali e culturali.
Per fare ciò, è stato necessario capire nel dettaglio chi effettivamente possa essere chiamato hacker, questi soggetti pressoché anonimi di cui tanto si sente parlare con riferimento alla criminalità informatica.
E' stato necessario studiarne le origini, i principi, l'etica che condiziona il loro agire e dove quest'ultima esce dal campo della legalità.
Dopo una documentazione sia in campo sociologico che giuridico, nonché grazie all'ormai irrinunciabile ausilio della rete internet, è stato possibile capire le ragioni che inducono a considerare la condotta degli hacker espressione di disagio, che non può essere banalizzata.
Del resto, non si può continuare ad ignorare come lo spazio virtuale, pur non essendo tangibile, faccia tuttavia parte della realtà del nostro tempo, in qualità di luogo in cui le azioni avvengono e in seguito portano conseguenze concrete.
E' in questo modo che la transizione verso la società dell'informazione, dipendente dalla tecnologia informatica, porta con sé nuove metafore e nuovi comportamenti.
"La sfera privata cessa d'essere il palcoscenico dove noi esistiamo come attori poiché siamo divenuti i terminali di reti multiple"(Baudrillard - 1987).
Lo spazio pubblico è così ridotto allo spazio privato della nostra scrivania col computer che crea un nuovo regno semi-pubblico, però ristretto.
Abbiamo ipotizzato che l'identità simbolica dell'hacker crei una controcultura ricca e diversa, comprendente abilità altamente specializzate, reti di scambio di informazione, norme, gerarchie di status, linguaggi e significati simbolici condivisi.
I rischi corsi da chi, come gli hacker, vive ai margini della legalità e tenta di sostituire le definizioni dominanti di comportamento accettabile con nuove alternative, la giocosa parodia della cultura di massa e la sfida all'autorità, costituiscono un'esplorazione dei limiti della tecno-cultura mentre, nel contempo, resistono ai significati legali che controllerebbero tali azioni.

E' per questo che Considerare gli hacker solo come l'ennesima forma di devianza, oscura l'elemento ironico, sovversivo, la "*volontà di potenza*" *Nieztschiana* riflessa

nel loro tentativo di conoscere a fondo la tecnologia sfidando contemporaneamente le forze che la controllano.

Invece di abbracciare la cultura dominante, l'hacker ha creato un'irriducibile cultura alternativa che non può essere compresa se isolata dal contesto di cambiamento sociale, politico ed economico che stiamo sperimentando.

Bibliografia

- . Abrahamsen C., 1960, *The psicology of crime*, Columbia University Press, New York, 1967
- .Bernardi M., *Adolescenza*, Fabbri, San Giuliano Milanese, 1998.
- .Berra M., A. R. Meo, *Informatica Solidale*, Bollati Boringhieri Editori.
- .Berzano L.- Prina F., *Sociologia della devianza*, La Nuova Italia Scientifica, Roma 1995, pp. 9-10.
- .Blos P., 1962, *On Adolescence: a Psychoanalytic Interpretation,* New York: Free Press; in Ladame F., 1987, *La mente adolescente*, Borla, Roma.
- .Capello V., *Essere hacker – sul significato di essere hacker,* in
- www.thepentagon.com/valcap, Copyright © 1999.
- .Castells M., *The information age*, Blackwell, Oxford (UK), 1996.
- .Cohen S., Young J., *Folk devil and moral panics: the creation of moods and rockers*, London: Constable.
- .Contessa G., *Metodologia e tecniche dell'intervento preventivo",* in *Animazione sociale,* n. 47-48, 1982.
- .Cortigiani F., Aspetti psico-sociali della criminalità informatica, in www.thedailybit.net.
- .Erikson E. H., 1982*, The Life Cycle Completed. A Review,* New York,
- .Norton, trad. it. *I cicli della vita*, Armando, Roma, 1984.
- .Fici A., *Mondo hacker e logica dell'azione collettiva*, Ed. Franco Angeli, Milano, 2004.
- .Foucault M., *L'ordre du discourse*, Paris: Gallimard, 1970; trad. It. *L'ordine del discorso. I meccanismi sociali di controllo e di escluzione della parola*, Torino, Einaudi, 1972.
- .Gallino L. (a cura di), "*Dizionario di Sociologia",* Utet, Torino, 1988.
- .Goffman E., *The presentation of self in everyday life*, New York,
- .Oubleday Achor; trad. It. *La vita quotidiana come rappresentazione,* Bologna, Il mulino, 1975.
- .Guerrini F, *Gli hackers come controcultura tra identità e rappresentazione.*

- .Himanen P., *L'etica hacker e lo spirito dell'età dell'informazione,* Feltrinelli, Milano.
- *.La regola di San Benedetto*, XLVIII, Mondadori , Milano, 1995
- .Levy S., *Hacker: eroi della rivoluzione informatica*, Ed. Shake, Milano,1984.
- .Lévy-Strauss C., *La Pensée saubage*, Paris: Plon, 1962; trad. It. *Il pensiero selvaggio*, Milano, Il saggiatore, 1964.
- .Livraghi G., *L'umanita dell'internet.*
- .Maggiolini A., Riva E., *Adolescenti trasgressivi, le azioni devianti e le risposte degli adulti,* Franco/Angeli, 1999.
- .Merton, R., *La struttura normativa della scienza*, in *La sociologia della scienza*, F. Angeli, Milano 1981.
- .Monti A., Chiccarelli S., *Spaghetti hacker,* Apogeo, Milano, 1997,www. spaghettihacker.it.
- .Palmonari A., *Adolescenza,* in S. Bonino, 1994*, Dizionario di Psicologia dello sviluppo*, Einaudi, Torino.
- .Pansa A., *Le strategie di contrasto al crimine informatico*, intervento alla Cybercrime International Conference, Palermo, 3, 4, 5 ottobre 2002.
- .Piaget J., *Dal bambino all'adolescente*, (a cura di), Andreani Dentici
- .O., Gorla G., La Nuova Italia, Firenze,1969.
- .Plant M., 1992, *Risk-takers. Alcohol, drugs, sex and youth,*
- .Routledge, London, New York; trad. it. *Comportamenti a rischio negli adolescenti*, Ed. Centro Studi Erickson, Trento, 1996.
- .Pomante G*, Hacker! Criminali o eroi della rivoluzione informatica* intervento al Convegno "*Information Technology & Law*", Università di Urbino - 20 novembre 2000.
- .Pomante G., *Hacker e computer crimes*, Ed. Simone, Napoli, 2000.
- .Raymond E. S*., How become a hacker* in
- http://virgolamobile.50megs.com/hacker-howto-it.html
- .Raymond E., *The Cathedral and the Bazar* in
- www.apogeonline.com/openpress/doc/cathedral.html
- .Regogliosi L., *La prevenzione del disagio giovanile,* NIS, Roma, 1994.
- .Sola L., Fondaroli D., *A proposito della criminalità informatica*, Cooperativa

Libraria Universitaria Editrice, Bologna, 1992.

- .Sola L., *I computer crimes nell'ordinamento giuridico italiano: alcune considerazioni* in *A proposito della criminalità informatica*, Editrice Clueb, Bologna, 1992, pag 9.
- .Sterling B., *The hacker Crackdown: law and Disorder on the electronic frontier*, 1992; Trad. It. *Giro di vite contro gli hacker,* Milano, Shake Edizioni underground, 1993).
- .Stone A. R., 1995, *The War of Desire and Tecnology, at the Close of the Mechanical Age*; trad. it *Desiderio e tecnologia (il problema dell'identità nell'era di Internet)*, Feltrinelli, Milano, 1997.
- .Strano M, "*Dal cyberfuturismo al cybercrime, la spiegazione del comportamento criminale connesso alla tecnologia digitale",* intervento al convegno internazionale *FUTURNET*, Roma 4,5,6 dicembre 2003.
- .Strano M, *La nuova frontiera del disagio giovanile: l'illegalità sulla rete internet*, in www.poliziadistato.it.
- .Strano M, La *psicologia degli hacker criminology*, in www.criminologia.org.
- .Strano M, *Nuove tecnologie e nuove forme criminali*, intervento al Cybercrime International Conference, Palermo, 3, 4, 5 ottobre 2002.
- .Strano M. et alt., *Applicazione di un assessment criminologico per lo studio di casi: un giovane hackers. Comunicazione al Convegno internazionale*, in *Media digitali e psicotecnologie: viaggi nella mente dei mondi virtuali,* Erice, Villa San Giovanni, 28 giugno-1 luglio 2001.
- .Strano M. et alt., *Aspetti personalogici degli hacker: uno studio clinico: relazione al convegno computer crime,* 27 aprile 2000, Biblioteca del CNEL, Roma.
- .Strano M., *Computer crime: manuale di criminologia informatica*, Ed. Apogeo, Milano, 2000.
- .Strano M., *La nuova frontiera del disagio giovanile: l'illegalità sulla rete internet*, in www.poliziadistato.it.
- .Strano M., *Relazioni digitali e comportamenti devianti,* Relazione al convegno: *Psichiatria, informatica e telemedicina. Realtà e prospettive nel campo dell'assistenza e della formazione*, Velletri, Sala Micara, 29 marzo 2001.
- .Tavassi La Greca Federico, Tesi di laurea in *Hacking e criminalità informatica.*

- .The Mentor, *La coscienza di un hacker*, testo integrale consultabile all'indirizzo www.hacker.com.
- .Vulpiani D*., L'esperienza italiana nel contrasto al crimine informatico,* intervento alla *Cybercrime International Conference,* Palermo, 3, 4, 5 ottobre 2002.
- .Weber M., *L'etica protestante e lo spirito del capitalismo*, Rizzoli.
- .Winkler I., *Corporate espionage*, Hardcore, 1997.