WWW.Criminologia.org
TELEMATIC JOURNAL OF CLINICAL CRIMINOLOGY

Il computer crime nelle aziende e nella Pubblica Amministrazione.

(M Strano[1], ottobre 2002)

introduzione

Nelle aziende private e nella Pubblica Amministrazione sono collocati una grande quantità di computers a cui sono affidate funzioni organizzative e gestionali fondamentali come il controllo di informazioni, di know-how e del denaro. Herbert Edelherz[2] (1977) già alla fine degli anni 70' aveva sottolineato come il rapido sviluppo tecnologico in ambito informatico, creasse un notevole cambiamento nella routine manuale di prendere ordini, registrare entrate o uscite di denaro, immagazzinare o registrare articoli permeando la cultura aziendale. Per tale motivo la maggior parte dei computer crimes viene statisticamente commessa in ambito aziendale. Gli autori di questo genere di crimine, sono quindi in prevalenza i dipendenti di organizzazioni pubbliche e private o i consulenti esterni (specie di informatica).

Solo quindi in alcuni casi, quando l'azione criminale proviene dall'esterno dell'organizzazione, la responsabilità del crimine è dei cosiddetti hackers (professionisti o dilettanti) che acquisiscono, modificano o distruggono le informazioni contenute nella rete aziendale forzandone le difese. Statisticamente però gli attacchi esterni costituiscono una porzione minore dei crimini informatici.

In altri casi, infine, l'autore è rappresentato dal consiglio di amministrazione (o da parte di esso) quando l'azione illegale si riferisce ad una precisa strategia aggressiva nei confronti di un'organizzazione concorrente che tenta di spiare o sabotare un'azienda rivale.

L'avvento della tecnologia digitale e il computer crime

Il processo di diffusione della tecnologia informatica all'interno delle aziende e del sistema sociale in genere sta inducendo dei processi adattivi evidenti su cui si focalizza l'attenzione – in ottica multidimensionale - degli scienziati sociali e tra questi degli studiosi di Cybercriminologia. L'impatto dell'information technology sul sistema sociale è genericamente correlato a tre diverse dimensioni, poste su livelli diversi ma interagenti tra loro.

La prima dimensione è quella sociale, osservabile attraverso le grandi modificazioni culturali e attraverso la produzione di norme specifiche da parte dei sistema-Paesi. La seconda dimensione è quella delle organizzazioni, che trova indicatori nelle modifiche strutturali di tali compagini (es. l'acquisizione di sistemi di sicurezza da parte delle aziende). La terza dimensione è quella individuale, che si riferisce soprattutto alle modifiche cognitive da parte dei singoli attori sociali.

La *dimensione sociale* del computer crime è strettamente legata all'aumento dell'allarme politico-istituzionale e alla sempre maggiore influenza che le grandi imprese acquisiscono nel processo di produzione delle norme che tutelano i loro legittimi interessi. Tutte le nazioni industrializzate e terziarizzate negli ultimi tre decenni hanno infatti prodotto uno specifico corpo normativo riguardante il computer crime e hanno allestito dei reparti specialistici di

[1] Psicologo, specialista in Criminologia clinica applicata al computer crime

[2] H. Edelherz, *The investigation of white-collar crime*, Washington, 1977, cit. in *Computer Technology and Computer Crime* di A. Solarz, 1981, National Council for Crime Prevention (Stockholm).

polizia in grado di investigare su tali illeciti. La questione degli hackers (gli attacchi provenienti dall'esterno delle organizzazioni), soprattutto in termini preventivi sembra essere ad esempio al centro dell'attenzione del Governo degli Stati Uniti. Secondo *John M. Deutch*, direttore della CIA, "*..la guerra dell'informazione è diventata oggetto di interesse primario negli ambienti governativi e l'unica munizione precisa in questo genere di battaglie è l'elettrone*". In altri termini è possibile contrastare eventuali attacchi provenienti dal cyberspazio solamente aumentando la competenza degli specialisti di sicurezza e diminuendo i tempi di risposta in caso di attacco. In tal senso, la creazione del CERT e la sua interconnessione con le strutture investigative e di intelligence rappresenta un fattore significativo. Il CERT *(Computer Emergency Response Team)* è un gruppo di esperti, di stanza in una prestigiosa università statunitense, che opera in maniera indipendente dalle altre agenzie, a stretto contatto di gomito però con l'FBI e con il Secret Service del Dipartimento del Tesoro. Viene finanziato dal Dipartimento della Difesa ed è investito della responsabilità di vigilare sull'intera infrastruttura informatica e telematica della nazione. Tra i suoi compiti c'è anche quello di studiare la sicurezza su internet (e intranet) avvisando gli utenti di eventuali buchi nella sicurezza e di rischi di varia natura e cercando di ridurre i tempi di intervento in caso di hacking.
All'inizio del nuovo millennio le nazioni sviluppate tecnologicamente che hanno registrato un'elevata concentrazione nel cyberspazio di interessi economici ed elevati investimenti da parte di singoli individui e di aziende oltre che lo spazio di interconnessione tra i vari comparti della Pubblica Amministrazione hanno dovuto conseguenzialomente dare corso ad un processo di costruzione di un quadro normativo specifico, attraverso la produzione di norme penali che definiscono la proprietà privata nell'ambito del *cyberspazio.* Le nuove norme del digitale e le relative sanzioni costituiscono di fatto l'elemento primario fondamentale per la definizione di forme criminali nuove e di nuovi autori di crimine. Le ricerche criminologiche condotte sotto questa ottica sono in prevalenza statistico-quantitative, relative ad esempio all'incidenza del fenomeno, al suo numero oscuro, ai costi sociali del computer crime eccetera.

La dimensione relativa alle *organizzazioni* si riferisce alla modifica di dinamiche e di strutture da parte di aziende e Pubblica Amministrazione per prevenire e contrastare azioni illegali poste in essere attraverso la tecnologia informatica. Dal mondo aziendale giungono vari segni di presa di coscienza sugli effettivi rischi e sulla vulnerabilità di un sistema industriale e sociale i cui gangli vitali sono interamente affidati a macchine informatiche[3]. Parallelamente alle richieste di costruzione di un quadro normativo specifico si registra infatti un incremento, da parte delle organizzazioni, degli investimenti nell'area della *security* tecnologica e nella formazione specialistica. Il concetto stesso di sicurezza industriale è rivoluzionato, spostando la sua attenzione progressivamente dallo stato "fisico" a quello "virtuale". Una delle peculiarità dell'era post-industriale d'altra parte è proprio l'aumento di valore delle conoscenze sui processi di produzione (know-how) a scapito dei beni strutturali e finanziari. Nelle aziende moderne i patrimoni di maggior valore che necessitano quindi di assoluta tutela sono costituiti attualmente da informazioni (commerciali, industriali, finanziarie eccetera) che viaggiano solitamente nelle reti di computer o che sono memorizzate in banche-dati aziendali. E' quindi logico che gli sforzi progettuali dell'area *security* siano focalizzati ora sulla prevenzione del computer crime, maggiore potenziale aggressore delle nuove ricchezze. Nel convegno organizzato a Torino (maggio 2000) dall'Associazione industriali di Torino e promosso da Bull, Fiat, Pricewaterhouse Coopers, Politecnico di Torino e Intesis è emerso come molti grandi gruppi italiani hanno scarsamente considerato in passato il fattore sicurezza, ma adesso, forse con un po' di ritardo rispetto all'estero e magari dopo molti danni subiti, stanno diventando molto più attenti. Le richieste di attivazione di sistemi di protezione sono, infatti, in continuo aumento: nel '97 il mercato della sicurezza in Italia ammontava a 11.340 miliardi di lire, mentre nel 2001 dovrebbe toccare i 23.400 miliardi. Le ricerche criminologiche condotte su questa dimensione si riferiscono ad esempio ai cambi di cultura organizzativa o alla maggiore o

[3] tali indicatori sembrano emergere soprattutto dalle grandi società rimanendo in fase di arretratezza le piccole e medie imprese e molti comparti della P.A.

minore propensione, da parte della dirigenza di un'azienda, a denunciare alla magistratura i dipendenti scoperti a commettere un crimine informatico.
La *dimensione individuale* del fenomeno, infine, è soprattutto legata all'impatto dell'informatica sugli schemi cognitivi degli individui che sta inducendo dei processi adattivi e delle alterazioni percettive (anche in ambito criminale). Attualmente le ricerche psicologiche più avanzate sul computer crime si focalizzano infatti sullo studio delle variabili percettive e del comportamento indotte dalla tecnologia digitale, soprattutto quando tale tecnologia media una relazione tra autore di un crimine e vittima4. In alcuni casi le variabili indotte dal mezzo informatico sembrano infatti condizionare a tal punto la dinamica criminale da alterare la percezione che l'individuo ha della gravità del crimine che sta commettendo, delle conseguenze del suo gesto e dei rischi di scoperta e cattura. Altri studi criminologici partono dall'assunto teorico del "*disimpegno morale*" cercando di porre in evidenza come la presenza di un computer all'interno di un'azione criminale possa favorire delle pratiche autogiustificative del comportamento deviante. Alcuni studiosi si concentrano infine sull'impiego del computer come strumento del crimine e sull'aumento dell'efficacia dell'azione criminale. In tale ottica assume un certo significato il maggiore o minore "*indice di professionalità*" degli autori e la necessità di "*pianificazione dell'azione"* che possono rappresentare dei possibili elementi di valutazione nell'analisi generale del caso, sia in termini di *responsabilità penale* e sia per ciò che attiene alla ricerca di profili personologici dei criminali. E' possibile infatti ipotizzare la presenza di taluni tratti di personalità "funzionali" all'esecuzione di un crimine informatico in determinati individui. E' evidente però che tali tratti potrebbero essere riscontrati in soggetti completamente avulsi dal mondo del crimine e non possono quindi rappresentare un fattore discriminante in termini predittivi.

Parallelamente alle definizione delle diverse dimensioni del fenomeno (sociale, organizzativo, individuale), per lo studio criminologico del computer crime aziendale viene assunta in questo saggio una classificazione che contempla due aree, quella della criminalità informatica *intraziendale* (aggressioni provenienti dall'interno dell'organizzazione) e quella della criminalità informatica *interaziendale* (aggressioni provenienti dall'esterno dell'organizzazione).

La criminalità informatica intraziendale
Per criminalità *intraziendale* intendiamo soprattutto le attività illecite poste in essere dagli *insiders*, ovvero dai dipendenti e dirigenti di una azienda e della Pubblica Amministrazione ai danni dell'azienda stessa, sfruttando strumenti e procedure informatiche e telematiche. La Commissione Britannica Audit, scrive Bill O' Neill5, che controlla le finanze del Settore pubblico inglese, ha pubblicato una ricerca in cui si evidenzia che a fronte di 26 miliardi spesi in Gran Bretagna per la sicurezza su internet ogni anno, le frodi informatiche e gli abusi sono in aumento e sembrano diventare più frequenti tanto più l'uso di internet si diffonde. La ricerca, basata sulle risposte fornite da 900 organizzazioni pubbliche e private, aggiorna il rapporto della commissione del '94 denominato "*L'opportunità fa il ladro*". Il settore maggiormente vittima delle frodi e abusi informatici è quello dell'Educazione, con 59% delle organizzazioni che denunciano incidenti, rispetto al 36% della rilevazione precedente. La ricerca pubblica anche 17 casi, dai più gravi ai più ingenui, in diversi settori dell'economia. Complessivamente emergono alcuni dati interessanti:

1. Il 45% delle organizzazioni riporta danni subiti dall'uso illecito di internet nel 1997 (nel 1994 era il 36%);
2. La metà delle organizzazioni pubbliche e un terzo delle aziende private subiscono frodi via internet;
3. L'infezione da virus rappresenta la forma prevalente di abuso

4 In Italia questo genere di studi è attualmente condotto dal Gruppo di Ricerca sul computer crime che opera presso l'Istituto di Psichiatria e Psicologia dell'Università Cattolica del Sacro Cuore e dallo IURC (sito internet www.criminologia.org)
5 The Guardian- 19 Febbraio 1998, "*Esposti all'abuso* " di Bill O' Neill,

4. Il numero delle organizzazioni che riportano incidenti dovuti agli hacker si è triplicato;
5. Personale in posizione manageriale commette almeno un quarto di tutte le frodi;
6. L'accesso ad internet espone maggiormente le organizzazioni al rischio di frodi o abusi;
7. I sistemi telefonici sono i nuovi obiettivi dei criminali informatici;
8. Una organizzazione su quattro ha elaborato delle strategie anti-frode (nel '94, nessuna);
9. Una frode su due è scoperta per caso;
10. La dirigenza più anziana lascia a desiderare per quanto concerne gli interventi tesi ad incrementare la sicurezza delle aziende su Internet;
11. Solo metà di chi ha frodato con il computer, è stato licenziato o denunciato.

Gli studiosi del fenomeno e gli esperti di sicurezza quindi sono giunti alla conclusione che ogni azienda subisce da parte dei suoi impiegati dei furti anche se difficilmente riesce ad individuare gli autori. Le aziende medie o piccole, in virtù della loro organizzazione meno complessa e della maggior facilità nei controlli, sembrano subire meno l'incidenza dei furti dei dipendenti (o sono meno propense alla denuncia), per lo meno nelle statistiche ufficiali. Tali illeciti, infine, sono commessi in ogni settore di lavoro, dagli esercizi di vendita al dettaglio a quelli della grande distribuzione, dagli ospedali alle industrie manifatturiere. Nel maggio del 1999, l'FBI ha individuato ad esempio alcuni scienziati di origine cinese sospettati di spionaggio, impiegati presso i laboratori atomici di Los Alamos, che avevano trasferito dati riservati su computer poco sicuri, accessibili via internet. Gli scienziati in esame hanno affermato di aver effettuato il trasferimento dei dati per poter lavorare da casa sui progetti su cui erano impegnati. L'FBI non è riuscita a reperire sufficienti prove a carico degli interessati ed ha archiviato il caso, pur con notevoli dubbi.
I computer crimes aziendali possono essere *esclusivamente informatici* (consumati esclusivamente mediante un computer) come nel caso di un'intrusione utilizzando una password "indovinata" dall'hacker o *parzialmente informatici*, quando in pratica è necessaria anche un'azione di tipo tradizionale per poter eseguire efficacemente il reato (esempio aprire un cassetto di un collega per acquisire una password utilizzata poi per un accesso illegale). Tale classificazione appare utile poiché nel secondo caso la percezione dei rischi di cattura da parte dell'autore è forse maggiormente assimilabile a forme criminali di tipo tradizionale.
In una ricerca condotta negli Stati Uniti nel 1996 dal WarRoom Research su un campione di aziende, è emerso che il 62,9% di tali società aveva subito un attacco informatico ad opera di un *insider*. La ricerca condotta nel 1998 dal Computer Security Institute insieme all'FBI ha invece dimostrato che il costo medio di un attacco da parte di un *outsider* (hacker) è pari a 56.000 dollari mentre l'attacco condotto da un *insider* ha un costo medio di 2,7 milioni di dollari. Tali stime inducono quindi delle valutazioni sui reali rischi del computer crime aziendale e collocano in posizione primaria le azioni che provengono dall'interno delle società. I reati informatici più diffusi in ambito aziendale (frodi, spionaggio, sabotaggio) vengono effettuati da infatti da coloro che meglio conoscono i sistemi dell'azienda. Attualmente però la maggior parte degli investimenti destinati ai sistemi di sicurezza e alla ricerca scientifica sono orientati verso gli attacchi che provengono dall'esterno delle strutture.
Le ragioni che sottendono ai crimini informatici da parte degli insider sono molteplici. In molti casi, azioni di sabotaggio informatico o di estorsione sono stati commessi da dipendenti desiderosi di vendetta per il loro licenziamento o trasferimento o che ritengono in genere di aver subito dei torti. Talvolta le motivazioni sono legate al semplice desiderio di gratificazione dell'ego o per risolvere problemi di insicurezza psicologica. In altri casi gli autori sono dei dipendenti che vogliono proteggere la loro carriera o trarre vantaggi finanziari sfruttando la loro posizione all'interno dell'azienda[6]. Alcuni studi focalizzati sui profili di personalità ricorrenti negli autori di computer crime "insiders" (soprattutto statunitensi)[7] hanno cercato di offrire

[6] Greenberg J. (1990), "*Employee theft as a reaction to underpayment inequity*", in Journal of applied psychology, dic. Vol 75(6), pp.667.
[7] Parker D. (1976), *"Crime by computer"*, Charles Scribner's Sons, New York, 1976, pp.12; Parker, D. (1998). *Fighting computer crime: A new framework for protecting information*. New York: John Wiley & Sons, Inc.

informazioni utili a migliorare le strategie di prevenzione e di produrre delle metodologie di selezione per l'assunzione degli specialisti di informatica in azienda. In tale ambito una figura su cui si focalizza l'attenzione è ovviamente rappresentata da coloro che progettano e gestiscono dei sistemi informatici vitali all'interno della struttura e che per esigenze gestionali vengono in possesso di dati vitali per l'organizzazione. Le figure professionali che appartengono a tale categoria destano infatti notevoli preoccupazioni essendo in possesso delle competenze necessarie (e delle possibilità di accesso) che permettono loro di procurare i maggiori danni in caso di abuso. Tali professioni comprendono gli amministratori di sistema, i programmatori e gli operatori di rete (definiti in U.S.A. con l'acronimo C.I.T.I *critical information technology insiders*) e necessitano secondo gli esperti di specifiche valutazioni (fedeltà nei confronti dell'azienda e motivazione) nell'ambito delle procedure di selezione per l'assunzione (o per l'assegnazione di contratti di consulenza). Abitualmente, infatti, le valutazioni più rigorose vengono effettuate dall'azienda nei confronti dei dipendenti che saranno inseriti in maniera più o meno stabile nell'organico (full-time o part-time) mentre minore attenzione viene usualmente rivolta a soggetti che hanno rapporti di lavoro con posizione più esterna (es. consulenti, tecnici, manutentori) che rappresentano sovente l'ossatura dei dipendenti C.I.T.I nell'azienda. E' importante considerare che, per quanto riguarda il settore informatico, anche soggetti che operano temporaneamente e marginalmente nella struttura aziendale acquisiscono un grande potere gestionale e possono essere in grado di procurare danni gravissimi in caso di disonestà. Si rileva inoltre un'approssimativa richiesta di informazioni da parte dell'azienda che assume dei consulenti (o dei dipendenti con contratti a termine) con scarsa valutazione di eventuali precedenti, ad esempio di appartenenza a gruppi di hacking, anche per la reticenza di molti imprenditori nel fornire informazioni su loro ex-dipendenti per non rivelare problematiche aziendali riservate.
Tra i crimini che avvengono all'interno delle aziende e che vedono implicati i dipendenti, analizziamo quelli più diffusi:

Furto di tempo macchina da parte dei dipendenti (impiego dei computers per finalità personali): Tali comportamenti, sul piano criminologico, sono assimilabili ad un vero e proprio furto (il furto di tempo macchina) dove la refurtiva non è rappresentata da oggetti tangibili (es. una penna) ma dal tempo di funzionamento del computer sottratto al profitto dell'azienda. La peculiarità di questa forma di illecito è intuitivamente rappresentata dall'enorme diffusione sociale, in special modo per quanto riguarda l'uso di videogames in ufficio, l'utilizzo della videoscrittura per scopi personali e l'invio di e-mail private. La grande diffusione del fenomeno, da un verso riduce la percezione della gravità dell'atto da parte dell'autore e da un altro verso riduce la tendenza a prendere provvedimenti energici (la denuncia penale) da parte della vittima (l'organizzazione). Il danni subiti dall'organizzazione-vittima possono essere di *tipo primario* (in termini di mancato profitto previsto e di usura della macchina non soggetta ad ammortamento) e di *tipo secondario* (es. per l'introduzione di virus a seguito di uso non autorizzato).

Le sanzioni previste sono comunque anche di natura penale (es. per l'appropriazione indebita, per il peculato, per il danneggiamento di sistemi informatici e telematici eccetera) e come tali di interesse del criminologo. La casistica più consistente riguarda in effetti la navigazione su internet, la fruizione di videogiochi o dei programmi di videoscrittura per scopi personali temporalmente limitati. Sono stati però descritti, in tale ambito, casi di soggetti che utilizzavano il sistema elaborazione dati della società dove lavoravano per svolgere vere e proprie attività professionali collaterali (amministrazione di condomini, gestione patrimoniale, copisteria eccetera) talvolta addirittura in concorrenza con l'azienda di appartenenza. L'utilizzo non autorizzato del computer da parte di personale di un'impresa può provocare danni gravissimi, sia in termini di perdita di fatturato e sia per introduzioni accidentali di virus.

Furti o frodi ai danni delle aziende da parte dei dipendenti: Si tratta di azioni illegali che contemplano la somministrazione di istruzioni logiche ai computers aziendali al fine di ottenere dei benefici, attingendo dai capitali e dai beni prodotti dall'impresa. Un sistema adottato per

l'esecuzione di frodi è quello dell'acquisizione di password mediante *masquerading*. Tale sistema implica la ricerca della password di identificazione (con varie tecniche) che consente all'autore del crimine di farsi passare per un altro accedendo a informazioni o alterando il funzionamento di un computer per ottenere un vantaggio. In altri casi vengono utilizzate le tecniche di *piggyback* o di *tailgate* che consistono nello sfruttare l'apertura delle protezioni informatiche o fisiche da parte di un utente autorizzato che sta lavorando al fine di effettuare operazioni illegali "sfruttando la sua scia". Secondo David Shapshak8 in uno studio sul computer crime aziendale in Sudafrica del 1997, le frodi rappresentano il 34% dei casi investigati. Secondo tale studio le frodi informatiche nelle banche spesso sono compiute dal personale interno che sa come sfruttare i buchi già esistenti nei sistemi di sicurezza o al limite attraverso una collusione tra organizzazioni criminali e "insiders". Shapshak riporta anche le parole di David Brink, presidente delegato della ABSA, che afferma che la sua banca subisce in media una rapina al giorno nelle varie filiali del Sud Africa, ma che perde maggiori quantità di denaro a causa delle frodi dei colletti bianchi che penetrano elettronicamente nei conti e sottraggono denaro a loro favore, talvolta con la *tecnica del salame.* La tecnica del salame è una forma automatizzata che sfrutta l'inserimento di un troian horses all'interno di un elaboratore in modo da alterare il funzionamento del software che controlla i conti bancari. Il programma dispone la sottrazione ripetuta di modeste somme dai conti correnti bancari, somme che poi vengono accreditate su un altro conto. E' una forma oramai classica di abuso riscontrata nelle banche e nelle società finanziarie. In pratica l'operazione avviene con l'introduzione di un programma nel computer che fa dirottare delle piccolissime fette di conti e depositi in un conto prestabilito, aggirando i sistemi di sicurezza. Questo genere di crimine viene normalmente prevenuto con specifici software e con controlli mirati ciclici. In altri casi, infine, le frodi vengono effettuate attraverso il *false data entry* che implica l'inserimento di informazioni alterate nell'elaboratore.

Danneggiamenti dolosi dei sistemi: Queste azioni, ad opera di dipendenti, assumono notevole gravità a causa dell'alta concentrazione dei dati all'interno dei computers delle imprese moderne e in taluni casi possono mettere in crisi la sopravvivenza dell'impresa stessa, in special modo quando la quantità di procedure affidate al sistema informatico risulta molto elevata. I danneggiamenti possono avvenire sia con agenti fisici (incendi, acidi, magneti, rotture meccaniche ecc.) sull'hardware e sia con metodiche informatiche, attraverso ad esempio l'introduzione di virus e worm (programmi logici distruttivi) che danneggiano il software e producono perdita di dati. Dietro a tali azioni criminali spesso si celano dipendenti scontenti o consulenti informatici in contrasto con l'azienda e possono attivarsi anche dopo molto tempo che l'autore non è più fisicamente presente all'interno dell'organizzazione (la famosa time bomb);

Furto di informazioni: Si tratta di azioni, condotte dai dipendenti di vario livello, che acquisiscono informazioni di valore di proprietà dell'azienda dove lavorano (know-how, marketing, commercio, ricerca e sviluppo) e poi tentano di venderle alla concorrenza o cercano di porre in essere veri e propri ricatti al datore di lavoro. Il vero danno economico causato dal computer crime viene commesso dagli "insiders" che hanno già accesso alla rete, non dagli hackers che tentano di dimostrare la loro prodezza tecnica, ammoniscono gli esperti informatici. La maggior parte del crimine informatico infatti, non è ad opera di organizzazioni esterne dedite a loschi traffici, ma a impiegati scontenti e disonesti.
Possiamo ipotizzare in tal senso due dinamiche correlate a diversi profili criminologici dell'autore: nella prima l'*insider*, ad esempio in fase di conflittualità con l'azienda, opera attivamente per acquisire informazioni sensibili e ricerca un possibile acquirente esterno. Nella seconda dinamica l'*insider* viene casualmente in possesso di informazioni sensibili in virtù della sua collocazione all'interno dell'azienda (special opportunity crime) e decide di tentare una vendita alla concorrenza.

8 The Mail And Guardian, articolo di David Shapshak 18 Febbraio 1998

Nei casi di spionaggio informatico la tendenza è comunque quella di attribuire la responsabilità di queste azioni ad hacker esterni, motivati da sentimenti di sfida tecnica ed intellettuale, da scopi di lucro o da intenti vandalici[9]. In realtà, come sottolinea lo specialista di informatica statunitense David Breiner, il movente più comune è la vendetta o la bramosia di guadagno dei dipendenti scontenti. Un esperto di sicurezza della società Ernst and Young conferma a tal proposito che statisticamente circa l'80% dei rischi per la sicurezza informatica proviene dall'interno dell'azienda.

Estorsioni. Sono stati segnalati alcuni tentativi, in tutto il mondo, di dipendenti a cui era stata affidata una funzione informatica vitale nell'ambito dell'azienda, che hanno poi tentato di ottenere delle somme di denaro o vantaggi di carriera minacciando di rendere inutilizzabili le procedure o i dati da loro gestiti nell'ambito dell'organizzazione. Tale crimine assume particolare significato nelle organizzazioni che hanno totalmente informatizzato alcune procedure.

Una caratteristica di tutte le manifestazioni del computer crime *intraziendale* sopra descritte è infine rappresentata dall'alto numero oscuro che lo contraddistingue. In un convegno organizzato a Torino dall'associazione industriali è emerso ad esempio che nel 1997 il 75% di un campione di 563 società connesse a internet ha riportato danni economici a causa di intrusioni informatiche e che circa l'80% dei crimini non è stato scoperto. La situazione sembra comunque essere orientata verso una maggior presa di coscienza da parte delle aziende. Secondo il Computer Security Institute di San Francisco le denunce per effrazioni informatiche in USA, che nel 1997 riguardavano il 16% degli utenti aziendali, sono balzate ora al 64% alla fine degli anni 90'.

Una casistica di computer crime intraziendale
Riportiamo a titolo esemplificativo alcuni casi riscontrati nel corso della ricerca o tratti dalla letteratura scientifica internazionale in cui gli autori, sfruttando la loro collocazione nell'ambito dell'azienda, tentano (per vari motivi) di estorcere dei benefici:
CASO 1: Un professionista dei sistemi informatici che opera in una struttura militare in USA apprende che sta per essere declassato nel suo ufficio. Decide allora di criptare un gran numero di dati dell'organizzazione, rendendoli temporaneamente illeggibili e di trattenerli in ostaggio. Si mette in contatto con l'amministratore di sistema responsabile dei data base, offrendogli di decodificarli per 10.000 dollari (da inserire nella sua liquidazione). L'azienda non accetta il ricatto e il professionista viene licenziato con l'accordo di non procedere ad alcun intervento legale. La motivazione del crimine è probabilmente correlata alla bassa tolleranza alla frustrazione da parte dell'autore.
CASO 2: Un ingegnere che lavora presso un impianto di trasformazione dell'energia entra in conflitto con il nuovo supervisore (un amministrativo che non capisce molto di tecnologia). La moglie dell'ingegnere è una malata terminale e le cure necessarie stanno mettendo in crisi finanziaria la famiglia. Dopo aver creato difficoltà sul luogo di lavoro, anche per problemi psicologici dovuti alla situazione clinica della moglie, il professionista viene messo "in prova". Dopo un certo periodo viene licenziato e lo staff tecnico dell'azienda scopre (a distanza di tempo) che il professionista ha effettuato delle modifiche ai sistemi informatici di controllo degli impianti. In pratica ha sostituito le parole di accesso rendendo impossibile la manutenzione della struttura. L'ingegnere viene interrogato dallo staff tecnico su queste modifiche sospette (che minaccia anche un intervento dell'FBI) ma decide di non rivelare le password delle procedure modificate. L'azienda è costretta a chiamare dei consulenti per riprogettare il sistema informatico di controllo dell'impianto. La motivazione del crimine sembra essere soprattutto legata in questo caso al sentimento di vendetta nei confronti dell'azienda

[9] Gertz Bill, *Spies use Internet to build files on U.S.*, in *Washington Times*, january 3, 1997. Flanagan William G. and Gutner Toddi, *The perils of voice mail*, in *Forbes*, january 17,1994, pp.106-107. Young Jeffrey, *Pay to hack your own system?*, in *Forbes Asap*, june 3, 1996, p.80. Young Jeffrey: *Spies like us*, in *Forbes Asap*, june 3, 1996, pp. 71-92.

visto che il professionista non tenta di essere riassunto. La situazione clinica della moglie potrebbe aver influito sul piano emotivo esasperando ulteriormente l'autore.
CASO 3: Un professionista con un contratto a termine si occupa della gestione informatica della rete telefonica interna di una grossa compagnia internazionale del settore energetico. Il professionista (ex-membro di un gruppo di hackers) sta per essere licenziato per negligenza e pigrizia sul lavoro. Anche se è assunto con un contratto a termine detiene una posizione di potere enorme nell'ambito della struttura e ne è consapevole. E' anche cosciente di non aver difficoltà a trovare un altro lavoro, magari di maggior prestigio. Decide di alterare i programmi di gestione della rete telefonica e acquisisce tutte le informazioni necessarie ad inserirsi clandestinamente anche quando non lavorerà più per la compagnia. L'azienda, che si rende conto dell'operazione avvenuta deve riorganizzare interamente le protezioni della sua rete telefonica, non più sicura, spendendo una considerevole cifra. La motivazione del crimine è legata soprattutto a sentimenti di vendetta nei confronti dell'azienda. Il passato di ex-hacker potrebbe aver influito sulla condotta criminale dell'autore, soprattutto per quanto riguarda la dimensione di "sfida" nei confronti dell'azienda e la pianificazione di un ingresso clandestino a distanza di tempo.
CASO 4: Un anziano programmatore appartenente al M.I.S (management information systems) di un'azienda statunitense che sviluppa un programma missilistico (la General Dynamics) si sente poco apprezzato per il suo lavoro all'interno della compagnia. Il programmatore inserisce allora una "logic bomb" nel sistema informatico, progettata per cancellare i dati dopo un certo periodo di tempo dal suo licenziamento (chiesto dall'autore del crimine). In un secondo tempo il programmatore si offre di rientrare nell'azienda per risistemare il sistema informatico e recuperare i dati cancellati. Chiede di essere assunto con un livello gerarchico superiore al precedente e con un maggiore compenso economico. Secondo i resoconti investigativi l'autore dell'estorsione dichiara una motivazione non legata all'esigenza di sopravvivenza economica (è lui che si licenzia) ma esclusivamente legata alla voglia di maggior gratificazione della sua professionalità.
CASO 5: Un manager impiegato in una catena di supermercati si trova improvvisamente in difficoltà economica a causa della separazione dalla moglie e della conseguente necessità di corrispondere grosse cifre per gli alimenti. Dopo un certo periodo organizza ed esegue una complessa frode informatica coinvolgendo tre impiegati che lavorano all'interno di supermercati della catena. La frode è costata all'azienda oltre due milioni di dollari in due anni. Tra le strategie utilizzate per l'esecuzione del crimine si rileva in questo caso la manipolazione del programma che gestisce la contabilità al fine di veicolare alcune somme su un conto fittizio. Al termine della giornata i complici dell'organizzatore prelevano somme in contanti dai vari registratori di cassa mentre il manager si occupa di cancellare le tracce informatiche di tali somme agendo dal sistema centrale. Secondo i resoconti investigativi la motivazione iniziale del crimine è soprattutto da ricercare nelle difficoltà finanziarie del manager. In seguito però, si affacciano la cupidigia e l'esaltazione dell'ego.

La criminalità informatica interaziendale

La criminalità *interaziendale* informatica si riferisce soprattutto ad azioni illegali, organizzate e pianificate, poste in essere da individui esterni all'organizzazione o da aziende rivali. Tali azioni possono riferirsi all'acquisizione, tramite intrusione telematica, di informazioni riservate a fini di *spionaggio industriale*, ad operazioni di *sabotaggio* finalizzato alla riduzione di efficacia (o alla paralisi) dell'azienda concorrente, alla realizzazione di *truffe via internet sui titoli di borsa* o, infine, al *cyberterrorismo*[10].
Per quanto riguarda lo *spionaggio industriale* si registrano in tutto il mondo sempre più casi di società che cercano di acquisire pacchetti informativi utilizzando sistemi illegali per potersi mettere alla pari di aziende rivali più avanzate riducendo i costi destinati ai settori di ricerca e sviluppo aziendali.

[10] Gattiker, U., & Kelley, H. (1997). *Techno-crime and terror against tomorrow's organization: What about cyberpunks*?

Una società di telecomunicazioni potrebbe ad esempio incaricare i suoi ingegneri (o una ditta esterna di consulenza) di progettare un sistema informatico maggiormente efficace di gestione del traffico telefonico UMTS o WAP da offrire ai propri clienti. Una società concorrente che acquisisse illegalmente tale programma otterrebbe sia il guadagno relativo al risparmio dello studio del programma e sia un vantaggio in termini di marketing strategico potendo conoscere in anticipo le mosse commerciali dell'avversario.
Lo spionaggio industriale telematico può essere effettuato attraverso varie metodiche. Tra i sistemi descritti troviamo lo *scavenging* (rovistare nella spazzatura), l'*eavesdropping* (intercettazione di dati o di radiofrequenze), lo *spying* (la generica acquisizione di informazioni con varie modalità). Lo *scavenging* è un metodo per ottenere o riutilizzare le informazioni che rimangono in circolazione dopo l'attività di elaborazione dati da parte di un computer. Tale tecnica si riferisce sia alle informazioni su carta (es. tabulati, copie nei cestini della spazzatuta), sia alle informazioni ancora presenti nella memoria del computer (es. nella memoria buffer o copie dati backup di lavoro) dopo che è stato eseguito un lavoro. Per quanto riguarda lo *scavenging* fisico uno dei punti critici dell'azienda è rappresentato dal normale circuito di smaltimento dei rifiuti aziendali (contenitori, sacchi eccetera) che rappresentano un obiettivo allettante per eventuali malintenzionati.
Il fenomeno dell'intercettazione di dati sembra essere in grande espansione secondo quanto segnalato dagli esperti della sicurezza. La scoperta di tale fenomeno, oltretutto, risulta essere particolarmente difficile e sovente non viene denunciata. L'autore di *eavesdropping* non sa però in quale momento i dati di cui lui ha bisogno vengono trasmessi dal sistema che sta controllando per cui è costretto a ad acquisire una grande quantità di informazioni (nel cui ambito poi selezionare quelle utili) protraendo così i tempi operativi e il rischio di essere scoperto. Alcune di queste intercettazioni sono denominate *Wave catcher* (acchiappa onde) che è una forma di parassitismo elettronico mediante intercettazione di radiazioni emanate dall'elaboratore che, come tutte le apparecchiature elettroniche, propaga segnali via etere compatibili e decodificabili da altri elaboratori non collegati. Tale metodo allo stato attuale presenta una scarsissima casistica e sembra essere, apparentemente, ad esclusivo appannaggio dei servizi di intelligence governativi o di gruppi di professionisti in possesso di strumentazioni e competenze sofisticate. L'apparecchiatura necessaria è oltretutto molto complessa e costosa e l'operazione, tranne in casi di computer isolati, presenta difficoltà di localizzazione dei dati sensibili da acquisire. Talvolta l'acquisizione di dati avviene attraverso l'installazione di trasmittenti clandestine sul computer collegate ad un apposito ricevitore. Tali strumenti necessitano però una manomissione del computer e la possibilità di avvicinamento "fisico" nel luogo dove è situato l'elaboratore da spiare. Gli enti governativi e alcune aziende attuano una prevenzione a questo tipo di intercettazione collocando i computer che contengono dati sensibili all'interno di speciali ambienti schermati da *gabbie di faraday* e da pareti in fibra di carbonio che limitano l'emissione all'esterno di radiofrequenze. Talvolta, per i dati particolarmente sensibili, vengono adottati sistemi informatici dedicati a bassa emissione di onde e il software viene trattato con programmi crittografici. Esistono anche degli appositi software in grado di indicare eventuali acquisizioni di dati dall'esterno. Gli autori tipici delle varie forme di *eavesdropping* che sfruttano tecnologie sofisticate sono quindi intuitivamente rappresentati da specialisti delle telecomunicazioni, mentre per le tecniche più semplici è possibile anche l'azione di soggetti con modeste competenze informatiche.
L'attuazione di operazioni di *spying* da parte di un'azienda implica spesso il coinvolgimento di parte o dell'intera dirigenza che deve ingaggiare un professionista in grado di portare avanti l'azione illegale. Possiamo ipotizzare in tal senso due diverse situazioni: nella prima l'azienda sleale ingaggia un hacker professionista che tenta di penetrare nel sistema della concorrenza o che tenta di contattare un *insider*. Nella seconda situazione l'azienda sleale tenta di contattare direttamente un insider cercando magari di assumerlo tra i suoi dirigenti.
Il fenomeno del furto di segreti commerciali delle aziende sembra essere dilagante in tutto il mondo. La tecnologia informatica, che tende alla concentrazione di una grande quantità di dati in un ridotto spazio fisico, sembra del resto favorire alcune di queste attività illegali. Un altro punto di vulnerabilità è poi rappresentato dall'esigenza di circolazione e fruizione delle

informazioni archiviate all'interno dell'organizzazione e tale circostanza riduce implicitamente le possibilità di difesa.
Una casistica rilevante è anche relativa al furto di computer portatili in uso a manager e dirigenti di azienda anche se tali azioni sono solo marginalmente legate al computer crime essendo consumate interamente in ambiente fisico. "*L'onnipresente laptop-computer è un obiettivo allettante..".*, dice Richard Heffernan, presidente della R.J. Heffernan, a Brandford, Conn. Cita a tal proposito le statistiche delle assicurazioni industriali del 1995 che dimostrano che un laptop su 14 viene rubato, principalmente a causa dei dati che contiene. "*E' meno rischioso rubare un laptop che violare la proprietà della società*", dice. E fornisce qualche avvertimento: "*mettete il vostro laptop in valigette anonime, usate mezzi di archiviazione estraibili (CD drive su cui si può leggere/scrivere, per esempio) portate dischetti e drive addosso e agganciate il computer alla scrivania o al sedile dell'aereo quando lo lasciate momentaneamente*"11.
Un altro punto critico dell'organizzazione aziendale è rappresentato dai sistemi di comunicazione interni e dalle caselle vocali di posta. Si sono infatti registrati numerosi casi di hacker che si introducono nei sistemi di posta vocale, sistemi computerizzati di raccolta e smistamento dei messaggi vocali. Gli intrusi possono cancellare messaggi legittimi, spiarli o molestare l'utente con messaggi osceni, possono eseguire scherzi. A volte possono addirittura escludere gli utenti autorizzati o bloccare completamente il sistema. Alcune ditte utilizzano infatti un sistema di caselle vocali digitalizzate e governate da computer dove i dipendenti lasciano messaggi attinenti a questioni di lavoro. La penetrazione all'interno di tali sistemi consente così, sovente, di acquisire informazioni, commerciali e gestionali, che possono rivelarsi utili alla concorrenza e tali intrusioni possono di conseguenza essere commissionate a hacker risoluti.
Secondo una ricerca dell'ASIS (una società statunitense specializzata nella sicurezza industriale) su un campione di 325 aziende USA, il numero dei casi di spionaggio industriale per via informatica ha avuto un incremento da 10 a 32 al mese nel periodo 1992-1995 (più del 30% di aumento in tre anni).
Ulteriore importante manifestazione della criminalità interaziendale è costituito dai *sabotaggi di sistemi informatici* della concorrenza. In questi casi i computers delle aziende rivali vengono violati con mezzi telematici o fisici per ridurre o neutralizzare la loro efficacia, auspicando che questa azione possa influire sull'attività della stessa azienda. Il sabotaggio con tecniche telematiche vede spesso l'utilizzo di troian horses, ovvero di programmi che vengono inseriti all'interno del software alterandolo e provocando malfunzionamenti o cancellazione di dati. Talvolta tali programmi entrano in azione a distanza di tempo (in un momento programmato) rendendo difficile la localizzazione dell'autore. Spesso per questo genere di crimini è necessaria la collaborazione di qualche dipendente dell'azienda vittima.
Sono stati segnalati, ad esempio, casi di cracking di siti web di società commerciali o di alterazione dei messaggi pubblicitari da essi veicolati. Talvolta il sabotaggio è stato effettuato mediante la spedizione per posta di dischetti contenenti virus o attraverso l'inserimento di *worm* per via telematica, utilizzando email infette.

Le truffe via internet sui titoli di borsa meritano una trattazione a parte. Possono essere attuate attraverso la manipolazione di informazioni riguardanti le aziende con la finalità di ottenere variazioni di mercato azionario. Tali azioni, classificabili come truffe telematiche, si basano sulla diffusione di false notizie soprattutto su compagnie dalla bassa capitalizzazione di mercato provocando sbalzi artificiosi della valutazione dei loro titoli. I truffatori rastrellano grandi quantità di azioni nella breve fase temporale in cui il titolo si abbassa a seguito della manipolazione. Da queste operazioni, ovviamente, vengono danneggiati migliaia di risparmiatori e l'azienda che subisce per un certo intervallo temporale il crollo delle sue azioni.
Interessante il recente caso di Mark Jacob, uno studente 23enne che e' stato arrestato dall'FBI a Los Angeles, in quanto ritenuto il responsabile di un falso comunicato stampa che ha fatto crollare in Borsa il titolo della società californiana Emulex specializzata nella produzione di fibre

11 DeYOUNG H. G., *Among us*, in Industry Week, june 17, 1996, pp.13-16.

ottiche (annunciando uno stato di crisi societaria). In un quarto d'ora il titolo dell'Emulex è crollato del 65 per cento. L'autore della truffa era impiegato del sito Internet Wire che ha pubblicato il comunicato fasullo. Ha ottenuto 250mila dollari dal suo crimine rastrellando le azioni mentre erano calate di valore. Per eseguire la truffa ha pianificato accuratamente la sua azione operando da un computer "neutrale" collocato nel suo college di El Camino in California. Mark Jacob è stato però scoperto dopo solo una settimana dall'FBI ed è stato accusato di *distruzione dell'integrità del mercato azionario e truffa aggravata*.
A seguito di tale eclatante e allarmate crimine la *Securities and Exchange Commission* (Sec), l'autorità che vigila sulle attività di Borsa, ha intensificato i controlli specifici e ha presentato numerose denunce contro individui ed aziende ritenuti colpevoli di truffe ai danni degli investitori realizzate via internet per un totale di 10 milioni di dollari (oltre 22 miliardi di lire) sottolineando come con l'avvento della rete le operazioni di borsa non sono più di esclusivo appannaggio degli operatori ed intermediari finanziari professionisti ma, di fatto, alla portata di qualsiasi utente dotato di modem e computer. Tale condizione di fatto aumenta i rischi di truffe ai danni di risparmiatori e costituisce dei possibili "fattori di perdita" elevatissimi per le aziende[12]. Ovviamente è possibile ipotizzare che un'operazione di manipolazione informativa possa essere progettata ed eseguita anche da aziende concorrenti in particolari fasi del mercato (acquisizioni, fusioni, scalate eccetera) che potrebbero minare la credibilità dell'azienda rivale agli occhi degli investitori o ridurre il suo prezzo di acquisto.

Il cyberterrorismo costituisce l'ultima possibile forma di aggressione alle organizzazioni. Le aziende e la Pubblica amministrazione delle nazioni maggiormente sviluppate, hanno strutturato le loro funzioni vitali attraverso la creazione di sofisticate forme di immagazzinamento elettronico dei dati (dipendendo quindi dal successivo recupero, analisi, e trasmissione di tali dati) e attraverso la trasmissione dell'informazione mediante canali telematici[13]. Le loro attività vitali possono quindi esplicitarsi solo grazie alla tecnologia digitale e alle reti di computer. In tal senso il loro sabotaggio da parte di un terrorista potrebbe porre in poche ore l'intera organizzazione in condizione di non funzionare. Una moderna azienda di telecomunicazioni può ad esempio essere considerata da un gruppo terroristico come uno dei gangli della nuova economia e quindi un possibile obiettivo ai cui danni eseguire varie azioni tattiche:

- sabotaggio di sistemi fisici e logici (ripetitori, centrali, elaboratori, cavi sotterranei) per ridurre l'efficacia delle comunicazioni e generare panico;
- sabotaggio logico di sistemi informatici mediante istruzioni logiche e introduzione di virus per ridurre l'efficacia delle comunicazioni e generare panico;
- acquisizione di informazioni riservate dagli archivi informatici per localizzare soggetti e strutture;
- utilizzo abusivo dei sistemi di telecomunicazione per veicolare notizie false destabilizzanti.

Gli hackers

Pur se come si è visto la maggior parte dei crimini informatici aziendali sono eseguiti dagli insiders, trattando le manifestazioni di computer crime appare necessario soffermarsi sulle attività e sulle varie figure di hacker. Il verbo to hack assume numerosi significati. La letteratura internazionale sul computer crime riporta infatti più di 20.000 definizioni del termine hacker a dimostrazione che su tale figura esistono svariati atteggiamenti e connotazioni, più o meno criminali[14]. L'hacker è ritenuto talvolta un utente del computer che passa molto tempo sul sistema in un rapporto quasi feticistico. Altre volte il termine è riferito a qualcuno che conosce molto sui computer, anche se non è un programmatore. Per alcuni

[12] notizia di agenzia ANSA - NEW YORK, 31 AGO –
[13] Schwartau, W. (1994). *Information Warfare*. New York: Thunder Mouth Press; Shaw, E., Post, J., & Ruby, K. (1998). *Information terrorism and the dangerous insider*, Meeting of InfowarCon'98, Washington, DC.
[14] Strano M., Kertesz C., L'Occaso C. M., di Giannantonio M., De Risio S., *Aspetti personologici degli hackers: uno studio clinico*, Relazione al Convegno "Computer crime", 27 aprile 2000, Biblioteca del CNEL, Roma.

l'hacker è semplicemente un appassionato di computer che usa le sue abilità in maniera illegale in qualsiasi maniera, normalmente per entrare (bucare) in un altro sistema attraverso una rete. L'*Hacker malicious* detto anche Cracker (per distinguerlo dagli hacker che aggirano le protezioni senza provocare danni consapevoli), è normalmente ritenuto chi usa la sua particolare abilità nel manipolare programmi e sistemi per fini nefasti come formattare dischi, fare saltare (crashare) server di rete, inserire virus. Il termine hacker può anche essere attribuito però alla volontà di rendere disponibili per tutti le risorse della tecnologia telematica assumendo così significato politico e riferendosi in special modo a una tipologia di soggetti libertari e trasgressivi che fanno dell'hacking una sorta di battaglia etica. [15]

L'allarme sociale per tali soggetti sembra comunque diffondersi in tutti i Paesi terziarizzati, soprattutto dove la telematica ha una tremenda influenza sociale[16]. Gli hacker hanno infatti il grande potere di alterare delle funzioni sociali vitali in modo assolutamente imprevedibile e questo potere rappresenta motivo di grande allarme sociale, come sottolineato dalla nascita e potenziamento in tutto il mondo di strutture governative deputate alla prevenzione ed al contrasto delle intrusioni telematiche[17].

Tra i settori di studio della Cybercriminologia quello dell'hacking risulta essere particolarmente attuale e denso di controversie. Le intrusioni clandestine nei sistemi telematici sembrano infatti avere molteplici motivazioni, da quelle più ludiche a quelle maggiormente vandaliche[18] per giungere a vere e proprie operazioni professionali di intrusione o sabotaggio finalizzato alla concorrenza sleale. Presumibilmente i profili personologici, motivazionali e percettivi degli autori di tali crimini varieranno notevolmente in base al tipo di intrusione e non sembra quindi scientificamente corretto affrontare il fenomeno parlando genericamente di hackers. Dietro all'esecuzione di un accesso illegale troveremo infatti una tipologia di autori notevolmente variegata dal punto di vista psicologico che necessita di approfondite tassonomie, ricerche e comparazioni criminologiche sfruttando teorizzazioni nuove.

Secondo Marc Rogers (University of Manitoba)[19], ad esempio, le classiche teorie criminologiche di matrice psicodinamica sono efficaci per spiegare i crimini che derivano da conflitti inconsci ma poco si adattano a quei crimini che viceversa necessitano di accurata pianificazione e soddisfano finalità razionali, come in molti casi di computer crime. Effettivamente il fenomeno dell'hacking risulta di difficile interpretazione utilizzando le teorie criminologiche classiche, soprattutto per le notevoli differenze riscontrabili nel suo ambito già con un'osservazione superficiale. Si evidenzia insomma la necessità, da parte della comunità scientifica, di definire preliminarmente un'idonea tassonomia rispetto a tale fenomeno che contempli sottogruppi verosimili e che proponga una tipologia di base su cui costruire indagini esplorative e profili di personalità, anche di natura comparativa. Dalle prime ricerche "sul campo" si evidenziano infatti differenze motivazionali e caratteriali in categorie di soggetti che hanno in comune talvolta la sola competenza necessaria per l'applicazione di tecniche per l'esecuzione del crimine.

Alcuni studi clinici hanno ad esempio evidenziato l'esistenza di soggetti che considerano l'hacking principalmente un vezzo o un gioco e un sistema per dimostrare a sé e agli altri la perizia acquisita in campo informatico. Altri soggetti, viceversa, eseguono attività di hacking professionale (es. spionistico o aziendale) evidenziando profili criminologici completamente diversi. La motivazione di questo genere di azioni illegali è così talvolta comparabile, nel primo caso, con quella di certe forme di violenza contro le cose e contro le persone, apparentemente

---

[15] Spafford, E. (1997). *Are hacker break-ins ethical*? In, Ermann, Williams, & Shauf, (Eds.) Computers, Ethics, and Society. (pp. 77-88). New York: Oxford.

[16] Chandler, A. (1996). *The changing definition and image of hackers in popular discourse*. International Journal of the Sociology of Law, 24, 229-251. Chantler, N. (1996). *Profile of a computer hacker*. Florida: Infowar.

[17] Littman, J. (1995). *The fugitive game: online with kevin mitnick*. Toronto: Little Brown & Company. Littman, J. (1997). *The Watchman: The twisted life and crimes of serial hacker kevin poulsen*. Toronto: Little Brown & Company.

[18] Hafner, K. & Markoff, J. (1995). *Cyberpunks: Outlaws and hackers on the computer frontier*. Toronto: Simon and Schuster

[19] Rogers, M. (1999). *Psychology of hackers: Steps toward a new taxonomy*. Rogers, M.A. Modern-day Robin Hood or Moral Disengagement, Understanding the Justification for Criminal Computer Activity DAILY MAIL & GUARDIAN 10 February 1999

senza un vantaggio pragmatico per l'autore (es. danneggiamenti di pubbliche infrastrutture) ma spiegabili nella valenza comunicativa che tali azioni implicano, sia diretta verso l'ambiente esterno e sia diretta verso il sé dell'autore: danneggio il sistema informatico per mostrare/mostrarmi che sono in grado di farlo e per aumentare il livello di autostima. Nel secondo caso le categorie di interpretazione criminologia sembrano essere maggiormente attigue a quelle utilizzate per spiegare i delitti professionali laddove la dimensione pragmatico-utilitaristica assume valenza primaria.
Attualmente, secondo quanto evidenziato dai pochi studi criminologici disponibili, sembra infatti ipotizzabile la possibilità che l'hacking possa rappresentare uno strumento per alcuni giovani per entrare in comunicazione con il mondo degli adulti "a livello paritetico" attraverso il canale criminale, costringendo la società a difendere i propri gangli vitali da coloro che, non essendo ancora direttamente implicati nei processi produttivi, vengono usualmente trattati con "sufficienza". L'essere considerati importanti (anche se in ambito illegale) potrebbe così costituire un elemento affascinante per alcuni soggetti con tratti di personalità particolari ed inseriti in una rete di interazioni subculturali con altri soggetti che, per così dire, condividono e rinforzano tale attività. In generale, una subcultura deviante contempla diverse definizioni di ciò che è lecito rispetto alla cultura dominante. La produzione di subculture devianti, nel mondo digitale, può divenire però svincolata dal luogo fisico delle gangs di strada e dai contatti face to face, allontanandosi anche da questioni di gerarchia sociale, mettendo rapidamente in crisi il paradigma di indagine scientifica tradizionale oltre che le usuali strategie di controllo e prevenzione da parte degli organi istituzionali. La teoria subculturale offre spunti interpretativi soprattutto per le dinamiche di apprendimento e rinforzo legate al codice morale diffuso. Nonostante gli hackers si autodefiniscano come soggetti che amano operare in solitudine, dal loro comportamento emergono altresì delle contraddizioni in tal senso. Spesso, infatti, sembra emergere invece una ricerca della gruppalità, espressa in forma atipica e riconducibile a una rete di cyberinterazioni. Essi tendono ad associarsi con soggetti simili, che svolgono le medesime azioni, spesso solo attraverso la rete, alcune volte anche in contatti face-to-face nell'ambito di club o di specifiche *convention*. Questa situazione suggerisce l'elevato livello di apprendimento, circolazione di informazioni e scambio di tecniche all'interno di tali comunità, centrate evidentemente sul possesso di competenze (e spesso sulla competitività) e su uno specifico universo morale e simbolico.
Osservando la situazione da parte della vittima (l'azienda) la differenziazione nel mondo dell'hacking può assumere relativa importanza poiché i danni scaturiti da intrusioni (o infestazioni con virus) di origine "ludica" sono in grado talvolta di provocare dei danni ingenti quanto quelle di origine "professionale".
Gli hacker vengono anche assunti da alcune aziende che si occupano di sicurezza informatica per mettere alla prova le loro ultime misure di sicurezza. Altre volte ex-hackers, abbandonata oramai l'adolescenza e bisognosi anch'essi di lavorare, allestiscono vere e proprie società di consulenza informatica grazie alle competenze acquisite durante il periodo "selvaggio". Sull'assunzione di ex-hacker da parte delle aziende sono in corso parecchie dispute, in special modo sulla reale affidabilità a lungo termine di tali soggetti e sulla rapida obsolescenza delle loro conoscenze una volta abbandonato il mondo dell'hacking attivo. Interessante a tal proposito il caso di *Redattack*, che ha violato numerosi siti internet in Belgio. Il suo scopo dichiarato era quello di dimostrare quanto siano vulnerabili i meccanismi di sicurezza che dovrebbero proteggere internet, lanciando una campagna volta ad alzare gli standard di sicurezza. Recentemente l'hacker si è introdotto nel sito internet dell'agenzia di stampa "BELGA" lasciando un messaggio che auspicava la creazione di un'associazione tra i pirati informatici di tutto il mondo e gli operatori della sicurezza finalizzata a ridurre i "buchi" nella rete delle reti. L'hacker, che afferma di appartenere all'RHF (redattack hackers foundation) auspica anche un impegno comune nella repressione del fenomeno pedofilia su internet20.
In effetti molti giovani hackers ricevono dei rinforzi, spesso ipocriti, alla loro attività illegale. Un possibile rinforzo alla condizione di hacker è rappresentato ad esempio dal "mito dell'hacking invincibile", descritto spesso dai media che contribuiscono così ad amplificarne le gesta.

20 agenzia ANSA, 15/8/99.

Rinforzi possono anche giungere dalla possibilità (in realtà modesta) di essere assunti da aziende nel settore della security. Ulteriore illusione può giungere dalla considerazione e dalla legittimazione espressa da agenzie governative nei confronti della comunità hacker, come nel caso di una Commissione del Senato degli Stati Uniti che ha invitato i membri del già famoso club di hacking statunitense L.O.P.H.T. per testimoniare davanti alla Commissione sui livelli di sicurezza dei sistemi informatici americani. In Italia, nella fase iniziale del fenomeno, tale genere di rinforzo può essere stato fornito anche dagli organi investigativi ad alcuni hackers arrestati, a causa della situazione di impreparazione operativa che caratterizzava la fase iniziale dell'attività di tali agenzie. Spesso gli aspetti negativi derivanti dalla cattura e dall'arresto dei giovani hackers vengono mitigati dalla mancanza di normative e procedure efficaci costituendo ulteriore rinforzo legato a un senso di invulnerabilità giudiziaria.

I costi del computer crime aziendale

Molte agenzie e istituti di ricerca internazionali hanno cercato di quantificare i danni economici indotti dal computer crime, con dati talvolta discrepanti. Secondo alcune stime della Ernst&Young, il computer crime potrebbe costare negli USA fino a cinque miliardi di dollari l'anno, mentre un istituto di ricerca californiano, denominato Search, sostiene addirittura che le stime per le perdite attribuibili al computer crime arrivano a 40 miliardi di dollari l'anno. Le perdite sono generalmente legate allo spionaggio industriale, al furto di tempo macchina, alle frodi, ai sabotaggi, alla duplicazione abusiva del software e ai virus informatici[21]. Nel rapporto annuale 2000 del CSI e dell'FBI viene riportato che nel 1999 le perdite verificabili causate dagli hacker hanno raggiunto, solo negli USA, i 265 milioni di dollari (oltre 500 miliardi di lire), raddoppiando rispetto l'anno precedente. Il 90% dei responsabili delle 640 aziende (banche, grandi corporations e organizzazioni governative) che hanno risposto all'indagine, ha ammesso di avere avuto problemi di sicurezza. Solo il 42% degli intervistati ha azzardato una ipotesi "economica" sui danni causati alla propria azienda dai reati informatici: quindi il danno è solo calcolato, ma la cifra reale potrebbe essere più alta. Il 74% degli intervistati ha ammesso furti di informazioni riservate, frodi finanziarie, sabotaggio dei dati o della rete aziendale, *denial of service* e incursioni nella rete interna. Il furto di informazione e la frode finanziaria hanno causato i danni maggiori, rispettivamente 68 e 56 milioni di dollari. Nel 1999 il costo degli attacchi dei siti con i "*denial of service*" è stato di 116.000 dollari: nel solo febbraio del 2000 la stima (dopo gli attacchi a Yahoo, Ebay, ecc.) è già di 8,2 milioni di dollari di danni.22

L'Association of British Insurers, che rappresenta la maggior parte delle compagnie assicuratrici inglesi sostiene che molti dei loro membri riferiscono il computer crime come il crimine che aumenta più velocemente di ogni altro e di cui non si riesce a vedere ancora una pausa d'arresto. Nel 1996 il costo che il computer crime avrebbe inflitto al mondo degli affari britannico sarebbe calcolato attorno a 1,54 miliardi di dollari, stando ai soli danni pagati dalle assicurazioni che ammontano a 308 milioni di dollari all'anno, anche se, considerando le perdite non assicurate, le opportunità di affari perdute, le perdite di produzione e di vendita legati al computer crime, il vero costo che l'impresa subisce ogni anno è verosimilmente maggiore.23

Per quanto attiene al settore bancario la *House Banking Committee* ha pubblicato un rapporto in cui si sostiene che gli istituti finanziari statunitensi perdono attualmente almeno 2 miliardi di dollari l'anno per furti informatici, dovuti ad un incremento delle transazioni via internet, senza una parallela diffusione dei programmi necessari per proteggersi dai furti informatici.24

Le perdite legate al *furto di tempo macchina* sono elevate ma spesso di difficile quantificazione. Fare una stima del costo dei furti di denaro, di beni e servizi, messi in atto dai dipendenti all'interno di un'azienda è infatti complesso perché la maggior parte di tali furti non viene resa nota. Vanno da quelli insignificanti come rubare delle penne a quelli più gravi come la vendita

[21] Behar Richard, Who's reading your e-mail?, in Fortune, february 3, 1997, pp.56-70; Clarke, R. (1998). Technological aspects of internet crime prevention.

22 Il Resto del Carlino 10-1-2000

23 Articolo su internet (senza riferimenti se non "Distribuited by Scripps Howard Service")

24 Bankers'hotline, Vol VIII, n°1

di segreti aziendali che procurano lauti guadagni. Negli Stati Uniti tali furti sono stati quantificati da Adler in 6 miliardi di dollari annui già nel 1977 e da Pope nel 1978 in 10 miliardi di dollari annui. Da varie ricerche risulta che comunque un buon numero di dipendenti commette furti tanto che Adler attribuisce ad esempio il 30% dei fallimenti di società negli Stati Uniti alla loro disonestà.
Sempre negli Stati Uniti analisi più recenti del "*Department of Commerce*", dell'"*American Management Association*", del "*Joint Economic Committee of Congress*", nonché di alcune Università ed Associazioni imprenditoriali, hanno ipotizzato che le perdite economiche causate dal furto dei dipendenti oltre ad incidere sui profitti possono avere un effetto drammatico sulla stabilità delle imprese, in quanto è stato calcolato che tali furti ammontano annualmente tra i 60 e i 120 miliardi di dollari, (escludendo dal calcolo i miliardi spesi per i sistemi di sicurezza e controllo).
I danni per *frodi* vengono da più tempo analizzati dagli studiosi e dalle aziende stesse. Già dall'inizio del decennio scorso numerose riviste scientifiche e vari periodici avevano posto l'attenzione sui rischi aziendali di frode. Secondo Le Figarò, del 30 Novembre 1995, il Ministero del tesoro Americano aveva stimato nel 94' che il danno subito dalle aziende, società ed enti per furti e rivendita degli archivi del parco clienti, distruzione di dati commerciali a profitto dei concorrenti, utilizzazione fraudolenta di carte di credito, ammontava ad oltre 100 miliardi di dollari l'anno. *Internet News*, nell'Aprile 1998 riporta le stime dei servizi segreti americani, secondo i quali il danno economico prodotto dal furto di informazioni sulle carte di credito da banche dati on-line, ammonta a mezzo milione di dollari l'anno. In un'altra ricerca segnalata dal C*redit risk report,* durata due anni e mezzo in cui sono stati analizzati 2608 casi di frodi e di abusi informatiche, risulta che una azienda media perde circa il 6% del suo guadagno annuo per frodi e abusi commessi dai propri dipendenti. Secondo tale studio le frodi e gli abusi sono costate nel 1998 alle organizzazioni statunitensi più di 400 miliardi25. Il costo ad esempio per le compagnie telefoniche statunitensi relativo al furto e l'uso illecito di numeri di carte di credito telefoniche, è stato stimato annualmente a 50 milioni di dollari26. L'ammontare delle frodi per i web-commercianti in Francia è difficile da quantificare: le cifre variano da 200 agli 800 milioni di franchi nel 199927.
La *duplicazione abusiva del software* costituisce un'altra fonte di perdite per le aziende. Le aziende che subiscono i maggiori danni sono ovviamente quelle produttrici del software ma tale forma di illecito procura delle perdite anche alle aziende utilizzatrici che subiscono la concorrenza sleale di altre organizzazioni che risparmiano il denaro necessario all'acquisizione legale di programmi talvolta molto costosi. Da una ricerca della BSA (Business Software Alliance, associazione internazionale senza fini di lucro impegnata nella lotta contro la duplicazione e l'utilizzo, di software illegale) risulta che nel 96 in Italia, il 55% dei programmi installati nei personal computer era di provenienza illegale, a fronte di una media europea del 43% e nord-americana del 28%. Ciò ha causato in Italia un danno economico di circa 580 miliardi di lire, che ha colpito tutti gli operatori del settore28.
Il *virus informatico* può essere considerato secondo l'esperto statunitense Joseph Froenlich la moderna piaga che affligge il nuovo millennio e una rilevante fonte di danni per le imprese. I numeri "dell'infezione" sono inquietanti: il danno economico annuale relativo ai virus, è stato stimato a oltre 1 miliardo di dollari nel '96. Una ricerca del 97' ha infatti rilevato che il 98% delle imprese Nord Americane sono state infettate da più di 6000 tipi di virus che sono attualmente catalogati.
I costi dello *spionaggio industriale informatico* sono anch'essi molto elevati. Secondo l'ASIS, American Society for Industrial Security, i cui rapporti forniscono al governo americano i dati sulla perdita economica subita dalle imprese a causa dello spionaggio industriale, gli attacchi

25 Credit Risk Report, 6 Aprile, 1998
26 Pittsburgh City Paper, Vol. 4, n° 34, pp. 8-9
27 dati ripresi da Le Figarò in occasione della riunione dei rappresentanti del G8 a Parigi per fare un bilancio sulle frodi telematiche, dal 15, al 17 Maggio 2000
28 "pirateria il vizio continua" in *Microsoft Magazine*, Estate 97', p. 89

contro le società USA sono aumentati nel 1997, a tal punto da procurare una perdita alle imprese in termini di "proprietà intellettuale", di oltre 300 miliardi di dollari29.
Secondo PC World Italia, del Maggio 1997, la minaccia di un *sabotaggio* a volte può arrecare più danni di un furto di dati: è stato stimato che una grande compagnia assicurativa può arrivare a perdere 275 mila dollari al giorno (poco meno di 500 milioni di lire) se i suoi computer si fermano. Una grossa compagnia aerea perderebbe 20 mila dollari al minuto (ovvero poco meno di 40 milioni di lire in caso di blocco totale dei suoi sistemi informatici.
Come si può facilmente evincere talvolta nelle ricerche presentate si rilevano delle discrepanze tra le varie stime che sono probabilmente dovute a scelte metodologiche diverse o alla considerazione di variabili difformi nonché alla possibilità di "logiche aziendali". Un dato sembra comunque emergere: il computer crime è in grado di generare delle perdite enormi per le aziende, in alcuni casi può condurre addirittura al fallimento di realtà imprenditoriali che hanno affidato all'informatica e alla telematica i loro gangli vitali.

Le cause del computer crime
Individuare la causa specifica (negli individui o nell'ambiente) che determina un comportamento criminale informatico rappresenta fattore di grande attrattiva per gli studiosi di Criminologia che hanno tentato di fornire delle spiegazioni verosimili, talvolta supportate da ricerche complesse. La possibilità di isolare degli elementi identificabili, antecedenti all'azione criminale, in grado in qualche modo orientare l'azione preventiva "localizzando" i soggetti a rischio potrebbe infatti costituire uno strumento prezioso nella comprensione e nel contrasto al crimine. Purtroppo tale percorso non sembra offrire grandi certezze e sovente ha condotto gli studiosi in condizioni di impasse teorica e metodologica. La letteratura specialistica, in questo ambito, ha fornito una grande varietà di fattori personologici, sociali, motivazionali, razionali, strumentali ed economici come cause del computer crime, utilizzando campioni di autori certi, vale a dire di soggetti scoperti. Talvolta sono stati proposti confronti tra computer crimes dettati da questi motivi ed altre forme di abuso o di furto (Bologna, 1982)[30]. Altri autori (Franklin, Nycum, Myers)[31] hanno enfatizzato il fatto che alcune forme di computer crime si configurano più come un gioco che come un crimine vero, ritenendo ad esempio che gli hacker si impegnano in determinate azioni per desiderio di sfida intellettuale, istruttiva ed eccitante anche se le loro imprese comportano spesso notevoli perdite finanziarie per le vittime. Diverse ricerche si sono orientate esclusivamente sulle cause insite nelle caratteristiche individuali o ambientali proponendo numerose tipologie. Parker[32] ad esempio, afferma che le situazioni di lavoro che producono insoddisfazione possono aumentare le probabilità di un uso improprio del computer. Riassumendo, alcuni studi basati su approcci tipologici e deterministici suggeriscono che si possono isolare varie cause (interne ed esterne all'individuo-autore) che in qualche modo determinano la commissione di un crimine connesso all'uso del computer: ragioni finanziarie, sociali, di sfida, di rivolta, di vendetta, frustrazione, depressione, psicopatologiche, di curiosità eccetera. Riportiamo alcune delle principali ricorrenze motivazionali, descritte da vari autori, riscontrate negli autori di computer crime aziendali:

1. motivazioni economiche e sociali, sia dovute a crisi finanziarie dell'autore che al suo semplice desiderio di raggiungere posizioni più elevate nella scala sociale anche in maniera illegale;
2. motivazioni di sfida che possono indurre un soggetto a commettere un abuso tramite computer per dimostrare (anche a se stesso) le proprie capacità. Tale circostanza può riferirsi sia agli hackers esterni che a eventuali insiders che compiono azioni illegali all'interno dell'azienda;

29 ANSA 12 GENNAIO 1998
30 V.Sacco – E. Zureik, *Correlates of Computer Misuse*, cit. in *Artificial Intelligence Review*, N. 6, 1992, KLUWER ACADEMIC PUBLISHER
31 *Ibidem*
32 D. B. Parker, *Crime by Computer,* 1976, CHARLES SCRIBNER'S SONS, New York

3. motivazioni di vendetta nei confronti dell'azienda o di un suo dirigente da parte di persone che ritengono di aver subito un'ingiustizia o che hanno perso il posto di lavoro.

Tali approcci, pur se tendenzialmente rassicuranti per l'opinione pubblica in quanto portatori di elementi causali classificabili ed individuabili, in realtà sembrano non considerare la complessità dell'azione umana e la sua caratteristica prevalentemente costruzionistica influenzata, ovvero, da elementi predisponenti antecedenti ma anche da dinamiche di interazione e significazione effettuate attraverso i processi di pensiero che rendono assai più incerte le predizioni comportamentali. Pur se le difficoltà finanziarie dell'autore o la bassa tolleranza alla frustrazione, ad esempio, sembrano essere frequenti nelle cases analisys sul computer crime, come in quella proposta da Jack Bologna[33], tali fattori saranno sicuramente riscontrabili, all'interno di un'azienda, in molti altri soggetti (forse la prevalenza) che pur trovandosi nelle medesime condizioni non eseguono e forse non eseguiranno mai alcun crimine. E' necessario pertanto considerare le caratteristiche sociali ed individuali con la debita accortezza e mai svincolate dall'analisi più complessa e sofisticata dei processi di percezione del crimine, di disimpegno morale e, più genericamente, di attribuzione di significato alla propria condotta da parte dell'autore.

Riferimenti bibliografici

Andrews Edmund L., *Europeans see U.S. encryption proposal as threat to privacy*, in *The New York Times*, october 9, 1997.
Committee Oks protections for computer systems, in *CQ*, august 10, 1996, p.2255.
Discouraging the inside job, in *Inc.*, april 1994, p.122.
Gatecrashers, in *National Review*, april 21, 1997, pp.14-16.
Hack attack, in *Forbes Asap*, june 3, 1996, pp.97-110.
House panel approves bills to criminalize Internet theft, in *CQ*, october 4, 1997, p.2404.
How to secure your Web site, in *Datamation*, september 1996, p.18.
How we invaded a Fortune 500 company, in *Fortune*, february 3, 1997, pp.58-61.
Keys to the kingdom, in *Time*, spring 1995, p.64.
Noted & notorious hacker feats, in *Byte*, september 1995, pp.151-162.
Paranoia strikes deep, into the Web it will creep, in *PS*, november, 1996, p.74.
Safeguarding your network, in *Black Enterprise*, october 1996, p.48.
Security on the cheap, in *Inc.*, june 1996, p.123.
Senate passes bill to punish computer hackers, in *CQ*, september 21, 1996, p.2677.
Teach your children well, in *U.S. News & World Report*, january 23, 1995, p.60.
Technology unlocks the architecture of a crime, in *American City & County*, august 1996, p.58.
Basile Robert, *Techno-theft robs millions from consumers and manufacturers*, in *Usa Today*, september 1996, pp.26-27.
Behar Richard, *Who's reading your e-mail?*, in *Fortune*, february 3, 1997, pp.56-70.
Bernasconi P., *La prevenzione del computer crime nel settore bancario: l'esperienza svizzera*, in *Dir-Inf*, 1988, Giuffrè, Milano, pp.723-748.
Boudon R., *Metodologia della ricerca sociologica*, 1970, Il Mulino
Brown Eryn, *The myth of E-mail privacy*, in *Fortune*, february 3, 1997, p.66.
Bunn Austin, *Hackers, Inc.?*, in *Village voice*, august 19, 1997, p.37.
Butera F., *Il castello e la rete*, F. Angeli, 1991
Canterucci Jim, *Intranet security*, in *Training & Development*, february 1997, p.47.
Caragata Warren, *Crime cyber*, in *Maclean's*, may 22, 1995, pp.50-52.
Castells Manuel, *Cittadini, tutti su Internet!*, *El Paìs*, pp.106-108.
Chidley Joe, *Cracking the Net*, in *Maclean's*, may 22, 1995, pp.54-56.
Chisholm Patricia, *Fighting infection*, in *Maclean's*, may 22, 1995, p.56.

[33] J. Bologna, *Computer Crime: wave of the future*, 1981, ASSETS PROTECTION, S. Francisco

Clark Charles S., *Regulating the Internet*, in *The CQ Researcher*, Vol.5, n.24, june 30, 1995, pp.561-584.
Caryl Christian, *Reach out and rob someone*, in *U.S. News & World Report*, april 21, 1997
Cohen Fred, *Porous as Swiss cheese*, in *Forbes Asap*, june 3, 1996, p.76.
Cohen Fred, *Your firewall won't save you*, in *Forbes Asap*, june 3, 1996, p.84.
Cook William J., *Scrambled signals from Washington*, in *U.S. News &World Report*, october 14, 1996, p.64.
Cortese Amy, *Warding off the cyberspace invaders*, in *Business Week*, march 13, 1995, pp.92-93.
De Leo G, Patrizi P., *La spiegazione del crimine*, 1992, Il Mulino
DeYoung H. Garrett, *Among us*, in *Industry Week*, june 17, 1996, pp.13-16.
Edwards Owen, *Hackers from hell*, in *Forbes Asap*, october 9, 1995, p.182.
Elmer-DeWitt Philip, *I've been spammed!*, in *Time*, march 18, 1996, p.77.
Eng Paul M., *The best defense remains a good offense*, in *Business Week*, august 11, 1997, p.80A.
Ercolani A.P., Areni A., Mannetti L., *La ricerca in psicologia*, 1990, Nuova Italia Scientifica
Flanagan William G. and Gutner Toddi, *The perils of voice mail*, in *Forbes*, january 17,1994, pp.106-107.
Freedman David H. and Mann Charles C., *Cracker*, in *U.S. News & World Report*, june 2, 1997, pp.57-65.
Gertz Bill, *Spies use Internet to build files on U.S.*, in *Washington Times*, january 3, 1997.
Givon Moshe, Mahajan Vijay & Muller Eitan, *Software piracy: estimation of lost sales and the impact on software diffusion*, in *Journal of Marketing*, vol.59, january 1995, pp.29-37.
Godwin Mike, *Cops on the I-way,* in *Time*, spring 1995, pp.62-64.
Goodell Jeff, *The samurai and the cyberthief*, in *Rolling Stone*, may 4, 1995, pp.40-71.
Gray Robert T., *Clamping down on worker crime*, in *Nation's Business*, april 1997, pp.44-45.
Hafner Katie, *Kevin Mitnick, unplugged*, in *Esquire*, august 1995, pp.81-88.
Holland Bill, *Net hearing may be precursor to bill*, in *Billboard*, september 20, 1997, p.86.
Huber Peter, *One cheer for hackers*, in *Forbes*, october 7, 1996, p.148.
Jefferson Jon, *Deleting cybercrooks*, in *Aba Journal*, october 1997, pp.68-74.
Krauss Clifford, *Eight countries join to combat computer crime*, in *New York Times*, december 11, 1997.
Mannheim H., *Trattato di criminologia comparata*, 1975, Einaudi
Mannix Margaret, *Can hackers break into 'Netscape'?*, in *U.S. News & World Report*, october 2, 1995.
Marcelli G., *I reati informatici a danno dell'INPS*, in *Dir-Inf*, 1993, pp.1007-1023.
Matza D., *Come si diventa devianti*, Il Mulino, Bologna, 1976
McCarthy Vance, *New tools. Authenticate remote users*, in *Datamation*, september 1996, pp.92-96.
McCollum Kelly, *Attacks on USENET. Affect 200 machines*, in *The Chronicle of Higher Education*, march 28, 1997, p.A30.
McLeod Jonah, *Let the buyer beware of Internet commerce*, in *Industry Week*, may 1, 1995, p.58.
O'Malley Chris, *Information warriors of the 609th*, in *Popular Science*, july 1997, pp.71-74.
Ota Alan K., *Congress eyes Internet regulation*, in *Journal of Commerce*, december 11, 1997.
Pellegrini D., *Uso non autorizzato del computer. Limiti e prospettive della tutela penale*, in *Dir-Inf*, 1987, pp.289-311.
Ponti G.L., *Compendio di criminologia*, 1980, Raffaello Cortina Editore
Securité Informatique, fevrier 1989, n.35, pp.1-8, Publinews 3, avenue Galliéni 92000 Nanterre.
Quittner Joshua, *Cracks in the Net*, in *Time*, february 27, 1995, pp.34-45.
Quittner Joshua, *Kevin Mitnick's digital obsession*, in *Time*, february 27, 1995, p.45.
Quittner Joshua, *Panix attack*, in *Time*, september 30, 1996, p.64.
Quittner Joshua, *The hacker's revenge*, in *Time*, may 12, 1997, p.60.
Quittner Joshua, *Unmasked on the Net*, in *Time*, march 6, 1995, pp.72-73.

Reynolds Rhonda, *The NexGen-eration*, in *Black Enterprise*, february 1996, p.30.
Roush Wade, *Hackers: taking a byte out of computer crime*, in *Technology Review*, april 1995, pp.33-40.
Schafer Sarah, *Case study: On-line crime (part I)*, in *Inc.*, may 1996, p.126.
Schafer Sarah, *Firewalls defined*, in *Inc.*, may 1996, p.126.
Schafer Sarah, *On-line crime (part II)*, in *Inc.*, june 1996, p.123.
Serra C., Strano M., *Nuove frontiere della criminalità,* 1997, Milano, Giuffré
Shear Kenneth, *So protect yourself*, in *Forbes Asap*, june 3, 1996, p.84.
Snyder Beth, *Bad rap: companies patrol Internet for online abuse*, in *Advertising Age*,october 6, 1997, p.44.
Snyder Beth, *Hackers alter ValuJet site*, in *Advertising Age*, october 6, 1997, p.44.
Stephens Gene, *Crime in cybers*, in *The futurist*, september-october 1995, pp.24-27.
Sussman Vic, *Gotcha! A hard-core hacker is nabbed*, in *U.S. News & World Report*, february 27, 1995, pp.66-67.
Sussman Vic, *Policing cyberspace*, in *U.S. News & World Report*, january 23, 1995, pp.55-60.
Sutherland E.H., W*hite collar criminality*, in American Sociological Rewiew, 1940
Taninecz George, *High tech, high crime*, in *Industry Week*, april 17, 1995, pp.51-56.
Tiedemann K., *Criminalità da computer*, in F. Ferracuti (a cura di), *Trattato di criminologia, medicina criminologica e psichiatria forense*, vol.X, *Il cambiamento delle forme di criminalità e devianza*, Giuffrè, Milano, 1988.
Traverso Silvia, *Assicurazione e software*, in *Dir-Inf*, 1987, pp.312-324.
Wanat Thomas, *Hackers alter NCAA Web Site*, in *The Chronicle of Higher Education*, march 21, 1997, p.A54.
Wanat Thomas, *Two Internet-savvy students help track down the hacker of an NCAA Web Site*, in *The Chronicle of Higher Education*, march 28, 1997, p.A30.
Wilson David L., *Computer experts find new security problem*, in *The Chronicle of Higher Education*, september 27, 1996, p.A31.
Wilson David L., *U.S. planning an emergency-response team to cope with attacks on information networks*, in *The Chronicle of Higher Education*, july 5, 1996, p.A19.
Young Jeffrey R. and Wilson David L, *Researchers warn of the ease with which fake Web Pages can fool Internet users*, in *The Chronicle of Higher Education*, january 10, 1997, p.A25.
Young Jeffrey, *Cyberdicks and virtual gumshoes*, in *Forbes Asap*, june 3, 1996, p.82.
Young Jeffrey, *Pay to hack your own system?*, in *Forbes Asap*, june 3, 1996, p.80.
Young Jeffrey: *Spies like us*, in *Forbes Asap*, june 3, 1996, pp.71-92.