hAcK3rZ and Information Warfare

«Quaderni di Sociologia», vol. XLIV, Rosenberg & Sellier, Torino, 2000, pp. 22-47

Gianluca Miscione

Abstract:

This piece of work attempts to suggest an outlook on hacking-related phenomena which are usually enquired according to many different disciplinary perspectives, and it especially focuses on their social aspects. Hackers are here considered as system-intruders, an activity which doesn't imply computer systems only as the boundaries of hacking are overlapping those of the cultural and aesthetic fields. As a consequence of this, social institutions we believe in could loose their legitimacy when their errors are shown. The deeper the error is rooted into the mechanism, the more it spreads mistrust. What is socially relevant is the use we make of networks and the confidence we accord to them. «Hacking is an attitude» constitutes a way to approach information and communication technology (ICT) in accordance to the «hands on» and «information wants to be free» mottos which contrast any confidence in economically or politically managed development. Anyone who respects the hacker ethics is bound to explore the «natural rules» of an electronically simulated place. The «daydream nation», the «matrix» evoked by W. Gibson proves to be an environment where not only signs but also acts are meaningful. The democratization of technology is defining new economical and military settings, new forms of sociality and knowledge, but it enables anomy either.

«War games», «The Net», «Hackers» sono film che sicuramente non entreranno nella storia del cinema, ma la cui trame, svolgendosi, toccano temi rilevanti quali: intersezione fra guerre e sistemi di telecomunicazione, dipendenza delle persone da informazioni archiviate in Rete, opposizione degli hacker alle multinazionali.

I mass media riportano periodicamente e con enfasi violazioni di sistemi informatici, blocco di grandi siti, appropriazioni di informazioni riservate [1]. Le questioni sollevate dalla pratica dell'hacking non hanno una definizione che le riconduca ad un solo ambito. A seconda degli attori in campo e dei loro obiettivi ci si riferisce a discipline diverse, a scapito di una visione non unitaria ma organica del fenomeno. Le più significative tematiche sollevate sono:

- sicurezza dei sistemi informatici
- dipendenza di individui e società dalle informazioni
- rifiuto di delega dello sviluppo telematico
- sfida alle grandi istituzioni
- cambiamento di alcuni aspetti dei conflitti militari, economici e politici.

Il fenomeno è in crescita, tanto che nel 1999 il dipartimento americano della difesa ha riscontrato 22.144 attacchi alle sue reti; l'anno precedente erano stati 5.844 [2]. Analoghi aumenti si registrano nel settore privato, che però denuncia solo una piccola percentuale degli attacchi subiti a causa dei negativi ritorni d'immagine.

1. Chi sono gli hacker

Chi siano davvero gli hacker è difficile a dirsi. Per governi e grandi software house sono solo pirati, una variante tecnologica dei delinquenti comuni. Ma per buona parte del popolo dei programmatori, dei

ricercatori, degli internauti della prima ora, sono al contrario interpreti dello spirito autentico della telematica [3]. Una definizione a maglie larghe include attivisti impegnati nell'ampliare la libera circolazione dell'informazione, progetti di autoproduzione del software, attività mirate a svelare la debolezza dei sistemi telematici, difensori di una rete mondiale non sottomessa a istituzioni e corporazioni; ma anche coloro che danneggiano sistemi e dati accessibili dalla Rete. Il motto «information wants to be free» è ricorrente. Può essere interpretato in tre maniere che non si escludono: senza restrizioni contenutistiche (contro le censure), senza controllo degli autori (contro la proprietà intellettuale), senza vincoli monetari (gratuità) [4].

Ogni lettura è ispiratrice di innumerevoli iniziative. Attorno all'insofferenza per l'intrusione di terzi sul contenuto delle comunicazioni si coagulano rivendicazioni sulla libertà di pensiero ed espressione, difesa della privacy e delle libertà civili correlate, nonché il rifiuto di qualsiasi deliberata estromissione dall'agora comunicativo (cioè di un esercizio del potere di inclusione/esclusione). La proprietà intellettuale è sentita come limite per individui e società affinché traggano il massimo vantaggio dalla produzione intellettuale. Il costo marginale di copia quasi nullo per testi, immagini, video, musica (ciò che è consuetamente definito «contenuto») in formato digitale accentua l'arbitrarietà delle restrizioni alla diffusione dei saperi a uso e consumo di tutti. Le istanze «NoCopyright» mirano a trasformare le conoscenze in beni pubblici senza che interessi particolari impediscano di trarne la massima utilità [5]. Oltre alle questioni economiche, la proprietà intellettuale riduce le possibilità da parte di altri di riutilizzare il lavoro altrui, di derivarne prodotti differenti, innescando un circolo virtuoso che non distingua fra autori e fruitori ma renda tutti «wreader» più di quanto effettivamente permettano gli ipertesti [6]. Spirito di collaborazione e gratuità degli scambi hanno dimostrato (anche) la loro efficacia ed efficienza nello sviluppare buona parte delle tecnologie che costituiscono Internet.

Comunque non mi occuperò direttamente di alcuna di queste tre posizioni. Seguendo una definizione più ristretta e più vicina all'uso comune, hacker è colui che si intrufola in sistemi informatici senza le consuete autorizzazioni, colui che usa la tecnologia (e soprattutto i suoi difetti) a modo proprio [7]. L'hacker prima di tutto cerca, ciò che fa quando trova è un altro discorso. Si comincia magari per gioco, gareggiando per accedere ad un computer molto protetto, sfida più appassionante di qualunque videogioco [8]. Poi può diventare hobby, passione o anche di più. Hacker è un etichetta che abitualmente si attribuisce a: *a)* chi si intrufola in computer di tutto il mondo, *b)* phreak che si avventurano nelle reti telefoniche senza pagare, *c)* programmatori di virus e worm [9], *d)* cracker, che rimuovono le protezioni dei software affinché siano utilizzabili gratuitamente e senza restrizioni [10], *e)* lamer, che distribuiscono (o vendono) il lavoro altrui, *f)* cypherpunks o crittoanarchici che sviluppano strumenti crittografici per sottrarre le comunicazioni in rete al controllo di terzi [11], e soprattutto a *g)* chi compie illeciti attraverso Internet. Fra di essi vi sono divisioni e rivalità, in particolare fra hacker veri e propri, programmatori di virus e cracker [12] (presenti soprattutto nei paesi dell'Europa orientale, area dove il livello economico non è così basso da impedire lo sviluppo telematico e la legislazione in materia è pressoché nulla). Con l'informatizzazione delle reti telefoniche i phreak vanno sparendo; i lamer godono di cattiva fama presso di tutti.

I cosiddetti pirati informatici sono persone curiose di esplorare i limiti della tecnica, di appropriarsene piegandola alla propria volontà [13]; di operare una critica senza i paroloni della teoria ma con la forza dei fatti. Si assiste ad azioni che rilevano possibilità e limiti di un campo di attività, scavalcando, in parte, gli ambiti intellettuali che dovrebbero precedere la pratica, almeno secondo una prospettiva moderna. Se gli attori impegnati nello sviluppo non sono più disposti a concedere un ruolo prioritario all'analisi teorica, il lavoro critico è spinto a scendere sul medesimo piano applicativo se non vuole trovarsi spiazzato. La ricerca scientifica e le sue applicazioni tendono a spostare sempre più a monte sia il momento di analisi che quello, conseguente, politico-decisionale. Risultato è che spesso i luoghi di rappresentanza istituzionali possono al massimo accettare o rifiutare la nuova situazione ma non influire sul processo indirizzandolo secondo obiettivi negoziati. Oltre alle caratteristiche in sé delle tecnologie, si tende a proporre un senso di conformismo nel loro impiego. Da questo punto di vista i corsari della Rete mettono in dubbio la pretesa naturalezza di un uso ortodosso dei mezzi, evidenziandone l'arbitrarietà; mostrano come l'uso normale non sia una necessaria conseguenza della tecnica. Oltre che ricordare come la Rete (come insieme di tecnologie e di usi che se ne fanno) sia una costruzione sociale e non il semplice risultato di progetti fatti a tavolino, la loro critica dà consapevolezza del fatto che controllare gli strumenti vuol dire controllare gli utilizzatori. Gli esempi possono essere molto vari: monitorare i mail server di una nazione fornisce ricchissime informazioni sulle attività che vengono svolte, possedere programmi serve ad indurre gli utenti a fare scelte secondo gli interessi dell'azienda, supportare comunità virtuali favorisce

il raccogliersi di consumatori omogenei e così via [14].

Non si vuole legittimare qualunque eterodossia nell'uso della tecnica; chi rapina una banca con computer e modem rimane un rapinatore, un attacco dei servizi segreti a calcolatori stranieri rimane un'azione militare. Il fatto che gli hacker siano d'accordo su questo punto non significa però che l'hacking non vi abbia nulla a che vedere. Gli strumenti sono molti e facilmente reperibili (gratuitamente) [15]; la difficoltà sta nel saper usare software per decifrare password, sniffer per appropriarsi di dati in transito, scanner per analizzare gli accessi lasciati incautamente incustoditi, cavalli di Troia da infiltrare oltre i firewall, etc [16]. Poi si cancellano le tracce.

Il rapporto fra leggerezze nell'amministrazione dei sistemi informatici e allarme sociale è di concausa. Se gli hacker possono arrivare un po' dappertutto lo si deve anche al fatto che i sistemi sono pieni di buchi, che si cerca di risparmiare su costi che non hanno rendimenti nel breve periodo e che i responsabili della sicurezza spesso non sembrano dare peso alle regole di protezione [17]. Ciò con ricadute negative su tutti perché quando le mancanze vengono evidenziate dall'azione degli hacker, si invocano regole più restrittive, mentre un lavoro più accurato non le rende necessarie. Dalle statistiche del Cert, emerge però che la fonte più sospetta delle infrazioni commesse lo scorso anno non sono gli hacker ma gli impiegati autorizzati [18].

Nella prima metà degli anni '80 nascono alcuni punti di riferimento per gli hacker: 2600: The Hacker Quarterly e il Chaos Computer Club [19]. Mantengono un ruolo tuttora molto rilevante, anche in questioni non strettamente legate all'hacking: il primo sta affrontando un processo sul diritto di far circolare un programma per leggere i Dvd [20]. Il secondo ha visto eleggere un suo membro come rappresentante all'Icann (Internet Corporation for Assigned Names and Numbers, l'autorità internazionale che regola l'assegnazione dei numeri e degli indirizzi Internet). Dal 17 ottobre il direttore europeo dell'Icann è, per volontà popolare, un hacker; anche chi sbrigativamente bollava lui e il "computer underground" come anarchici, dovrà tenere conto della sua azione istituzionale [21].

2. Dalla cibernetica ai crackdown, le vicende dell'hacking si intrecciano alla storia recente

Nei suoi quarant'anni di vita l'hacking ha lasciato segni evidenti in una possibile storia sociale dell'informatica. Le radici sono indistinguibili dall'origine dei primi calcolatori elettronici e dalle questioni filosofiche e sociali che contemporaneamente si posero, in particolare nel campo della cibernetica.

Negli anni '70 nasce il phreaking per telefonare gratuitamente, ma anche i tecnici iniziano a «bucare» i sistemi per fare conoscenza con i colleghi e scambiare idee e conoscenze. Furono i phreaker a pensare l'uso del telefono per parlare contemporaneamente fra più di due persone, anticipando le chat-line.

Jobs e Wozniak, due hacker californiani, dal loro garage avviarono la rivoluzione del personal computer. Crearono il primo Apple, che metteva le potenzialità dell'informatica alla portata di tutti [22]. Il progetto rispecchiava le istanze di democratizzazione espresse dai radicali dell'area di San Francisco, l'aspirazione a creare una tecnologia dell'informazione alternativa ai grandi elaboratori nelle mani di pochi [23]. La democratizzazione più che la pura innovazione tecnica era il fine degli attivisti di allora; così le redini di molti settori passarono dal controllo di poteri economici consolidati e di austeri matematici/informatici a geni del fai da te. Il personal diventa una realtà quotidiana per molti occidentali e l'informatica acquista un'immagine meno fredda e più creativa, anche ludica con la diffusione dei videogiochi (che sono tuttora un impulso determinante per l'home computing). Sempre negli anni '80 nascono le Bbs (Bulletting Board System), banche dati accessibili via modem gestite da privati cittadini per il gusto di dialogare ed essere utili alla comunità informatica, farsi conoscere e scambiare conoscenze.

Nel 1988 il virus Warm contagia in pochissimo tempo migliaia di computer. Università e centri di ricerca rimangono bloccati e si iniziano a prevedere i reali rischi cui si è esposti in assenza di una seria struttura preposta alla sicurezza. Tra il 1993 ed il 1997 l'hacking esplode nella maggior parte del mondo, con esempi e casi clamorosi. Nascono le prime leggi ad hoc e gli interventi dalle forze dell'ordine si

fanno incisivi: nel1990 ha luogo negli Stati Uniti l'Hacker's Crackdown, quattro anni dopo è la volta dell'Italian Crackdown che stroncò sul nascere la telematica amatoriale italiana [24].

Vale la pena ripetere che a metà anni '80, da una costola dell'hacking sono nati i movimenti «free» e poi «open», fautori della libera circolazione dell'informazione e degli strumenti per elaborarla (stessi principi che hanno dato forma alla tecnologia di Internet). Finalità consone a quanto dichiarato dall'International Telecommunications Union (ITU) delle Nazioni Unite, secondo la quale è un diritto umano fondamentale comunicare e associarsi liberamente, senza interferenze.

Non è secondario che le competenze diffuse fra la popolazione, soprattutto in California, siano l'humus ideale sul quale è germogliato e cresciuto il predominio economico della Silicon Valley.

Altra ragione che rende il mondo degli hacker degno d'interesse è l'anticipazione di alcuni tratti culturali tipici delle comunità virtuali, fra i quali l'individualismo, la scarsa gerarchizzazione, l'importanza del carisma, l'ideazione di un linguaggio adatto al medium, l'essere costruite attorno ad un interesse e l'essere poco invasive della sfera privata. La grande questione se la disponibilità di tecnologie informatiche per un ampio numero di persone avrebbe prodotto una ridistribuzione del potere e della ricchezza rimane ancora senza risposta.

3. Organizzazione per gruppi e attività bellicose

La casistica delle intrusioni è sterminata e talvolta non si può distinguere al suo interno fra realtà e leggenda. Bucare un sistema richiede approfondite conoscenze tecniche (pratiche più che puramente teoriche), programmi adatti e informazioni. Per accedere a tutto il necessario basta un accesso a Internet; competenze, informazioni e strumenti sono a disposizione, gratis [25].

I tipi di attacchi più comuni sono: *a)* intrusione e modifica non autorizzata di dati, *b)* DoS (denial of service), vale a dire impedire al sistema di svolgere le proprie funzioni [26] e *c)* intercettazione e/o modifica di messaggi. Le procedure:

- «scanning» per individuare i punti deboli
- «sniff» per rubare password o altri dati in transito [27]
- il «social engineering» consiste nel farsi passare da un dipendente autorizzato informazioni critiche sull'accesso al sistema
- invio di cavalli di Troia
- «mailbombing»
- diffusione di «virus» e «worm».

Il solo elenco dei tipi di attacco non rende conto di quello che si può fare con essi. L'aspetto altrettanto importante è che la rilevanza anche sociologica del fenomeno è dovuta, in ultima istanza, a quanto si è delegato ai sistemi di telecomunicazione. Trovo si possano individuare due dimensioni lungo le quali analizzare gli aspetti sociali della telematica: una che ponga in risalto lo sviluppo della telematica come campo tecnologico con ampie influenze extra-ingegneristiche, l'altra attenta ai mutamenti e alle prospettive sociali dovuti alla diffusione di tali mezzi. I due assi non sono indipendenti in quanto l'evoluzione tecnologica non è mai aliena dalle richieste della società e la ridefinizione dei processi sociali non è indipendente dai mezzi disponibili. Le pratiche dell'hacking si trovano in un emblematico punto di intersezione delle due prospettive in quanto traducono istanze sociali sul piano della tecnica, plasmandola; d'altro canto, mostrano alla società alcune implicazioni di scelte di delega poco meditate.

Gli effetti di accessi e manipolazioni non autorizzati negli archivi delle banche, delle amministrazioni, etc rendono chiare le conseguenze di una cieca fiducia nel passaggio a strumenti digitali più di

avvertimenti più o meno apocalittici e tendenzialmente retorici (o quantomeno percepiti così). Sebbene probabilmente non sia la prima intenzione dell'hacker, l'effetto significativo è reificare un rischio, permettere al dubbio verso le «magnifiche sorti progressive» non solo di muoversi fra gli astratti poli apocalittici o integrati (magari frutto di speculazioni a tavolino) ma di misurarsi con azioni virtuali quanto mai reali [28]. Da ricordare che le azioni di sabotaggio, oltre ai danni immediati a ditte e stati, contribuiscono a creare e diffondere negli utenti il dubbio sulla sicurezza dell'utilizzo di servizi telematici, in particolare per quanto riguarda carte di credito, con l'effetto di rallentare l'e-commerce. Forzare i sistemi informatici non crea solo danni. Infatti ha l'indubbio merito di evidenziare i punti deboli delle tecnologie impiegate, quindi di indicare cosa vada migliorato (non è raro che aziende offrano un compenso a chi riesce a penetrare i propri server) e in che direzione concentrare lo sviluppo. Le aziende che forniscono strumenti e assistenza per la security sono legate a doppio laccio a questo mondo, che ha creato dal nulla il ricco mercato della sicurezza informatica e che ne muove l'evoluzione individuando i limiti tecnici e dandone conoscenza a tutti (quindi anche alle imprese che non esitano a far «man bassa»).

Per anni l'intrusione in sistemi informatici è stata prerogativa di pochi. Non è da tutti passare notti insonni cercando gli strumenti più adatti, scansionando la Rete per trovare ponti da cui portare a termine le incursioni, analizzando il bersaglio per cercarne i punti deboli e le leggerezze dell'amministratore. Nel corso degli anni le consuetudini si sono cristallizzate in norme e le fantasiose espressioni in un colorito linguaggio incomprensibile ai più. Recentemente la situazione è cambiata. Praticamente tutti i settori dell'informatica stanno orientando il proprio sviluppo tenendo conto delle necessità dell'utilizzatore oltre agli imperativi della tecnica. Proliferano programmi dedicati all'hacking provvisti di interfaccia user-friendly e che automatizzano tutte le procedure che abbiano una qualche ricorsività. Risultato è che oggi un qualunque quindicenne con buona dimestichezza con i computer avvia uno scanner di vulnerabilità all'ora di cena, va a una festa e al suo ritorno trova una lista di centinaia di computer attaccabili. Copia-incolla dell'indirizzo e quel computer è nelle sue mani. La diffusione dell'uso di Internet e di strumenti «amichevoli» comporta un rapido aumento del numero di hacker, o presunti tali. La difficoltà era il gradino che impediva all'ultimo arrivato di cambiare le regole del gioco. La possibilità di salire da soli il gradino d'accesso alle competenze e una crescita numerica così improvvisa, sfaldano la comunità e il ruolo latente che ha svolto, generando anomia. Senza approfondire è pertinente dire che le comunità hanno avuto la funzione sia di insegnare le tecniche, sia di far maturare un senso di identità e un modo di relazionarsi alla tecnologia [29]. Il senso di appartenenza ha veicolato la trasmissione di valori e orientamenti, in particolare una «cultura del dono», spesso determinante nel regolare il comportamento.

Da ognuno ci si aspetta abbia una propria forte motivazione, ma che non sia egoista [30]. Tuttora comunque rimane una forte organizzazione tribale, nel senso che esistono numerose «crew» indipendenti fra di loro; ciò non significa che non ci sia una ricca circolazione di informazioni, tuttavia i vari gruppi mantengono una marcata autonomia decisionale [31]. Altri tratti comuni alle società tribali sono la scarsa differenziazione funzionale e l'esercizio del controllo attraverso norme consuetudinarie più che ferree regole formali; la reperibilità delle risorse previene il costituirsi di forme di potere stabile. La pubblica disponibilità delle informazioni e delle risorse ha il duplice effetto di tenere teoricamente aperto l'accesso alle conoscenze affinché chiunque possa portare il suo contributo, e di disperdere le responsabilità [32].

L'esercizio di un potere da parte di individui che non si costituiscono in attori corporati, l'individualismo come tratto culturale, l'oggettiva difficoltà di una regolazione secondo norme esteriori e l'impossibilità di imporre un'etica sono fattori che accentuano l'anomia. La divergenza degli interessi e degli orientamenti, a parte la loro legittimità, pare non permettere di delineare posizioni unitarie condivisibili. L'assenza di una vera e propria testa del movimento lo rende difficilmente attaccabile dall'esterno [33]. Oltre agli abituali strumenti di scambio di cui dispongono, non mancano più tradizionali raduni nei quali scambiare conoscenze, fare il punto della situazione sui temi caldi del momento, festeggiare, avvicinare altre realtà e rendersi più comprensibili al mondo offline [34].

4. L'informazione diviene fulcro della società e un'etica matura durante il processo

Senza andare sul piano psicologico, si può dire che le motivazioni dell'hacking sono la curiosità, la

voglia di sfida, la riluttanza ad accettare le cose a scatola chiusa, la ricerca della fama, il denaro, la volontà di dimostrare l'inadattabilità del mondo offline (leggi e commercio, fra gli altri) alla Rete. «Access denied» è un limite di per sé insopportabile, infatti esperti di sicurezza del settore pubblico e privato notano che spesso le violazioni sono una sorta di sfida intellettuale, come testimoniato dal fatto che i danni provocati sono spesso nulli o inferiori a ciò che sarebbe possibile [35]. C'è chi si vanta, chi vende la soluzione al «buco» scoperto, chi mette a disposizione della comunità le sue scoperte.

Non è vero che tutti gli obiettivi si esauriscano all'interno della Rete stessa, dando vita ad un intreccio di azioni, relazioni sociali, desideri assolutamente autoreferente. La consapevolezza, non necessariamente formalizzata ed esplicitata, della dipendenza della società dalle reti e della possibilità di accedere a segreti altrimenti inaccessibili muove anche verso obiettivi con risvolti oltre i confini di Internet. Dagli anni '50 e '60, quando gli elaboratori erano usati in pochi centri di ricerca, maturano i primi valori da cui poi si consoliderà una vera e propria etica, avviata soprattutto al M.I.T. di Boston e a Stanford e poi divenuta una cultura, un modo di regolazione sociale consolidato dall'uso [36]. La prima etica, imbevuta dei valori della contestazione americana, promuove un totale accesso alle informazioni, presupposto necessario a qualsiasi democratizzazione della società. Riecheggiando, forse incosapevolmente le idee del padre della cibernetica Norbert Wiener, l'informazione è sentita come un bene in sé, una ricchezza che qualunque barriera sottrae all'umanità [37]. Si era già affermata la convinzione che il controllo sociale è legato a doppio laccio con il controllo dell'informazione [38]. Negli anni '90, con il web, ha avuto inizio la diffusione capillare della telematica nella quotidianità e pertanto la dipendenza più diretta delle persone da tali sistemi. Senza rinnegare i propri principi, l'attività hacker si è così tendenzialmente spostata dall'appropriazione al rilevamento dei rischi che si corrono accettando acriticamente il progresso tecnico. La denuncia ha trovato come arma più efficace gli atti dimostrativi [39]. Parallelamente si è affiancato il principio di non creare danni deliberati [40].

«L'hacking è un'attitudine mentale. Un modo di imparare facendo. È guidato dal desiderio di apprendere come funziona la tecnologia e supportare la libertà dell'informazione» [41]. Trasgressivi d'altronde lo sono sempre stati, criminali no [42]. I punti fondamentali del codice di comportamento dei nuovi hacker (o «computer underground») sono: proteggere dati e hardware, rispettare e proteggere la privacy, usare ciò che viene sprecato, superare le restrizioni non necessarie, promuovere il diritto di comunicare, non lasciare tracce, condividere dati e programmi, vigilare contro la «cyber-tirannia», controllare la sicurezza dei computer [43]. Qui va rilevata l'oggettiva divergenza fra la difesa della privacy e la libera circolazione dell'informazione. Nemmeno la proposta di assoluta trasparenza per questioni di interesse pubblico e la riservatezza per quelle di ordine privato può poggiare su una solida fattibilità empirica, quantomeno a causa del labile confine che separa sfera pubblica e privata, dicotomia sempre meno solida, non solo per effetto dei mezzi di comunicazione elettrici. Come detto, la comunità hacker rischia di sfaldarsi, e sempre più frequentemente le azioni sono indipendenti da ogni regola o intenzione non vandalica. Anche per questo, da più parti si sostiene la necessità di basare la sicurezza sulla reciproca fiducia [44]. Il problema si snoda fra la responsabilità degli utenti in un sistema tendenzialmente decentrato e il perenne dubbio sull'attendibilità di persone e mezzi. Un esempio utile arriva dalla crittografia. Non volendo mettere in mano alle particolarità di ogni politica il diritto a comunicare, sono stati scritti programmi che permettono l'inaccessibilità a terzi a ciò che circola su Internet. Fondamento è la fiducia fra le parti più che in un garante super partes. Il programma di crittografia Pretty Good Privacy (solitamente chiamato Pgp) è un esempio della necessità di un rete fiduciaria che garantisca, al di là della tecnica, l'inattaccabilità del sistema di comunicazione crittato [45]. Per evitare che fra gli interlocutori si interponga un terzo, fornendo una chiave pubblica falsa e accedendo ai messaggi tramite la corrispondente chiave privata, la chiave di un nuovo utente del Pgp deve essere fornita e autenticata da qualcuno della cui chiave e delle cui competenze si sia sicuri. Date tali condizioni la rete può crescere senza smagliature. La fiducia fra gli utenti di un software ai limiti della legalità è probabilmente venato da una dose di «complicità» (nel senso buono del termine) legata alla condivisione di valori, obiettivi e metodi. Ciò che trovo possa giovare alle comunicazioni in rete è dare al concetto di fiducia un senso più astratto dalle particolarità in cui si è originata questa necessità. In tal maniera un panorama variegato che va da comunità virtuali crittografate all'autenticabilità del materiale che circola su Internet darebbe, quando necessario, una maggiore credibilità e peso alle attività svolte attraverso Internet.

Intanto la cultura hacker conquista territori nemici. A metà ottobre 2000 Andy Mueller-Maguhn, portavoce del Chaos Computer Club e direttore europeo dell'Icann ha dichiarato che la realtà della Rete è e dev'essere definita dagli utenti [46]. D'accordo o meno con l'implicito riconoscimento dato a

quest'istituzione, la filosofia di appoggiare la libertà dell'informazione e la riservatezza dei dati personali contro l'ingerenza degli apparati statali non aveva mai ottenuto tanto potere decisionale. Oltre a dare spazio ai diritti dei netizen, Mueller-Maguhn, nelle dichiarazioni d'intenti, si è detto intenzionato a promuovere la cultura del dono nel «paradiso elettronico», la coesistenza di culture differenti con regole proprie, la promozione degli interessi economici entro ambiti chiari e definiti, affinché non monopolizzino Internet. In conclusione ha definito la sua elezione un ottimo «hack».

5. Le tre anime dell'hacking

L'underground digitale è più variegato di quanto normalmente si pensi. Si è proposto di classificarlo in tre (artificiose) categorie: individualista, sociale ed estetico/culturale; tutte accomunate dal motto “hands on” (metterci le mani).

La corrente individualista è quella più sensibile agli aspetti tecnici e a superarne i limiti. Quella sociale coincide in parte con i movimenti «free» e «open» che lavorano a superare gli ostacoli che intralciano la società nel disporre di tutti gli aspetti relativi alla comunicazione [47]. Ad essi si aggiungono gli attivisti, non solo quelli che usano Internet come strumento di comunicazione ma soprattutto coloro che ne fanno un'agora dove rivendicare istanze sociali e politiche [48]. Rilevante l'idea di un collettivo italiano, presto adottata da altri gruppi: il netstrike o corteo telematico che consiste nel coinvolgere il maggior numero di manifestanti e a invitarli a collegarsi ripetutamente al sito bersaglio finché l'eccessivo traffico lo blocca [49]. Le manifestazioni del cosiddetto popolo di Seattle hanno avuto scioperi del genere come parallelo telematico. Indymedia è l'agenzia stampa autoprodotta del movimento antiglobalizzazione, che si propone come anello di congiunzione fra l'attivismo di rete, i movimenti di attivisti di base e i media tradizionali che continuano a influenzare profondamente l'opinione pubblica [50].

L'evoluzione più singolare è l'intersecarsi dell'hackeraggio con correnti dell'ambito artistico. Dalle avanguardie del primo '900 l'arte ha spesso perpetrato la sua critica al sistema culturale e sociale. In particolare il Dadaismo, che ha segnato, al di là delle particolarità storiche, quasi tutti i movimenti espressivi del secondo dopoguerra, non vuole affermare ma portare contraddizioni (o evidenziarle, secondo altri critici). Non vi è uno stile o una poetica in cui il movimento si riconosca; tratti comuni sono l'ironia e l'irriverenza. « [L’anti-arte prodotta dai Dada] Si riduce così alla pura azione, immotivata e gratuita ma proprio perciò demistificante nei confronti dei valori costituiti. [...] Il Dadaismo si propone un’azione di disturbo il cui scopo è di mettere in crisi il sistema, ritorcendo contro la società i suoi stessi procedimenti o usando controsenso le cose cui essa attribuiva un valore» [51]. Non dare nulla per scontato è l'intelligenza di un'avanguardia spesso sfrontatamente superficiale.

Voler rendere indistinguibile vita e arte (assimilando la seconda alla prima e non viceversa come il filone inaugurato da Oscar Wilde), togliere il quid sacrale all'opera d'arte avrebbe potuto permettere «il riscatto estetico di tutta l'esistenza quotidiana» [52]. «Ciò che determina il valore estetico, dunque, non è più un procedimento tecnico, un lavoro, ma un puro atto mentale, una diversa attitudine nei confronti della realtà» [53]. Eredità che tuttora sono ben chiare ad artisti che operano su Internet, che hanno scelto i segni come attrezzi per operare nel «simulmondo». Il campo d'azione e le sue regole sono lontane da quelle hacker ma l'attitudine è affine: per quanto un sistema appaia enorme ed intaccabile, ha punti deboli che, adeguatamente sfruttati, lo mettono in crisi. Non è una questione di potenza ma di conoscenza e acutezza [54]. Da una parte computer, algoritmi, codici e password possono essere scardinati a causa dell'intrinseca debolezza della tecnologia, degli inevitabili bug, dell'imperizia umana. Dall'altra i paradossi, le contraddizioni di convenzioni considerate necessità, la possibilità di fare altrimenti, i meccanismi che regolano produzione e diffusione della cultura. È difficile organizzare una tassonomia delle operazioni, degli interventi e delle opere realizzati; due progetti sono particolarmente significativi: i nomi multipli e il «Digital Hijack» [55].

Il «Digital HiJack», il primo rapimento virtuale della storia, è stato opera degli Etoy che volevano diventare popstar ma si sono dedicati ad atti provocatori in rete, fino a diventare un’azienda con azionisti che produce «hacking culturale e mediatico e smascheramento dei meccanismi del controllo via Internet» [56]. Nel 1996 vincono Ars Electronica, il più significativo premio di Net-art a livello mondiale [57]. Il meccanismo del dirottamento è abbastanza semplice. Abitualmente si usano i motori di ricerca per rintracciare ciò che interessa, quindi essi sono uno dei punti nevralgici per quanto riguarda la visibilità dei contenuti. Pochi sanno come funziona l'indicizzazione dei documenti presenti in Rete. Tutti

possono gratuitamente inserire un sito negli archivi dei motori ma nessuno garantisce che le parole chiave indicate come significative corrispondano ai contenuti delle pagine web. Inoltre esistono graduatorie stilate secondo l'occorrenza delle parole cercate, in base alle quali i siti attinenti all'interrogazione fatta vengono ordinati. Nessuno vieta però di inserire pagine «fantasma» con le parole più cercate dagli utenti per far apparire il proprio sito nella prima schermata di risultati. Si è così innescata una febbrile competizione fra i webmaster che ha ridotto funzionalità e utilità di questi servizi, tutto ad insaputa dei navigatori di Internet. Preso atto della situazione i sette dirottatori hanno preso alcune delle parole più ricercate (sex, playboy, porsche... [58]) e hanno fatto scalare al proprio sito le classifiche che le contenevano. Nell'arco di pochi mesi, milioni di utenti si sono trovati sul loro sito senza volerlo; browser bloccato e praticamente obbligati a leggere la loro rivendicazione che fra il serio e l'ironico chiedeva la liberazione del «Condor», il famoso hacker Kevin Mitnick. Paradossalmente la procedura da loro inventata oggi è utilizzatissima, dai siti (soprattutto pornografici) che cercano di emergere fra gli innumerevoli che esistono.

Luther Blissett (nome di un ex-giocatore del Milan) è un nome multiplo nato nell'estate del '94 con l'intenzione di risolvere problemi relativi all'identità e al dualismo individuo e comunità [59]. Un «allegro inganno» per «sbarazzarsi una volta per tutte del concetto di in-dividuo in nome del con-dividuo, vale a dire di una singolarità multipla il cui profilo comporta nuove idee di responsabilità e di volontà. [...] Ogni singolo corpo-mente (ogni -dividuo) è attraversato da vorticosi flussi di comunicazione che, travalicando i confini del corpo individuale, creano un'elastica comunanza tra le singolarità, la condividualità» [60]. Condizione non rispecchiata dagli ordinamenti giuridici che necessitano della nozione di persona (fisica o giuridica) cui applicare le norme.

«Qualcuno afferma che, di fronte alla tirannia nichilista dello spettacolo, una soluzione potrebbe essere quella di spararle ancora più grosse, grossissime, nella speranza che in questo vortice di panzane si verifichi un corto circuito della comunicazione, e il mondo virtuale torni a lasciare spazio a quello reale» [61]. 0100101110101101.org e Luther creano a tavolino la vita e le opere dell'artista serbo Darko Maver. Il progetto, nell'arco di quasi due anni, coinvolge decine di persone in diverse città e culmina con la rivendicazione della beffa all'indomani della presentazione dell'artista alla 48° Biennale d'Arte Contemporanea di Venezia. Una beffa ai danni del mondo dell'arte contemporanea nella quale sono caduti numerosi dei più apprezzati critici [62]. Le raccapriccianti opere di Darko furono lette come simbolo del dramma delle violenze dell'ex-Jugoslavia e come critica alla realtà mediatica e alla strumentalizzazione delle immagini delle vittime del conflitto bellico. Nell'ansia di trovare qualcosa di nuovo da far macinare al sistema dell'arte, c'è stato chi ha anche detto di aver visto, intervistato e lanciato Maver, nell'illusione di veder anche la sua fama accresciuta. Il sistema dello spettacolo non è stato criticato da fuori ma usato per essere criticato, i suoi meccanismi ritorti contro se stesso [63]. Dai suoi stessi ideatori Maver è stato definito un cavallo di Troia, dimostrativo della permeabilità del sistema dell'arte. Il caso è indicativo del legame fra atti dimostrativi e sfiducia: l'incursione in un sistema può essere destabilizzante anche al di fuori dell'ambito informatico, la produzione artistica (in questo caso, culturale in genere) è regolata da meccanismi codificati formalmente o anche solo dalla consuetudine. La dimostrazione della fallacità di ciò in cui si crede lo delegittima tanto più profondamente quanto più la debolezza è intrinseca al suo funzionamento.

6. Interessi economici fra labilità delle distinzioni e necessità di chiarezza

A parte le dichiarazioni d'intenti, di solito avverse ai poteri economici, vi è un adagio che circola, dice che è molto più facile cambiare sponda (cioè passare a lavorare per grandi aziende o istituzioni) che finire in carcere. Ciò fornisce anche una spiegazione meno idealistica della premura a rendere note le incursioni portate a termine, nonché spiega come il dilagare del fenomeno sia stato contenuto più dalla cooptazione che dalla coercizione [64]. In occasione dell'ultimo G8 è stato presentato il Global Internet Project (GIP) [65]; in un documento relativo alla sicurezza su Internet, appoggiato da numerose lobby, si invitano i governi a lasciare che sia il settore privato a prendere l'iniziativa nella risoluzione della questione. «Se i governi sono chiamati in causa per i recenti casi di cyber-attacchi e vogliono agire per sviluppare una Internet solida e sicura per sostenere diverse applicazioni come l'e-commerce e il governo elettronico, devono resistere alla tentazione di proporre misure di regolamentazione. [...] La regolamentazione da parte dei governi nazionali non risolverà il problema globale, cosa che potranno fare le innovazioni e gli investimenti del settore privato» [66]. Ciò che chiedono alle legislazioni di definire

è l'hacking malintenzionato e di produrre leggi effettive ed applicabili. I governi sono invitati a facilitare la collaborazione internazionale sulla materia, promuovere standard aperti perché facilitano il vaglio delle soluzioni proposte, eliminare le restrizioni sulla crittografia, aprire lo scambio di informazioni fra servizi segreti e settori dedicati alla sicurezza delle imprese, investire nella ricerca in materia e nell'educazione dei giovani [67].

A parte casi eclatanti, un problema effettivo è tracciare una linea di confine chiara e formale fra «black hat hacking» e «white hat hacking» [68], in quanto le procedure e gli strumenti sono i medesimi. Gli esempi sulla labilità dei margini sono molti, per esempio il software BackOrifice scatenò molte preoccupazioni (arrivando fino ai tg di prima serata) perché permette a terzi di usare a piacimento i computer operanti con Windows, oggi la versione che lo fa visibilmente è un apprezzato software di amministrazione remota [69].

Un evento recente ha attirato l'attenzione della comunità hacker, e cioè la sfida da parte del Secure Digital Music Initiative a decifrare il suo standard di protezione [70]. Nonostante il tentativo di boicottare l'iniziativa, vista come la richiesta di servizi professionali a basso costo, nell'arco di poche settimane è stato violato un sistema costato cifre non indifferenti e molti mesi di lavoro [71].

L'accessibilità di segreti di vario genere non è passata inosservata a chi trae vantaggio dallo spionaggio, in particolare aziende e servizi segreti. Oltre alle consuete attività di intelligence, i servizi segreti americani hanno iniziato a dedicarsi allo spionaggio industriale a vantaggio delle compagnie statunitensi. Echelon, l'infrastruttura di spionaggio anglo-americana, è ormai nel mirino della Comunità Europea, preoccupata, oltre che per la sua sicurezza, da presunti casi i cui gli Usa si sono avvantaggiati illegalmente a scapito dei gruppi del vecchio continente [72]. In marzo il direttore della Cia James Woolsey ha dichiarato al Wall Street Journal che l'Europa è più arretrata tecnologicamente degli Stati Uniti e la loro attività è volta al solo controllo di eventuali truffe. Di portata certamente inferiore è la notizia, riportata da tutti i quotidiani, che hacker non identificati sono entrati nei sistemi della Microsoft e forse hanno sottratto il codice sorgente dei suoi prodotti più importanti [73].

7. Divergenza fra «natura» della Rete, consuetudini e leggi

Gli attacchi ai siti «.mil» e «.gov» (che identificano la presenza istituzionale americana sul web) sono in costante aumento. Sebbene sia più difficile fare delle stime, anche il settore economico subisce una aumento delle violazioni. Nonostante l'evoluzione del panorama, alcuni esempi storici continuano ad essere citati [74]. Riciclatori di denaro sporco, pedofili, mafie di vario genere sono abilissime ad utilizzare le nuove tecnologie [75]. Dati di questo genere non devono far dimenticare che ciò è sì reso possibile da un uso non ortodosso di Internet, ma non tutte le eterodossie/eresie possono essere ricondotte agli hacker.

La particolarità della situazione attuale è che non si è consolidato un senso di ortodossia dell'uso, e i divergenti interessi perseguiti e istanze rivendicate non fanno chiarezza. A complicare la definizione di un qualche crinale fra giusto e ingiusto ci pensano leggi frammentarie, inapplicabili, dettate da visioni unilaterali e che comunque non ottengono quel consenso necessario a renderle effettive.

Una qualunque pretesa di definizione del crimine non può essere meccanicamente dedotta dagli ordinamenti attuali, a causa dell'assenza di alcuni presupposti che non hanno consistenza in Internet e di alcune contraddizioni che la Rete evidenzia. Un'indagine giuridica o più generalmente politica non può prescindere in alcun modo dall'assenza di un'autorità sovrana riconosciuta la cui azione legislativa sia universalmente accettata, dalla mancanza di un insieme di persone che condividendo lingua, cultura e territorio possa dirsi nazione, da una cittadinanza anonima, dalla separazione dei contenuti dai supporti [76].

Il limite della stipulazione di trattati internazionali è che gli stati che non vi aderiscono non possono essere esclusi dalla Rete, se non a costi economici e sociali altissimi. Conseguenza è che esistono macchine spesso fuori da qualunque giurisdizione ma collegate a Internet come qualunque altra; pertanto chi ha ottime competenze può continuare, con qualche difficoltà in più, a fare ciò che crede,

sotto processo finiranno altri (magari usati come capri espiatori). Una soluzione sostanziale appare lontana, anche perché gli stati economicamente minori sono intenzionati a vendere cara la loro sovranità, nel momento in cui si scopre che vale tanto.

Anche l'Fbi si è accorta che non ci sono soluzioni sbrigative e ha intrapreso una campagna di formazione nelle scuole affinché insegnanti e genitori insegnino il confine fra bene e male per ciò che concerne Internet [77]. Più o meno consapevoli delle condizioni e delle implicazioni che le diverse strade percorribili comportano, gli stati stanno elaborando strategie per normalizzare Internet; gli accordi internazionali sono ovviamente la via più battuta per armonizzare le legislazioni nazionali, intensificare e rendere più efficaci le inchieste per combattere gli illeciti con metodi nuovi come la teleperquisizione e l'obbligo per i provider di tenere traccia delle informazioni sugli utenti [78]. Nel caso le tracce portassero gli investigatori fuori dai confini nazionali, l'altro stato proseguirebbe l'inchiesta. Gli interessi in tal senso sono enormi: infatti il pieno dispiegarsi del commercio elettronico e della new economy non possono prescindere dalle garanzie minime di cui il mercato necessita.

8. Un possibile livello macro: le infoguerre

Se una società dipende pesantemente dalle informazione archiviate, trasmesse ed elaborate elettronicamente, la sua infrastruttura informatica è un obiettivo appetibile per i suoi nemici. Le infoguerre non vanno ridotte ai contrasti fra opposte fazioni che ricalcano in Rete le tensioni politiche internazionali ma andrebbero considerate per l'effetto di ridefinizione della guerra che potrebbero comportare [79]. Alcune dimensioni del problema: *a)* violazione di sistemi contenenti informazioni importanti su stati (difesa, anagrafe, grandi infrastrutture) e imprese, *b)* attacchi a fini terroristici, *c)* accesso e manipolazione indiscriminati su dati personali su salute, fedina penale, risorse economiche, *d)* trasformazione delle modalità dei conflitti reali. È ormai patrimonio del genio militare controllare, manipolare, sfruttare le informazioni del nemico [80]. Raccogliere dati non è più solo un modo per padroneggiare il campo di battaglia e condurre più efficacemente il conflitto armato, ma fa parte di strategie che considerano la comunicazione come parte integrante del luogo di scontro. I piani del nemico possono essere alterati, le comunicazioni interne agli eserciti falsificate, i dati su cui vengono prese decisioni contraffatti. Secondo Richard Clarke, che coordina il Consiglio per la sicurezza delle infrastrutture e l'antiterrorismo, «non siamo più di fronte ad una minaccia teorica ma ad un dato di fatto». Il pericolo, per gli Usa, non consiste solo nel fatto di avere numerosi nemici ma di dipendere più di altri stati dalle infrastrutture di telecomunicazione [81]. Ciò che la US Air Force chiama la «digitalizzazione del campo di battaglia», promette, secondo alcuni suoi ufficiali, di colpire il nemico ai suoi punti deboli spendendo poche risorse (senza armi nucleari, chimiche, biologiche), ma con effetti anche peggiori. Teoricamente infatti è possibile paralizzare l'intera attività di un paese interferendo nell'attività delle centrali elettriche, del sistema di trasporti, della rete idrica o dei mercati telematici [82].

I costi d'accesso all'infoguerra sono relativamente bassi e non richiedono grandi eserciti [83]. Pertanto potrebbero avere l'effetto di riequilibrare le potenze mondiali; anche movimenti e gruppi particolarmente motivati possono intraprendere un'infoguerra (anche solo per acquisire visibilità), contraddicendo la teoria secondo cui il successo di un movimento dipende direttamente dalla quantità di risorse che riesce a mobilitare [84]. In ogni modo si tratta solo di prospettive (prive di capacità predittiva) che però forse per questo spaventano: l'assenza di un fronte, l'estrema difficoltà nel sapere cosa potrebbe essere colpito, da dove e soprattutto da chi, l'incertezza delle fonti fanno scivolare la guerra verso la guerriglia, in cui la paura dell'imprevedibile, la mancanza di limiti che circoscrivano l'ambito di combattimento complicano la *definizione della situazione* per tutti (militari e civili), e aggiungono elementi di guerra psicologica [85].

Sebbene lo scenario sia differente, e gli strumenti per renderlo reale si chiamino armi, i software e le procedure in questione sono in linea di massima quelli dell'hacking, pur con alcuni adattamenti. Si pone la questione della responsabilità (anche solo morale) di chi ha sviluppato i programmi in oggetto. Più che trarre conclusioni vale la pena sottolineare alcuni aspetti: qualunque software (per quanto non neutro) ha una gamma di impieghi molto ampia, che spesso il programmatore non può immaginare; le potenzialità sono legate alla diffusione e all'impiego di una tecnologia «bacata»; le violazioni dei sistemi informatici sono così efficaci perché il software (in particolare i sistemi operativi) hanno molte falle e ciò è dovuto all'ansia di uno sviluppo affrettato; la scelta delle soluzioni informatiche e dei tecnici per obiettivi a rischio

potrebbe essere più meticolosa.

9. Un medium «aperto»: humus per ecosistemi fortemente intrecciati

La stessa natura aperta di Internet, che la rende un medium utile e plasmabile, è la causa della sua debolezza [86]. Gli hacker analizzano le tecnologie e scovano i difetti, li rendono pubblici, gli sviluppatori trovano rimedi e li pubblicano, addetti alla sicurezza e amministratori di sistema aggiornano (almeno dovrebbero) [87]. Il meccanismo è innescato da anni e ha contribuito all'affinamento dei sistemi. La pubblicità dei buchi permette anche ad altri di sfruttarli, per fini propri. Qualcuno scopre che il tal sistema operativo ha un bug, qualcun altro (ad esempio un funzionario cinese) scopre che il suo nemico giurato (governo di Formosa) lo impiega (magari per gestire la borsa valori) e lo sabota. Stessa cosa accade da parte di attivisti contro multinazionali o regimi, il giudizio di bene-male non altera il meccanismo.

Più volte, su questioni analoghe, si è posto l'accento sull'interconnesione di realtà precedentemente distinte. Si tratta senz'altro di un aspetto rilevante, però la peculiarità sta nel fatto che nel mondo dell'economia globale si usano ovunque le stesse tecnologie (per gli usi più disparati) con i medesimi difetti e rischi (in questo caso tecnici, non culturali). Sarebbe un errore valutare solo una componente del fenomeno senza considerare l'insieme di relazioni in cui è immerso, senza vedere gli equilibri presenti e le funzioni svolte. Attraverso gli anni si è costituita una sorta di ecologia o quantomeno di catena alimentare in cui togliere un anello (ammesso sia possibile) può causare effetti imprevedibili. Infatti finché molti dei tecnici migliori seguono l'etica hacker, è probabile che i difetti più pericolosi vengano pubblicamente conosciuti [88]. Si può pensare di incorporare l'hacking nella ricerca, ma sebbene ciò sia consueto sia nel settore pubblico che privato il fenomeno non si esaurisce anche perché serpeggia una forte sfiducia verso i poteri statali ed economici [89]. Il volto attuale di Internet, luogo dove l'insicurezza va di pari passo alla facilità con cui si possono far circolare contenuti di ogni genere, è effetto anche dell'hacking.

Come conciliare la tensione idealistica verso un'appropriazione generalizzata delle tecnologie con l'effettiva settorialità della gran parte del fenomeno? Una prima risposta è che le ricadute dell'hacking vanno al di là degli attori che se ne interessano in prima persona. Approfondendo la questione si potrebbe abbozzare un'analisi antropologica in cui l'etica della distribuzione delle conoscenze acquisite è la prima leva per innescare quel meccanismo di assenza di scarsità che impedisce il costituirsi di organizzazioni gerarchiche in grado di controllare la distribuzione sociale di tali conoscenze. La consapevolezza più o meno implicita dell'intrinseco potere (e responsabilità) che danno queste informazioni può essere la forza latente che ha spinto a costituire l'etica hacker così com'è, particolarmente attenta allo scambio reciproco non mediato da meccanismi quali il mercato. Una necessità di adattamento alla situazione (se non all'ambiente) che contemporaneamente ha garantito il fenomeno nel suo insieme e la sua incoercibilità da parte dell'ambiente esterno, spesso ostile, nonché ha impedito che qualcuno potesse acquisire un potere poi incontrollabile. Del resto la ragione dell'enfasi con cui ci si riferisce alla pubblicità dei saperi, e la conseguente allocazione di prestigio che gode chi si prodiga per la comunità, va probabilmente cercata in cause più pressanti di un idealismo o della ricerca di ampi guadagni. Anche se non molto formalizzata, l'attività hacker non è un'ingenua difesa di principi né un brigantaggio contemporaneo ma l'autodifesa di una subcultura che contemporaneamente è funzionalizzata alla società dell'informazione ma ne è anche antitesi critica.

Una particolarità dell'hacking è di aver acquisito un potere senza passare per gli iter economici e istituzionali consueti e di esercitarlo senza che individui si costituiscano in attori corporati. L'autoregolazione di tali gruppi, in cui l'individualismo è un tratto culturale, passa per un'etica e non per norme esteriori, mancando spesso la coercibilità. In questa situazione si pone la questione attuale dell'anomia, e delle vie di evoluzione percorribili. Intrecciatasi alle smagliature della società dell'informazione, non ne rileva solo le debolezze ma propone un suo insieme di orientamenti di evoluzione. Chi opera nel rispetto dell'etica hacker esplora alcune «leggi naturali» del ciberspazio, e evidenzia come sia un ambiente in cui non solo i segni ma anche le azioni, possano essere significative.

[1] Non si vuole qui polemizzare con il modello comunicativo adottato (in linea di massima) dai mass media, che tratta un tema quando un fatto eclatante lo solleva. Ciò trovo sia soprattutto dovuto alle caratteristiche in sé di questo genere di media e dal modo di fruirli che si è diffuso. Rimane il fatto che, se da una parte pare essere l'unico modo di interessare o sensibilizzare la pubblica opinione (nonché di allargare l'audience), dall'altra confonde la parte per il tutto. Una parte che, essendo degna di nota, non è esemplare.

[2] Dichiarazione di Richard Shaeffer, direttore dell'ufficio di sicurezza informatica del Pentagono, riportata da Wired News dell'8 agosto 2000. Nemmeno i dati forniti dal settore pubblico sono completamente attendibili, anche perché manca una definizione precisa di cosa sia un attacco e cosa no. L'ampio margine entro cui non si può essere accusati di mentire, permette di dichiarare dati in relazione agli interessi particolari (per ottenere più fondi e leggi più restrittive oppure a dimostrazione del buon lavoro svolto); fatto ben possibile su temi di sicurezza nazionale.

[3] In linea di massima gli hacker sono appassionati di varia estrazione, ricercatori ed esperti di sicurezza informatica. Le pratiche che li caratterizzano hanno come principale gradino d'accesso la conoscenza della materia. Passa pertanto in secondo piano la composizione sociale, anche se ovviamente avere un accesso ad Internet e tempo non sono beni a disposizione di tutti.

[4] Si ricordi che la gratuità non implica l'assenza di fini commerciali; nel mercato delle merci aveva un ruolo marginale, mentre nell'economia legata a Internet è diffusissima per aumentare il numero dei propri utenti, che sono la ricchezza potenziale di un servizio.

[5] Iniziative come OpenContent (http://www.opencontent.org) e OpenCulture (http://www.openculture.org) o il meccanismo di commercio elettronico "Street Performer" (http://www.counterpane.com/street_performer.html) propongono strade per mantenere pubblicamente disponibili i contenuti e permettere a chi li produce di ottenere compensi. Strade più "tradizionali"

potrebbero essere, e in parte sono, la pubblicità, la tassazione dei supporti, i finanziamenti pubblici.

[6] «Wreader» è un gioco di parole fra «writer» e «reader» introdotto da Landow, teorico degli ipertesti, che con questa parola vuole esprimere lo sfumare dei confini di ruolo fra autore e lettore in relazione alla scrittura elettronica, in particolare ipertestuale.

[7] Nel 1986, l'8 gennaio, «The Mentor», hacker americano, diviene celebre scrivendo il Manifesto degli Hacker:

" [...]Ora è questo il nostro mondo, il mondo dell'elettrone e dello switch, la bellezza del baud. Noi usiamo gratuitamente servizi già esistenti che non costerebbero nulla se non fossero controllati da approfittatori, e voi ci chiamate criminali. Noi esploriamo e ci chiamate criminali. Noi cerchiamo conoscenza e ci chiamate criminali. Noi esistiamo senza colore di pelle, nazionalità, credi religiosi e ci chiamate criminali. Voi costruite bombe atomiche, finanziate guerre, uccidete, ingannate e mentite e cercate di farci credere che lo fate per il nostro bene, e poi siamo noi i criminali. Sì, io sono un criminale. Il mio crimine è la mia curiosità. Il mio crimine è giudicare le persone per ciò che dicono e pensano, non per l'apparenza. Il mio crimine è di essere più intelligente di voi, per questo non mi perdonerete mai. Io sono un hacker e questo e' il mio manifesto. Potete anche fermare me, ma non potete fermarci tutti." Il manifesto completo si trova presso http://www.virtualadept.co.uk/manifest.html

[8]Senza approfondire il discorso, qui si può notare come darsi all'hacking significhi «fare sul serio», rischiare veramente qualcosa e non solo la popolarità del proprio avatar in un ambiente simulato o il nickname in una chat. Ciò dovrebbe far venire qualche dubbio nel sostenere che la Rete (creando un'«iperrealtà», una realtà più vera del vero) stia perpetrando il «delitto perfetto», lo «scambio simbolico» fra reale e simulato (riferimento al pensiero di J. Baudrillard). Il postmoderno (inteso come clima culturale nel quale non c'è realtà al di fuori di narrazioni e interpretazioni) non rende conto che proprio nell'universo fatto di segni, completamente artificiale, simulato dalle espressioni e dal credito loro concesso, il fare e la capacità di ottenere concretamente risultati è spesso ciò che fa la differenza. La maggior parte delle figure eroiche (nel bene e nel male) che le comunità hacker e il popolo della Rete riconoscono sono persone che sono riuscite ad imporre la loro visione con la forza dei fatti, non retori. La valutazione strettamente pragmatica delle azioni, di stampo fortemente statunitense, permea gli ambiti più diversi: dalla new economy al popolo di Seattle, dagli hacker alle comunità virtuali.

[9] Un virus è un piccolo programma che si copia in un altro e lo modifica, si attiva assieme al software infetto replicandosi e producendo spesso effetti indesiderati. Un worm è un programma che assorbe risorse rallentando o bloccando una rete, e/o che causa la perdita di dati.

[10] A parte le allarmate dichiarazioni ufficiali delle case produttrici di software, c'è un certo accordo sul fatto che la pratica del cracking apra mercati altrimenti stagni. Frequentemente un programma nuovo che vuole scalzare i concorrenti affermati adotta protezioni facilmente violabili; stessa cosa a livello macro: nei paesi poco informatizzati il cartello dei produttori di software fa solo pressioni di circostanza sul rispetto della proprietà intellettuale, aspettando che l'informatica si diffonda abbastanza da non poterne fare a meno; poi si solleva il polverone di mancati introiti enormi e si invocano leggi severe. In Italia è successo negli ultimi dieci anni (culmine l'ultima legge sul copyright), in Sud America sta avvenendo.

[11] Nelle analisi più favorevoli, i criptoanarchici (manifesto: http://www.spunk.org/library/comms/sp000151.html) sono stati visti come la controparte all'invisibilità del potere, la congiura di palazzo contro i poteri che non rendono conto del proprio operato; «arcana seditionis» come reazione alle «arcana imperii». Trovo però più verosimile vederli come proponenti di una risposta concreta (e per molti aspetti estremamente efficace) all'oggettivo problema dell'erosione della privacy. Del resto, come fa notare fra gli altri Norberto Bobbio in *Stato, governo, società*, non siamo stati mai così visibili al potere. A proposito dell'importanza di strumenti di crittografia si ricordi che la decifrazione del Codice Enigma facilitò la vittoria alleata della Seconda Guerra Mondiale e che tuttora gli Usa considerano la crittografia superiore a 128bit un'arma da guerra.

[12] *The Difference between Hackers and Crackers* è un testo di CandyMan, reperibile in Rete e che

gode di un certo credito.

[13] *La comunicazione al computer* Paccagnella L., Il Mulino, Bologna, 2000, cap. 8, § 2

[14] Rispetto al controllo della corrispondenza elettronica, Carnivore è un software sul cui uso illegittimo da parte delle autorità statunitensi è stato chiamato a rispondere il ministro della giustizia; il governo brittanico ha autorizzato con il Regulation Investigatory Powers i propri servizi segreti a controllare tutte le e-mail. A proposito del possesso di programmi va ricordato che il consumatore non acquista un software ma solo la licenza d'uso. La Microsoft è stata ripetutamente portata in tribunale con l'accusa di aver fatto leva sulla diffusione del suo sistema operativo per diffondere altri suoi prodotti, violando le norme della libera concorrenza. Per quanto riguarda le comunità virtuali, fa parte delle strategie dei fornitori di servizi commerciali cedere l'attenzione di utenti dai gusti simili a commercianti di beni e servizi.

[15] La maggior parte dei siti non è indicizzata nei motori di ricerca. Quelli che vogliono rimanere per pochi sono semi-nascosti, cambiano di frequente indirizzo e non sono pubblicamente accessibili. Non è comunque difficile trovarne che forniscano informazioni minuziose su come accedere ai sistemi in rete, telefoni cellulari, telefoni pubblici e decodificatori per la Tv via cavo o satellite. Per farsi un'idea è sufficiente visitare: http://www.bismark.it; http://neworder.box.sk o http://www.hackertronics.com (sito di commercio elettronico). Ci sono persino numerosi libri, come per esempio *The hacker's handbook* di Hugo Cornwall e *Secrets of a Super Hacker* scritto da un fantomatico hacker che si fa chiamare Knightmare. La maggior parte dei siti avverte di parlare di conoscenza, non di vandalismo. Che ciascuno sia responsabile di se stesso è una convinzione tanto diffusa da essere uno dei tratti culturali dei corsari telematici.

Tra i siti di vocazione più politica prevalgono gli anarchici che reclamano l'eguaglianza tra tutti i pirati della Rete e l'assenza di ogni gerarchia. L'underground è altrettanto refrattario al potere ma meno ideologizzato.

[16] Un cavallo di Troia è nome metaforico per un software che si fa entrare in un sistema nascosto in dati autorizzati e che dall'interno dà accesso a operazioni altrimenti impossibili.

Esiste un gergo hacker non solo per indicare gli aspetti tecnici ma che rispecchia un'intera subcultura e che è significativa perché è una delle prime nata e sviluppatasi esclusivamente attraverso le reti telematiche (in particolare Internet e Bbs). Il «Jargon File» è una specie di dizionario dello slang utilizzato da tali comunità.

[17] I buchi sono i cosiddetti «bug». Per vedere l'effetto di un bug (se si usa Windows 9x), salvare tutto, chiudere le applicazioni ed eseguire: «nul\nul» o «con\con», vecchie chiamate Dos che mandano tutto il sistema in crash. Facendo eseguire questo comando da un attachment, da un semplice script...

Un esempio di cattiva amministrazione: utilizzando uno scanner scaricato dalla Rete un giovane «smanettone» alle dipendenze di una grande azienda del nord, ha scoperto ben cinque «buchi» sul sito della Polizia di stato. Non diversamente i telefoni Gsm: il loro protocollo (cioè l'insieme di regole che definiscono la comunicazione) è proprietario, quindi è distribuito solo a fornitori, produttori di hardware... La conseguenza è che i Gsm sono stati un banco di prova per gli hacker e i programmi per clonarli sono facilmente reperibili. Negli Usa ogni anno i danni dovuti alla clonazione nella telefonia mobile, si aggirano sui 650 milioni di dollari.

[18] Il sito del Cert è http://www.cert.org

[19] I cui siti sono rispettivamente: http://www.2600.com, http://www.ccc.de.

[20] Verso la fine del 1999, un gruppo di hacker norvegesi analizzando il flusso dei dati è risalita alle specifiche del protocollo ed è quindi riuscito a violare l'algoritmo di crittografia CSS, producendo DeCSS, un programma in grado di decifrare il contenuto dei Dvd. La questione non è marginale come potrebbe sembrare in quanto il Dvd è il formato che, nelle intenzioni delle multinazionali dell'audiovisivo, veicolerà la maggior parte dei contenuti nel prossimo futuro. Per dare un'idea dell'importanza degli standard basti

ricordare che la spartizione del mondo secondo gli standard televisivi (Pal, Ntsc, Secam...) ha diviso il mondo in aree di «influenza mediatica».

La MPAA (Motion Picture Association of America) ha portato in tribunale il sito 2600 per aver reso disponibile il DeCSS e numerosi link a siti che avevano messo a disposizione il programma.

[21] Non sono mancate le polemiche sulla modalità secondo cui si sono svolte le elezioni dell'Icann@Large (estate 2000). In area europea è arrivata seconda una ricercatrice di scienze politiche dell'università di Berlino, da tempo sensibile ai temi dell'autogoverno della Rete.

[22] Il simbolo si rifà alla casa discografica dei Beatles, al mondo agreste, a Newton e al peccato originale. «Il radicalismo dell'epoca era un miscuglio piuttosto vago di idee sinistrorse […], di buddismo Zen, di ecologia della sopravvivenza, di rock ed elettronica, di fantascienza mescolate al desiderio di un ritorno alle origini» da Breton P. (1992), *La storia dell'informatica*, Cappelli, pag.213

[23] idem, pagg. 205 e seguenti

[24] L'Italian Crackdown è l'iniziativa giudiziaria intrapresa in Italia nel 1994 contro le prime reti telematiche amatoriali (che si avvalgono solo delle linee telefoniche, senza le infrastrutture dedicate di cui si avvale Internet) arrivando fino al sequestro del nodo centrale di Peacelink (associazione pacifista di volontariato dell'informazione). A detta di molti l'operazione venne portata avanti con incompetenza sulla materia e in violazione di numerose norme da parte della magistratura. La vicenda è documentata da Giubitosa C., *Italian Crackdown*, Milano, Apogeo.

[25] Per curiosità, si può cercate «user.dat» o «admin.dat» sui motori di ricerca più utilizzati. Non è raro incappare in elenchi aggiornati dei sistemi peggio amministrati, che quindi meglio si adattano a fare da ponte per altri attacchi.

[26] Questo è il genere di attacco subito da Yahoo!, eBay.com, Cnn e altri, nella inverno 2000 e che ha suscitato tanto clamore a livello mondiale. Per mezzo di moltissimi computer usati come ponti/amplificatori i bersagli sono stati inondati da richieste di informazioni, finché si sono bloccati per sovraccarico. Si tratta di una tattica poco apprezzata in quanto si basa sulla banale "forza bruta" e non sull'arguzia, che tanto esalta gli animi degli hacker. Per inciso ricordo che le polizie di mezzo mondo hanno scovato il colpevole: "Mafiaboy", un quindicenne canadese che dopo un mese si stava ancora vantando della sua impresa. Volendo fare una piccola prova sul proprio computer basta (dopo aver salvato tutto) far partire un programma, mentre questo si apre farne partire rapidamente un altro, poi un altro e così via. Per quanto potente sia il calcolatore dopo un po' va in crash.

[27] Giova ricordare che i dati non seguono percorsi lineari dal mittente al destinatario, che per scrivere a un concittadino inviamo pacchetti di dati che magari attraversano mezzo mondo (molto probabile è che passino per gli Usa, siccome l'infrastruttura della Rete mondiale tende ad avere forma di stella, al cui centro si trovano appunto gli Stati Uniti). Ciò aggiunge un problema alle legislazioni, che dovrebbero considerare anche i server intermedi, di differenti paesi, che ricevono e ritrasmettono.

[28] Questa è una prospettiva sensibile agli effetti perversi, la cui sopravvalutazione è tipica del pensiero conservatore (Hirshmann). Il mondo degli hacker non è fortemente politicizzato e inoltre è difficile inquadrarlo nella griglia classica, soprattutto europeo-continentale. Qualche assonanza in più la si può rilevare con le disposizione politica anglosassone. Le istanze di parificazione, almeno in Rete, e l'avversione per il potere delle grandi compagnie li avvicina ai democratici ma il radicale rifiuto per l'ingerenza dei poteri forti li porta verso le due varianti dell'anarchismo, fortemente individualista o comunitario. In Europa (e in Italia in particolare) acquista maggiormente un colorito politico: si muove fra movimento «alternativo» e organizzazioni in difesa diritti civili, dei consumatori, dei cittadini.

[29]La massima «tutto ciò che può essere automatizzato dovrebbe esserlo» calza tanto a questo ambito come a quelli che pensano di trarre solo vantaggi dell'informatizzazione. Un automatismo sottrae agli atti consapevolezza, competenze, la necessità della cognizione di causa, attenzione, intenzionalità e immaginazione. Considerazioni del genere hanno perso di incisività, annegate nella retorica che spesso le circonda e spesso associate a un ideale (anche solo sotteso) purezza delle origini o del passato. Si

apprezzano le macchine perché svolgono i compiti ripetitivi senza sospettare che la ripetitività di molti compiti è dovuta ad automatismi o razionalizzazioni di origine precedente.

Sicuramente si è a un punto di non ritorno, non tanto perché si è percorsa troppo questa strada (in quanto il troppo non avrebbe punti di paragone saldi) quanto perché si è instaurato un circolo, virtuoso o vizioso dipende dal giudizio, fra sviluppo e automazione. Una società che vive di continue innovazioni, del continuo generare scarto (quindi vantaggio) non è più segnata dalla velocità, tipica dell'era industriale (macchine, trasporti di uomini e merci fra continenti...) rispetto a quella agricola, ma dall'accelerazione. Per aumentare sempre l'andatura l'unica via percorribile è delegare alle macchine tutto ciò si può, per spostare il focus dell'attenzione sul nuovo. Questo meccanismo, più che altri, penso sia motore della riduzione di quanti più processi (tecnici, sociali) possibile ad automatismi. La prospettiva non è però la "gabbia d'acciaio" che Weber (pensando alla burocrazia) temeva avrebbe imprigionato la società, in quanto la crescita non procede linearmente, non ci sono ambiti e processi che sono e rimarranno pura amministrazione, se esigenze ritenute prioritarie richiedono cambiamenti.

[30] «Individuals are expected to be highly self-motivated, but not selfish»

[31] Due gruppi molto conosciuti sono Attrition (http://www.attrition.org) e Rtmark (http://www.rtmatk.com). Oltre a newsgroup, mailing list e canali di comunicazione privati, http://www.antionline.com e http://www.hackernews.com sono due fonti di informazioni continuamente aggiornate sul panorama hacker.

[32] Diluire le responsabilità non andrebbe letto come una qualunquista intenzione di non rispondere del proprio operato ma come una modalità per «aprire» un ambito di attività che altrimenti sarebbe sviluppato con ben maggiori difficoltà, anche in relazione alla perseguibilità dei soggetti.

[33] C'è una leggenda secondo cui alla decisione del governo britannico di autorizzare le intercettazioni online ai servizi segreti, l'underground ha replicato prima gettando in Rete il virus «I love you», poi annunciando una sfida planetaria per il 1° maggio, che doveva trasformarsi nella prima giornata anticapitalista online della storia. Mettendo da parte la inverificabilità di storie del genere (che chiunque può essersi inventato a posteriori), ciò che colpisce è la frequenza con cui ci si imbatte in miti analoghi; storie che non sussistono per un loro valore di verità ma per l'immaginario che contemporaneamente sottendono e riproducono. Un'analogia con quelle che Walter Ong (in *Oralità e scrittura*, Bologna, Il Mulino, 1986) chiama società orali.

[34] I meeting più conosciuti sono Hope (Hackers Of Planet Earth, http://www.hope.net) organizzata da 2600: The Hacker Quarterly, Hackit (http://www.hackmeeting.org) in Italia e Spagna, Hacking in Progess (http://www.hip.nl) in Olanda. Età media sotto i trent'anni e poche le donne.

[35] Kevin Mitnick (http://www.kevinmitnick.com), detto il «Condor» è uno dei più famosi hacker di tutti i tempi, arrestato nel '95 (dopo un duello con un fisico giapponese) dopo quattordici anni di hacking, fughe e latitanze. Ha dichiarato: "dire a un hacker che qualcosa non può essere fatto comporta per lui l'imperativo morale di provare".

A fine ottobre 2000 i migliori esperti di sicurezza dei paesi più industrializzati si sono incontrati a Berlino, facendo il punto della situazione. (Wired News del 24 Ottobre 2000)

[36] «Cultura è una serie di meccanismi di controllo (progetti, ricette, norme, istituzioni: ciò che gli informatici chiamano programmi) per il governo del comportamento» Clifford Geertz.

[37] In Wiener N. (1950) *Cibernetica e società* non si cerca di fondare una nuova scienza ma di coordinare questioni che si trovavano in una «terra di nessuno» fra i diversi settori tradizionali. «L'informazione è un mezzo usato per trasmettere un messaggio, mentre la comunicazione, per i cibernetici, è praticamente una finalità, un fine in se stesso. L'informatica diventava, quindi, una tecnica di manipolazione dell'informazione, là dove la cibernetica si impegnava invece in una riflessione sulle finalità dell'uso delle varie tecniche nel mondo moderno».

«L'ideale prospettato da Wiener era di una società in cui l'informazione circolasse liberamente, dove

vivere significasse realmente disporre di un'informazione adeguata, in cui la vita consistesse in una partecipazione a quella corrente continua attraverso la quale viene scambiata l'informazione e dove le influenze del mondo esterno si combinassero con gli atti che permettono di intervenire su di esso. Ora tre sono le caratteristiche della nostra attuale società che si oppongono alla concretizzazione di questo ideale: la pratica del segreto, gli equivoci o le incomprensioni dovute all'ineguale accesso dei vari utenti all'informazione, la trasformazione dell'informazione stessa in merce. » (Breton, 1992, p.143 e 156).

[38]Chiaramente la questione qui affrontata non si limita ad un discorso sui mezzi di propaganda o di ricerca del consenso, ma più ampiamente a tutti i dati che riguardano la popolazione, l'attività degli organismi di potere; tutti le informazioni, quindi, che abbiano una qualche rilevanza sociale.

[39] Esempio «storico» è del 1984, quando il Chaos Computer Club di Amburgo si muove contro un sistema sviluppato dalle poste tedesche e IBM per comunicazioni personali e prenotazione di merci e servizi (intanto il governo tedesco lanciava l'iniziativa, poi sostanzialmente fallita, del censimento informatizzato di tutti i tedeschi). Risvegliata la paura del Grande Fratello, per far fallire il progetto il CCC inventa una beffa ai danni di una cassa di risparmio di Amburgo facendosi versare, attraverso il suddetto servizio, 135000 marchi. Rende subito pubblica la vicenda, dichiarando che non era intenzionato a ritirare il denaro, visto che il fine dell'azione era solo di rendere note le gravi lacune presenti nel servizio. Il caso suscita grande clamore in tutta la Germania, facendo fallire in maniera definitiva il progetto, mostratane l'intima fragilità.

[40] Molti hacker attuali potrebbero riconoscersi nel manifesto programmatico pubblicato alla fine del '99 da Emmanuel Goldstein, editore di 2600: The Hackers Quarterly: «Quello che ci accomuna è la consapevolezza che la libertà di espressione è il bene più prezioso. L'individualità è un patrimonio insostituibile e Internet, che fu sviluppato con uno spirito da hacker, è lo strumento più importante per coltivare entrambi». Ma avverte: «Una cosa da cui ci dobbiamo guardare bene è l'attuazione di un crimine. É facile per un hacker ottenere denaro attraverso il furto di password, calling card, numeri di carta di credito e la clonazione di telefoni. Ma una volta entrati in questo circolo vizioso, lo spirito di avventura e curiosità per le nuove tecnologie che ci contraddistingue muore per sempre per dar posto all'avidità. Sta a noi il compito di fare in modo da non ritrovarci inquinati da queste pratiche. Sta ai nostri nemici, invece, mostrare che lo siamo».

[41] Andy Mueller-Maguhn intervistato da Wired, 19 ottobre 2000

[42] Sebbene abbia riscosso reazioni contrastanti, si ricordi che alcuni hacker sono stati fra i primi a denunciare l'uso della Rete per far circolare materiale pedo-pornografico e che inoltre alcuni gruppi di hacker collaborano con le forze di polizia.

[43] Steve M. (1997), *Old and New Hacker Ethics*. Reperibile presso http://www.infowar.com.

[44] Il termine «trust» ha nel mondo anglosassone una connotazione molto più forte che in italiano, riferendosi anche al patto sociale, fondativo della società.

[45] Senza scendere nello specifico, basti qui ricordare che i sistemi di crittografia a doppia chiave si basano su una chiave pubblica e una privata. Servono entrambe per cifrare o per firmare univocamente un messaggio.

[46] L'ideale di un'autogestione dello sviluppo ha valicato le componenti tecniche, interessando disparati ambiti della Rete.

[47] Riferimenti sono, rispettivamente la Free Software Foundation (http://www.fsf.org) e l'Open Source Movement (http://www.opensource.org).

[48]Un punto di riferimento per il cosiddetto "hacktivismo" è la mailing list hacktivism@tao.ca, il cui archivio è online presso http://hacktivism.tao.ca

[49]Sebbene il risultato sia analogo ad un attacco «smurf» (quello che produce un'interruzione del

servizio), le modalità sono significativamente diverse in quanto nel primo uno o pochi moltiplicano la propria forza usando computer-ponte di utenti inconsapevoli, mentre nel secondo la forza è data solo dal numero effettivo dei partecipanti. I sostenitori hanno ricordato che se bastano pochi click per comprare, votare… devono bastarne pochi anche per dissentire.

L'uso del netstrike sta divenendo alquanto popolare. Nel mese di ottobre sia il comune di Milano che quello romano sono state vittime di scioperi analoghi. Il primo per lo sgombero di alcuni spazi occupati, l'altro per aver rimosso il testo *Lasciate che i bimbi* di Luther Blissett regolarmente in vendita nelle librerie. Come sempre in casi analoghi, il testo rimosso ricompare ovunque sulla Rete con visibilità maggiore.

Un esempio di azioni ancora più dirette si è verificato a Berlino, dove una completa mappa degli immobili in disuso è stata copiata dal catasto e recapitata agli squatter.

[50]C'è un sentimento ambivalente verso l'opinione pubblica. Da un lato è apprezzata perché è forma di pressione diretta, dall'altro si diffida a causa della sua mutevolezza che quindi mina i risultati. Il sito di Indymedia è http://www.indymedia.org

[51] Argan G. C. (1989) *L'arte moderna*, Firenze, Sansoni, pag. 326

[52] Riferimento al pensiero di Walter Benjamin in Vattimo G. (1997) *Tecnica ed esistenza*, Torino, Paravia, pag.92

[53] Argan, 1989, pag. 327.

[54] Che ricorda il «wit», tanto apprezzato dai dandy inglesi fine ‘800 di cui Wilde era esponente.

[55] Piro N. (1998), *Cyberterrorismo*, Roma, Castelvecchi racconta minuziosamente il dirottamento digitale, significativo nel momento in cui si vaneggiava che la distorsione della realtà da parte dei media sarebbe svanita ad opera di un medium punto a punto che avrebbe permesso agli attori sociali di rappresentare se stessi senza intermediari. Altra testimonianza del dirottamento è reperibile in http://www.hijack.org.

[56] Il sito Etoy è http://www.etoy.com è stato tra l'altro oggetto di battaglie (legali e a colpi di netstrike) con la Etoys.com, supermercato on line di giocattoli che prima degli acquisti natalizi del 1999 voleva sgombrare il campo da equivoci. La sconfitta dell'azienda è documentata presso http://www.toywar.com.

[57]Ha cadenza annuale, si tiene presso il Museo di Arte Contemporanea di Linz, Austria. Sito: http://www.aec.at

[58]A metà anni '90 l'utenza era ancora prevalentemente maschile.

[59]Fra i vari siti su Luther Blissett si segnala: http://www.pengo.it/luther. Luther Blissett è autore di numerosi testi, fra cui *Q* edito da Einaudi, *Mind Invaders* e *Lasciate che i bimbi* Castelvecchi, *Toto, Peppino e la guerra psichica* arrivato alla seconda edizione. *Net.gener@tion* di Mondadori, frutto di una burla ad autore ed editore, è stato invece ritirato dal mercato.

Rilevante inoltre il fatto che “formalmente ” lo scopo non è sollevare la questione della dicotomia individuo-gruppo ma risolverla, essendo problemi che è la società a creare.

[60] Da uno dei manifesti del Luhter Blissett Project.

[61] Blissett L. (marzo 1995) *La leggenda metropolitana di fine millennio* in *Derive Approdi* n°5.

[62] Tra i quali Achille Bonito Oliva, Renato Barilli, Jean Clair, Harald Szeemann, Francesca Alfano

Miglietti e coniuge, Maurizio Calvesi, Paolo Vagheggi e Giancarlo Politi.

[63] Parlando del fatto con una organizzatrice di mostre, mi ha colpito lo stupore con cui ha appreso il fatto che Maver fosse stato ritirato, gesto che, mirando a insabbiare l'accaduto, gli ha dato più valore e risonanza. Al contrario lasciarlo partecipare lo avrebbe assorbito nel sistema dell'arte che avrebbe dimostrato di saper valorizzare gesti significativi. Il materiale relativo al caso Darko Maver è reperibile all'indirizzo: http://www.0100101110101101.org/maver

[64] Sull'onda dell'entusiasmo per l'outsourcing e la piccola impresa chi ha voluto mettersi in regola senza rinunciare all'autonomia ha fondato i cosiddetti tiger team, gruppi di consulenza che mettono alla prova i sistemi dei clienti.

[65] http://www.gip.org

[66] Testo integrale presso: http://www.gip.org/publications/papers/gipwp0500.asp.

[67] Fino a pochi anni fa sarebbe stata impensabile una tale convergenza del settore privato verso le scelte fatte a suo tempo dall'underground, in particolare al riguardo di tecnologie aperte (quindi pubblicamente testabili e discutibili) e della crittografia «robusta». Da menzionare anche Publius software, sviluppato dai laboratori di ricerca dell'AT&T (la maggiore compagnia telefonica statunitense), che garantisce l'anonimato sulla Rete. Le dichiarazioni dei ricercatori, che probabilmente fino a qualche anno fa sarebbero state tacciate di internazionalismo proletario, oggi sono ben accette anche alle multinazionali, fiduciose di poter, con simili strumenti, aprire nuovi mercati dove oggi dominano dittature.

[68] In Italia solitamente si distingue fra buono e malizioso.

[69] BackOrifice è opera del 1998 del gruppo The cult of the death cow, scaricabile presso http://www.bo2k.com. Vietare software dedicato alla security sarebbe un po' come vietare le armi improprie (coltelli) senza considerare la loro duplicità.

[70] L'SDMI (http://www.sdmi.org) è un consorzio di industrie discografiche per lo sviluppo di sistemi anti copia per la musica in formato digitale, per evitare la continua violazione della proprietà intellettuale da parte degli utenti di Internet. La sfida è stata lanciata a metà settembre da http://www.hacksdmi.org.

[71] Si conferma, anche in questo caso, che la protezione sicura non esiste (e che probabilmente non può esistere) e che la migliore protezione contro la pirateria è la diminuzione dei prezzi, rendere ciò il costo marginale di copia uguale o più alto di quello d'acquisto; in questo caso a vantaggio degli ascoltatori ma con ricadute positive per tutti i consumatori dei mercati di contenuti (quindi anche editoria elettronica e cinematografia) i quali sono chiamati a trovare modelli economici adatti ai media digitali.

[72] Ovviamente non si dispone di dati ufficiali ma pare che le basi di intercettazione, collocate in Usa, Gran Bretagna, Nuova Zelanda e forse centro-sud America, siano in grado di monitorare tutto il traffico (telefonia, Internet, fax...) che transita sui satelliti.

[73] Il codice sorgente è il programma come è stato scritto dai programmatori, successivamente viene compilato, cioè tradotto in codice binario per essere eseguito da un computer. Sottrarre i sorgenti di Windows, Office... permette di comprenderne il funzionamento, la logica, i difetti; cosa impossibile dal codice binario. Il rilascio dei codici sorgenti è una delle principali differenze fra le aziende di software che vivono sul diritto d'autore e il free software che invece li lascia consultabili, utilizzabili e migliorabili da chiunque.

[74] Come lo sconosciuto russo che nel 1994 sottrasse 10 milioni di dollari alla Citibank, a conferma del fatto che i cardini della situazione non sono cambiati.

[75] Il colonnello della Guardia di Finanza Cosimo Sasso ha avvertito: «Le organizzazioni del riciclaggio sono in grado di far girare per via telematica la stessa somma di denaro per 72 volte». La Repubblica,

28 aprile 2000.

[76] A proposito dell'anonimato (o anche pseudonimato, plurinomato...): Mitnick, ora consulente e talvolta ascoltato dal Congresso degli Usa, ha sostenuto la necessità di mettere a punto un database basato sul Dna per evitare il furto delle identità digitali, furto che oggi può avere conseguenze pesanti per le vittime. «Credo che il governo debba creare qualche forma di database che utilizzi identificativi biometrici per accertarsi dell'identità. Questo può portare ad una drastica riduzione del furto di identità digitale». Ha però avvertito che nessuna tecnologia può mettere al riparo da attacchi basati su quella che definisce «ingegneria sociale» dell'hacking, quella persuasività che consente ad un hacker esperto di ottenere informazioni riservate da chi ha accesso a quelle informazioni, semplicemente inducendo quest'ultimo a ritenere che fornire quelle informazioni sia essenziale e urgente.

[77] Il 48% degli studenti delle scuole elementari e medie statunitensi - spiega un sondaggio riportato dalla Cnn - non ritiene che ci sia nulla di sbagliato nella pirateria informatica. Il problema di fondo rimane: l'uso deve adeguarsi alle leggi o le leggi all'uso? Tanto più che le consuetudini attuali danno corpo ad alcuni diritti civili fondamentali che non troverebbero più spazio se gli utenti perdessero l'anonimato o se la proprietà intellettuale si affermasse con rigore.

[78] La «teleperquisizione» consisterebbe nel perquisire con discrezione per via telematica i computer dei sospetti, in modo da ottenere le prove necessarie ad un'eventuale accusa. Contro questa proposta del Consiglio d'Europa non hanno tardato a schierarsi le o.n.g. che difendono i diritti civili.

[79] Si è parlato di cyberguerre nel '99 quando era aumentata la tensione fra Cina e Taiwan, in Medio Oriente quando gli Israeliani bombardavano telematicamente i server di Hamas, e Hezbollah mentre da tutto il mondo venivano colpiti quelli degli ebrei ortodossi, i Cecenia quando l'occidente organizzava netstrike contro obiettivi russi e anche in ex-Jugoslavia fra albanesi e serbi e degli attivisti contro i serbi.

[80] È già stato coniato un acronimo: C3I (Command, Control, Communications and Intelligence).

[81] Un paese prevalentemente agricolo evidentemente offre meno il fianco ad attacchi del genere.

[82] Qui il catastrofismo di alcuni commentatori ha trovato sfogo immaginando cosa succederebbe aprendo dighe, oscurando i radar, facendo deragliare convogli, manomettendo centrali nucleari, facendo combattere un esercito contro se stesso e via dicendo. Si tratta di strategie alquanto inverosimili, perché la comunità internazionale difficilmente tollererebbe disastri del genere. Per avere anche la certezza tecnica della loro irrealizzabilità bisognerebbe scollegare i centri di controllo più vulnerabili da una rete a pubblico accesso come Internet e connetterli attraverso network dedicati, sebbene più costosi.

[83] John Arqiulla, consulente del Pentagono, ha detto che l'unità di manovra non dev'essere più il grande battaglione meccanizzato ma unità di 500/700 militari perché maneggevole e preciso (grazie all'informatica). Diminuendo le unità e la loro consistenza numerica viene meno la necessità della grande struttura gerarchica pensata per controllare centinaia di migliaia di soldati e anzi sarebbe un freno alla sua efficienza. Parole affini a quelle pronunciate in casi di ristrutturazioni aziendali.

[84] A meno che non si trovi un modo per quantificare le conoscenze informatiche e attribuire loro il dovuto peso nel computo delle risorse spese rispetto ai risultati ottenuti.

[85] La difficoltà di una comprensione del fenomeno preoccupa tanto i militari, che non sanno come distinguere disastri occasionali dal principio di un attacco, quanto i civili che non potrebbero allontanarsi da un fronte che non ci sarebbe.

[86] Il protocollo di comunicazione Ip, standard grazie al quale reti eterogenee si connettono formando Internet, manca di algoritmi di autenticazione sicuri, e anche se venissero implementati il fattore umano (determinante in eventuali autorità di certificazione) rimarrebbe il ventre molle del sistema (cfr. nota 70). Per non considerare la necessaria diffusione di identificatori di retina (o altri mezzi di autenticazione) ad ogni terminale e la schedatura della popolazione. Questo è solo un degli esempi dell'inadeguateza del

protocollo Ip a rispondere a tutte le contrastanti istanze che rigurdano Internet.

[87] Tenere nella dovuta considerazione i costi della sicurezza quando si realizza un progetto è una strada caldeggiata da molti. Per favorirla dal '98 l'International Standard Organization assieme al Common Criteria Implementation Board, hanno definito standard comuni (IS 15408) per valutare la sicurezza nel campo dell'Infomation Technology.

[88]Se il processo di miglioramento tecnico non avvenisse pubblicamente fazioni di qualunque genere potrebbero scoprire e sfruttare a loro piacimento la permeabilità dei sistemi. La pubblicità della azioni degli hacker (per gloria, per fiducia nella libera circolazione delle informazioni, per ottenere un'offerta di lavoro allettante) è garanzia del loro operato, e permette la migliore allocazione delle conoscenze, quindi mantiene al più alto livello il dibattito e le azioni. Se il livello del dibattito pubblico fosse inferiore a quello fra privati questi avrebbero immediatamente un potere difficilmente controllabile.

[89] Compagnie e istituzioni offrono cifre enormi per assumere ex hacker. E a volte prendono clamorose cantonate. D’altra parte, come detto, è difficile che possa portare ai risultati sperati uno scontro frontale con gli hacker, perché non sono un vero e proprio movimento ma una moltitudine accomunata da alcuni tratti culturali; non vi sono né dei rappresentanti né dei capi, fermati i quali l'hacking sparirebbe.