Storia e Società

Federico Mazzini

Hackers

Storia e pratiche di una cultura

GLF Editori Laterza

Storia e Società

Federico Mazzini

Hackers

Storia e pratiche di una cultura

Editori Laterza

Edizione digitale: gennaio 2023

www.laterza.it

Realizzato da Graphiservice s.r.l. - Bari (Italy)
per conto della
Gius. Laterza & Figli Spa

ISBN 9788858151174

Indice

A Guido,
che mi ha portato sin qui

Introduzione. Cos'è un hacker?

Questa è una storia di maghi, spie, «nerd», agenti dell'FBI, giornalisti, hippies e capitani d'azienda. Una storia di computer, telefoni, radio e lucchetti. È la storia di un concetto, «hacker», che ha avuto negli anni e per diverse persone significati molto differenti e che è arrivato ad essere, che ne siamo consapevoli o meno, una delle parole chiave del nostro presente.

Chi sia interessato esclusivamente ai suoi elementi evenemenziali può iniziare la lettura dagli ultimi due paragrafi di questa Introduzione, dove proporrò una definizione provvisoria del concetto, che ci aiuterà a navigare nella sua storia, e riassumerò i fini e la struttura del volume.

I prossimi due paragrafi sono infatti dedicati a un pubblico che oggi in larga parte non esiste: gli storici che si occupano di hacking. In essi riassumerò cosa il mondo accademico sa e ha detto dell'hacking, con una particolare attenzione alla sua storia, spesso narrata da specialisti di altre discipline o da giornalisti. La speranza è che da questo retroterra emerga l'importanza di uno sguardo specificatamente storico sul fenomeno e, magari, che qualcuno dei lettori possa essere abbastanza intrigato da approfondire quei tanti elementi della storia dell'hacking che ancora devono essere raccontati e che per ragioni di spazio e di energie non è stato possibile includere in questo libro.

Hackers accademici

La parola «hacker» appare probabilmente per la prima volta in un testo accademico nel 1976. In una riflessione filosofica sul rapporto tra uomo e computer, Joseph Weizenbaum, professore del Massachusetts Institute of Technology (MIT) e uno dei pionieri dell'intelligenza artificiale, fa

notare che ognuno di noi, dall'ingegnere elettrico al violinista, è costretto dalle leggi della fisica. Non così il programmatore. Chi scrive codice di programmazione ha il controllo delle regole del gioco e i suoi soli limiti sono il talento e l'immaginazione: egli «può creare società nelle quali i prezzi salgono quando i beni diventano abbondanti e cadono quando diventano scarsi, e nelle quali solo le unioni omosessuali generano figli»[1]. Se il programma non funziona come previsto il programmatore non potrà guardare al mondo esterno o a fattori sociali o naturali: la colpa sarà solo sua, poiché solo suo è il controllo delle leggi che governano il software. Tali leggi sono seguite dal programma in una maniera così precisa e puntuale da distinguere, di nuovo, l'informatica da ogni altra attività umana: «Nessun autore, nessun regista, nessun imperatore, per quanto potente, ha mai esercitato un'autorità così assoluta»[2].

Un potere così completo non può che corrompere. Secondo Weizenbaum ovunque vi fosse un centro informatico (siamo negli anni appena precedenti la diffusione dei computer domestici) si trovavano giovani talentuosi, dai vestiti disordinati, dagli occhi arrossati e dalla dieta malsana, pronti a dimenticare il proprio corpo e a vivere solo attraverso e per il computer, in una dipendenza patologica e autodistruttiva. Tecnici eccellenti, essi avevano messo al centro della propria vita la sensazione di dominio e di controllo quasi divino che solo l'interazione con un software può dare. Questi giovani corrotti dal potere delle macchine chiamavano sé stessi «hackers» e le proprie attività «hacks».

Laddove un professionista scriveva codice per risolvere problemi, l'hacker cercava problemi per avere una scusa per interagire con il computer e ricavarne la scossa adrenalinica di cui non poteva fare a meno. Ma, come in ogni dipendenza, il piacere durava poco ed era sempre più difficile da raggiungere. L'hacker non si accontentava di aver dimostrato il proprio dominio sul computer con un programma funzionante, ma doveva trovare nuove sfide, spingere il computer verso nuove performances, creando artificiosamente nuovi problemi da risolvere. Questo infinito processo non equivaleva però, agli occhi di Weizenbaum, alla creazione di conoscenza. Agli hackers mancava un obiettivo che non fosse il soddisfacimento della propria dipendenza e del proprio ego:

[l'hacker] non può fissare un obiettivo di lungo periodo e formulare un piano per raggiungerlo, poiché egli ha solo tecnica, non conoscenza. [...] La sua capacità è quella di un monaco copista che, per quanto analfabeta, è un superbo calligrafo[3].

Questa inclemente analisi rimarrà per alcuni anni l'unica descrizione di successo accademico del nascente fenomeno dell'hacking informatico. Dopotutto, come nota Weizenbaum in un altro passaggio sferzante, gli scienziati sociali «non vedono giustamente alcun motivo di spendere le proprie energie a studiare le opere degli hackers»[4]. Questo rimase vero fino al 1984, quando Sherry Turkle, anche lei docente al MIT, diede alle stampe *The Second Self: Computers and the Human Spirit*[5]. La sociologa e psicologa offre una lettura decisamente più sofisticata, mettendo l'accento sulla costruzione sociale di alcune caratteristiche degli ingegneri e degli informatici del MIT, quali ad esempio la scarsa attrattività fisica o l'inettitudine sociale. Ma alcuni punti salienti non divergono sostanzialmente da quelli presentati da Weizenbaum. La differenza tra ingegneri e hackers sta nel fatto che i primi vedono i computer come strumenti per un fine, mentre i secondi li vedono come un fine in sé stesso, un luogo dove esercitare, attraverso la ricerca di un'impossibile perfezione tecnologica, il proprio dominio sulla macchina. Questa sfida allontana gli hackers dalla società e si configura come una dipendenza.

La studiosa aggiunge però un elemento fondamentale: gli hackers possono sentirsi «differenti», «unici», o essere visti come dei reietti, ma non lo sono. Non solo perché la dipendenza da prove sempre più difficili e viste dai più come fini a sé stesse non è loro esclusiva (si pensi agli sport estremi o a un hobby perseguito con particolare passione), ma soprattutto perché essere hacker significa essere parte di una cultura hacker, di una comunità di persone che ha specifiche gerarchie, rituali, gusti estetici (tra questi, nota Turkle, una onnipresente passione per la fantascienza e i videogames, in quanto intrattenimento che, come la scrittura di codice, permette la creazione di universi con regole proprie e differenti dalla realtà).

Al centro di questa cultura vi è l'hack, che la studiosa definisce come un atto che dimostra la capacità tecnica di un individuo e il suo dominio su una specifica tecnologia. L'hack non può essere fortuito, ma deve essere

basato su una conoscenza intima della tecnologia in questione e deve trovare il modo di raggiungere i propri fini nella maniera più semplice (o, agli occhi degli hackers, «elegante») possibile. In ultimo, l'hack deve essere basato su conoscenze acquisite «non ufficialmente» e alle spese di un «grande sistema» (come quello telefonico o universitario). Turkle è stata la prima studiosa a richiamare l'attenzione su una caratteristica della cultura hacker che è fondamentale per la sua comprensione, ma è spesso dimenticata, ieri come oggi, nella percezione pubblica e nella ricostruzione giornalistica: l'hack non è necessariamente operato su tecnologie informatiche. Gli esempi da lei riportati sono in particolare quelli del phone phreaking (una sorta di hacking del sistema telefonico che sarà oggetto del cap. 2) e della scassinatura di serrature. Quest'ultima attività rimarrà, come vedremo, una caratteristica delle culture hacker fino almeno agli anni Novanta, presente in pubblicazioni dell'underground digitale e nelle conventions hacker. Ma ancora più duraturo e importante è il motivo per il quale le serrature sono una tecnologia particolarmente congeniale alla cultura hacker: essa al contempo rifiuta e ricerca i sistemi chiusi, siano essi un ufficio sottochiave, un numero di telefono segreto, un network protetto da password o un software il cui codice non sia di pubblico dominio: «un sistema chiuso è una sfida. Una cassaforte è lì per essere scassinata. Un mistero esiste per essere svelato. È la variante hacker del più ampiamente conosciuto cliché del Monte Everest che è lì per essere scalato»[6].

L'analisi di Turkle è parzialmente superata, soprattutto nelle parti che condivide con Weizenbaum: la «dipendenza» è denunciata da alcuni hackers successivi (ad esempio Kevin Mitnick, vedi cap. 4), ma è lungi dall'essere la chiave di volta attraverso cui comprendere l'intera pratica. La mancanza di obiettivi è ravvisabile solo se non si considerano la definizione identitaria, la costruzione comunitaria e il compiacimento dell'ego delle mete degne di essere perseguite – e anche in questo caso non la si può oggi rimproverare a gruppi hacker con chiari obiettivi pratici, quali i movimenti Free Software e Open Source o «hacktivisti» (vedi rispettivamente capp. 5, 6 e 7). Anche l'immagine pubblica dell'hacker disordinato, goffo e asociale è oggi, come vedremo nelle pagine che seguono, almeno in parte cambiata. *The Second Self* è tuttavia

pionieristico nel suo mettere in evidenza caratteristiche che sarebbero rimaste costanti e centrali nelle culture hacker successive, quali l'individualismo, il parallelo tra arte, creatività e programmazione, l'importanza definitoria dell'hack, l'avversione e contemporanea fascinazione per i sistemi tecnologici chiusi ed inesplorati, il parallelo con appassionati di tecnologie non informatiche.

È per questo in un qualche modo sorprendente che, nella letteratura accademica sugli hackers, il libro più citato non sia ad oggi quello di Turkle, ma quello, uscito nello stesso anno, del giornalista Steven Levy, *Hackers: Heroes of the Computer Revolution*[7], che annuncia sin dal titolo la propria natura semi-agiografica e l'intento divulgativo più che scientifico o analitico. Il volume prende le mosse, ancora una volta, dal MIT e dal Tech Model Railroad Club, un'associazione di studenti impegnati, fin dagli anni Cinquanta, ad assemblare una complessa ricostruzione in miniatura di una ferrovia. Il club comprendeva esperti di storia ferroviaria, ma anche appassionati della tecnologia elettrica che permetteva al modellino di muoversi. Questi ultimi erano altrettanto attratti dalla tecnologia informatica (in un momento storico in cui i computer erano pochi, estremamente costosi, dal difficile uso e dal difficile accesso, soprattutto per gli studenti) e chiamavano sé stessi hacker. L'hack era per loro, secondo Levy, un qualsiasi atto che interviene «artisticamente» su una tecnologia, con «innovazione, stile, e virtuosità tecnica». Come nel caso del modellino, oggetto di continue modifiche da parte dei membri del club, l'hack non doveva avere risvolti pratici o utilitaristici ma solo dimostrare ingegnosità ed eleganza.

Merito del volume di Levy è quello di aver documentato come le parole hack e hacker siano state usate in riferimento all'informatica già dalla fine degli anni Cinquanta (precedentemente la parola indicava soltanto l'atto di tagliare in maniera rozza, come si può fare con un machete o uno scalpello). Più incerto se l'hack fosse fin dal principio definito come atto creativo, o se Levy non sia stato invece influenzato dalla definizione che sarebbe diventata prevalente all'interno dei circoli hacker dagli anni Settanta. Peter Samson, protagonista del primo capitolo di *Hackers*, membro del Railroad Club e probabilmente principale informatore di Levy per la parte riguardante «i primi hackers», ha scritto nel 1959 un

dizionario del gergo interno dell'associazione ad uso dei neofiti. In esso Samson definiva «hack» in maniera ironica e prosaica come «1) qualcosa fatto senza un fine costruttivo; 2) un progetto cominciato a causa di una cattiva autosuggestione; 3) l'atto di produrre o tentare di produrre un hack».

È solo in un commento del 2005 – dopo che, anche grazie al volume di Levy, la cultura hacker sarà più definita e conosciuta – che Samson aggiunge:

> Vedevo questo termine come sinonimo di applicazione non convenzionale o non ortodossa della tecnologia, generalmente deprecata per ragioni ingegneristiche. Non c'era nessun suggerimento di un intento maligno (o benigno). Al tempo di questo dizionario c'erano stati «buoni hacks»: usare un computer grosso come una stanza per suonare musica, ad esempio; o, qualcuno potrebbe dire, la scrittura stessa di questo dizionario[8].

In una conferenza tenuta poco dopo l'uscita del libro di Levy e da esso ispirata, che vedeva la partecipazione dell'autore e di molti suoi protagonisti, uno dei discussants, Peter Webster, notava: «l'ironia è che 'hacker' originariamente indicava qualcuno che non era molto bravo. Era qualcuno che non aveva capacità professionali, ma cercava di compensare in quantità quanto non riusciva a raggiungere in qualità»[9], dando peso all'ipotesi che inizialmente il termine avesse una denotazione benevolmente denigratoria piuttosto che celebrativa.

Il libro procede a raccontare la storia degli hackers della Silicon Valley negli anni Settanta e dei primi programmatori di videogiochi per personal computers. Ma la parte senza dubbio più influente del volume è il secondo capitolo[10], dove Levy definisce le caratteristiche dell'etica hacker in cinque punti.

In primo luogo «l'accesso ai computer – e a qualsiasi cosa possa insegnare qualcosa sul modo in cui funziona il mondo – deve essere illimitato e totale. Inchinatevi sempre all'Hands-on Imperative». Con quest'ultima espressione si intende la necessità di imparare, lavorare ed esplorare i sistemi tecnologici in maniera pratica, diretta e sperimentale, non attraverso la preparazione teorica. L'accesso totale postulato dal primo pilastro dell'etica hacker può arrivare ad estremi paradossali: «in un mondo hacker perfetto» chiunque avrebbe il diritto, secondo Levy, di

aprire la scatola di controllo di un semaforo e modificarlo, a patto di essere convinto della propria capacità di migliorarne il funzionamento.

La pretesa di accesso illimitato porta gli hackers in rotta di collisione con tutte le figure e le istituzioni che sono incaricate di far rispettare le regole. Il secondo punto recita: «Diffida dell'autorità – promuovi la centralizzazione»: la burocrazia universitaria, statale e aziendale è il primo ostacolo al libero scambio delle informazioni. Al tempo della scrittura del libro, l'azienda che meglio di tutte incarnava il nemico dell'etica hacker era l'IBM, che vendeva costosissime macchine con software proprietario e incompatibile con altri computer, ignorava l'innovazione in favore di tecnologie affidabili, mediocri e commercializzabili e promuoveva professionisti dell'informatica più vicini a un impiegato che non all'esploratore che voleva essere un hacker. Dieci anni prima, come vedremo nel cap. 2, il nemico era stata la American Telephone and Telegraph Corporation. Dieci anni dopo, Microsoft: il professionista dell'informatica che lavorava senza creatività e solo per «timbrare il cartellino» era sprezzantemente chiamato «microserf»[11] (microservo). Levy coglie qui un'importante caratteristica delle culture hacker e di molte «culture tecniche» e giovanili: la necessità di un avversario che definisca cosa il gruppo *non* è. Come vedremo, il rapporto è però più complesso di una semplice avversione e coinvolge anche un certo grado di fascinazione.

Il terzo punto recita: «Gli hackers dovrebbero essere giudicati dal loro hacking, non da criteri sciocchi come i titoli accademici, la razza, gli anni, o la posizione», e rivela il carattere divulgativo e ingenuamente elogiativo dello scritto di Levy. Se è vero che, con l'avvento dell'interconnessione informatica, l'hacker poteva assumere identità multiple e non corrispondenti alla sua realtà quotidiana, è anche vero che le persone di cui parla Levy hanno un nome e un cognome e sono immerse in ambienti sociali e lavorativi: è semplicemente impensabile che, anche nel giudizio su un atto tecnico, queste caratteristiche fondamentali dell'individuo potessero essere del tutto ignorate. Anche nel mondo potenzialmente anonimo dei *fora* online, peraltro, si creava e si crea una gerarchia basata sulla reputazione, nella quale la perizia tecnica è certo importante, ma ugualmente importanti sono la possibilità di

accesso alle tecnologie, la capacità comunicativa e i rapporti interpersonali, campi nei quali titoli, età e posizione contavano e contano ovviamente in maniera decisiva. Difatti le comunità hacker sono state, almeno fino alla metà degli anni Novanta, uniformemente bianche, giovani e di classe media. Significativo è qui il fatto che il genere non sia incluso tra gli «sciocchi» criteri che gli hackers sarebbero in grado di ignorare. Le comunità hacker sono infatti, oggi come ieri, nella grandissima parte composte da uomini, una caratteristica che non era sfuggita a Turkle.

Il quarto punto riprende quanto accennato in *The Second Self:* «Si può creare arte e bellezza su un computer», non solo perché questo può essere strumento di creazione di forme tradizionali d'arte, come la musica, ma soprattutto perché il codice di programmazione ha un proprio valore estetico. Come è possibile esprimere lo stesso concetto utilizzando un'espressione banale o una frase poetica, così è possibile dare istruzioni a un computer in maniera rozza (di solito sinonimo di complicata e perciò più impattante sulle prestazioni della macchina) o elegante (cioè in maniera diretta e succinta). Il risultato finale, il comportamento del computer, sarà lo stesso, ma il potenziale estetico sta nell'esecuzione, non nell'esito.

L'ultimo punto («I computer possono cambiare la tua vita in meglio») è, nella definizione di cosa sia un hacker, il meno importante. Non necessariamente perché questa non fosse realmente la convinzione degli hackers che hanno studiato Levy e alcuni successivi autori (si veda ad esempio il cap. 6), ma perché è un'affermazione talmente generica da poter essere adottata dalla maggior parte dei gruppi professionali, politici e di interesse che si sono occupati di informatica dalla seconda guerra mondiale ad oggi.

Hackers: Heroes of the Computer Revolution ha tutti i pregi e tutti i difetti di un ottimo libro di divulgazione. Da una parte la sua lettura è piacevole, accessibile ai non specialisti, e Levy si dimostra precoce e acuto nell'individuare alcune caratteristiche della cultura hacker e l'importanza dell'hacking nel mondo contemporaneo. Molte delle testimonianze dirette dell'epoca sarebbero oggi perse se non fossero state raccolte e valorizzate da un libro di successo. D'altra parte il valore storiografico del saggio è compromesso dall'ambiguità di Levy sulle proprie fonti, dal

gusto per l'aneddoto e, soprattutto, da una narrazione che segue in maniera sospettosamente fedele alcuni *topoi* letterari. Il genio distratto ed eccentrico, capace di comprendere istintivamente i più astrusi problemi matematici o ingegneristici ma incapace di relazionarsi con il prossimo o di comportarsi in società, è uno dei personaggi ricorrenti del libro, che Levy riprende da una lunga tradizione, risalente almeno alla fine del XIX secolo, propria della letteratura popolare su scienza e tecnologia. Peter Samson, racconta Levy, rispondeva sempre negativamente alla richiesta di sua moglie «Vuoi aiutarmi con le borse della spesa?», poiché la domanda, come un codice «buggato», era mal posta: non *voleva* aiutarla, ma lo avrebbe fatto se glielo avesse chiesto[12]. John McCarthy, uno dei padri dell'intelligenza artificiale, apparentemente rispondeva alle domande che gli si ponevano dopo svariate ore e fuori contesto: la sua risposta, in ogni caso, sarebbe stata brillante[13]. L'impressione è quella di una serie di personaggi che vogliono da una parte eroicizzare gli hackers e dall'altra confermare le aspettative del lettore sulle loro caratteristiche.

Perché, dunque, il libro si trova citato nella maggior parte dei saggi accademici sull'hacking? Il primo motivo è la mancanza di alternative. La letteratura successiva, di carattere perlopiù sociologico e antropologico, ha usato il libro di Levy e altre ricostruzioni giornalistiche perché non esistevano (e in larga parte ancora non esistono) saggi storici su un fenomeno che, nonostante abbia ormai una lunga storia, sembra congelato in un eterno presente. Ciò ha comportato importanti distorsioni, che questo volume intende in parte correggere. Prima tra queste l'idea che l'hacking sia un fenomeno nato nelle aule universitarie: se è vero che la parola è probabilmente nata nelle università statunitensi negli anni Cinquanta, e se è vero che il computer hacking ha da lì avuto inizio, le caratteristiche di quella che sarà definita «cultura hacker» sono rintracciabili, come vedremo nelle prossime pagine, ben prima nel tempo e in altre «culture tecniche».

Il secondo motivo, e la ragione per la quale il libro di Levy è qui discusso nel dettaglio, è che esso stesso è diventato parte della cultura hacker. Il volume non ebbe successo solo tra gli accademici, ma anche e soprattutto tra gli hackers e gli aspiranti hackers, che, operando perlopiù al di fuori delle università, potevano così sentirsi parte di una tradizione

prestigiosa e di lunga data – in netto contrasto con la narrazione perlopiù negativa che era fornita, a partire dalla fine degli anni Ottanta, dai media. Ancora nel 2007 un hacker olandese ricordava che «dopo aver letto il libro di Levy [...] ho capito cosa ero e che stavo per diventare parte di una comunità globale, anche se conoscevo solo pochi hackers attorno a me»[14]. Ogni lista delle letture essenziali pubblicata sulle riviste e su *fora* online hacker dopo il 1984 avrebbe compreso ai primi posti il libro di Levy.

I cinque punti dell'etica hacker furono dunque adottati da una comunità ben più ampia, acquisendo rilevanza culturale anche al di là della loro iniziale esattezza e del loro essere riferiti al solo hacking universitario. I punti specifici potevano essere contestati o del tutto ignorati, ma la questione di quali siano i confini dell'etica hacker, di cosa significhi essere «un vero hacker» (espressione che Levy riserva ai propri protagonisti), rimarrà centrale nei dibattiti della comunità e nella creazione dei suoi confini.

Cultura hacker

Se negli anni Ottanta e Novanta l'hacker è raccontato perlopiù da giornalisti, nella maggior parte dei casi molto meno simpatetici di Levy, ma non meno sensazionalisti, alla fine del millennio si risveglia l'attenzione delle scienze sociali. Il focus non erano più i primi hackers accademici, ma i giovani che, tramite i personal computers, sempre più frequentemente penetravano sistemi informatici aziendali e governativi.

Nel 1999 il sociologo Paul Taylor propone una lettura della cultura hacker, basata su interviste tenute in Europa nel decennio precedente, che mette al suo centro la contrapposizione tra gli hackers e gli esperti di cybersicurezza[15]. Se per le origini Taylor cita Levy e i mainframes del MIT, le domande che sottendono alla sua ricerca sono rivelatrici della mutata concezione degli hackers avvenuta nei quindici anni precedenti: cosa definisce un gruppo considerato «deviato» e criminale? In che modo la cultura hacker pensa sé stessa in rapporto al resto della società? Dopo aver notato, come i suoi predecessori, la centralità dell'hack e il suo estendersi a qualsiasi tipo di tecnologia o sistema sociale, Taylor sottolinea come l'illegalità non sia al centro dell'hacking (una distinzione che non era necessario rimarcare nella ricostruzione di Turkle o Levy).

L'hack, nell'ampiezza delle sue possibili applicazioni, può portare ad infrangere la legge. Ma il suo potere definitorio non sta nella sua illegalità, nei danni che può causare al prossimo o nei benefici che può portare all'hacker. Per definire chi entra nei sistemi per solo vantaggio materiale le comunità hacker hanno anzi un nome specifico: cracker. Ciò che rende un hack l'atto attorno al quale si raccoglie una comunità sono la sua originalità e l'ingegnosità individuale di chi per primo lo ha pensato. Trovare il modo di usare un computer per suonare musica per la prima volta è un hack. Seguire le istruzioni di chi per primo ci è riuscito per ottenere lo stesso risultato non lo è. Chi si limita ad applicare supinamente hacks inventati da altri è chiamato in maniera sprezzante script kiddie. Non solo: l'hack non deve essere dovuto alla semplice costanza e dedizione, ma deve essere frutto di intelligenza. Merito degli studi del sociologo è l'aver sottolineato come l'hacking sia un atto che ha quasi sempre risvolti pubblici, in contrasto con lo stereotipo dell'hacker solitario e asociale: «un buon hack dà maggiore soddisfazione quando è condiviso e può contribuire alla reputazione dell'hacker e garantirgli accesso a più informazioni messe in comune. Ad esempio l'accesso ad alcuni *fora* online è concesso solo a quelli che hanno provato il proprio valore»[16].

Douglas Thomas, teorico dei media, nel 2002 rilegge il fenomeno hacker partendo da simili premesse[17] (stessa cronologia, stessa centralità dell'hack creativo e di una tecnologia non necessariamente informatica), ma alla luce della categoria di «subcultura giovanile». Gli hackers di cui parla non sono più universitari, ma perlopiù studenti medi. Il computer era per loro

> un mondo proibito, governato da un'autorità principalmente maschile, nel quale essi potevano penetrare con relativa facilità e dove potevano esplorare e fare scherzi, spesso a spese di grandi istituzioni come le compagnie telefoniche. [...] Come la musica alta, la moda giovanile e il fumare sigarette, l'hacking è una forma di ribellione e un esercizio di potere. [...] L'hacking è uno spazio nel quale i giovani, e in particolare i maschi, possono dimostrare la propria capacità e il proprio dominio e sfidare le convenzioni dei genitori e della società[18].

La tecnologia è dunque per gli hackers un «campo giochi», attraverso il quale dimostrare, con scherzi e provocazioni, il proprio dominio sulla

tecnologia e l'inadeguatezza tecnologica dell'autorità adulta. Al centro dell'hacking sono, nell'acuta lettura di Thomas, le relazioni interpersonali e le gerarchie sociali, che vengono messe alla prova, rafforzate o contestate, attraverso la tecnologia: «gli hackers 'interpretano [*perform*] la tecnologia' creando e sfruttando le contraddizioni fondamentali e le relazioni che le persone hanno con le tecnologie e tra di loro»[19].

Al contrario di altre subculture giovanili, il cui stile è nel tempo incorporato dalla cultura egemone[20] (si pensi al rock, al rap, al punk, ai *teddy boys* o, oggi, alla «cultura geek»), l'hacking richiede capacità tecniche che rendono difficile il dialogo intergenerazionale e la comunicazione esterna alle comunità di iniziati. Anche per questo la «costruzione giuridica dell'hacker»[21] è così difficoltosa, caratterizzata, soprattutto alla fine del millennio scorso, da pene sproporzionate agli effettivi danni causati: l'incomprensione delle effettive possibilità e implicazioni tecniche spinge il legislatore, come vedremo nel cap. 4, a punire quello che si teme il criminale possa fare, non quello che effettivamente fa. La feroce, e a tratti paradossale, punizione degli hackers, unita alla evidente ignoranza delle forze dell'ordine e dei giudici in materia di computer e telefonia, aumenterà la sensazione di alienazione dalla società propria di ogni subcultura giovanile.

Vedere gli hackers nella loro contrapposizione con l'autorità «adulta» permette a Thomas di evidenziare alcune caratteristiche che erano precedentemente state ignorate, quali ad esempio la competitività tra i membri della comunità, che devono dimostrare il proprio dominio non solo sui sistemi tecnologici, ma anche sui propri pari; o la presenza di un gergo specifico, ispirato dalla disposizione della tastiera e analogo a quello di altre subculture. L'accento sulle relazioni permette allo studioso di dare il giusto spazio, nella cultura hacker, all'«ingegneria sociale» (social engineering), l'arte di comprendere e interagire creativamente con un sistema sociale per spingerlo a comportarsi secondo la propria volontà.

La migliore e più conosciuta studiosa degli hackers negli ultimi vent'anni è senza dubbio l'antropologa Gabriella Coleman. In una serie di studi sul campo, a stretto contatto con specifiche comunità, Coleman ha evidenziato elementi centrali della cultura hacker che erano sfuggiti a letture più distanti. Tra questi la natura 'pratica' della comunicazione

politica degli hackers, il loro legame con l'ideologia liberale[22] e il ruolo delle conventions, i grandi eventi che permettono agli hackers (e ad altre culture tecniche prima di loro, come vedremo) di «mettere in pratica, rendere visibili e di conseguenza celebrare molti degli elementi del loro quotidiano tecnologico»[23]. Più in generale, il lavoro di Coleman è stato capace di dimostrare che lo studio di quelle che possono a prima vista apparire come astruse comunità tecniche o, in virtù delle loro modalità comunicative, gruppi di «nerd» immaturi, volgari e a volte criminali, abbiano in realtà un ruolo fondamentale non solo nell'esperienza che oggi abbiamo del digitale, ma anche in campi non necessariamente collegati alle tecnologie o alla rete, come la proprietà intellettuale[24] o l'attivismo politico[25]. Come si vedrà, questo volume deve molto allo sguardo di Coleman sul mondo hacker, in particolare nelle parti dedicate al movimento Open Source e ad Anonymous.

La nostra definizione

La storia dell'hacking per come è stata scritta finora può essere dunque così riassunta: prima vennero gli hackers universitari, a Stanford, Harvard e MIT; l'hacking dei telefoni o phreaking è assimilato alla pratica dell'hacking, citato come un curioso progenitore o in alcuni casi del tutto ignorato. Poi, negli anni Settanta, l'hacking si sposa con il giovane capitalismo della Silicon Valley, dando i natali ad alcune delle aziende che ancora oggi dominano il campo dell'high tech. Alla fine degli anni Ottanta inizia la «golden age of cracking»[26]: grazie alla diffusione dei personal computers l'hacking esce dai laboratori universitari e aziendali e, nelle mani di ragazzini entusiasti e irresponsabili, diventa un fenomeno mondiale, perlopiù criminale.

Non vi è nulla di sbagliato in questa ricostruzione, e difatti parte di tale scansione è ripresa nei capitoli centrali di questo libro. Ma agli occhi di uno storico questo schema solleva tante domande quante sono quelle a cui esso è capace di rispondere.

La ricerca che ha portato a questo saggio parte dallo studio dei phone phreaks, gli «hackers dei telefoni» che, soprattutto negli Stati Uniti e tra gli anni Sessanta e gli anni Ottanta, hanno interagito creativamente con il sistema telefonico AT&T. Durante la lettura della loro principale

newsletter, «YIPL/TAP», pubblicata tra gli anni Settanta e la metà degli anni Ottanta, mi sono accorto che molte delle caratteristiche culturali ascritte agli hackers universitari e in seguito a quelli dei personal computers e della rete erano presenti, perfettamente riconoscibili, in comunità formate da studenti medi, che nulla avevano a che vedere con il MIT o con qualsiasi altra università. Se davvero l'origine dell'etica hacker è da ricercarsi nell'accademia, come sostengono Levy e praticamente tutti gli studiosi che si sono in seguito occupati di hacking, come è possibile che questa stessa etica si trovi, pressoché identica e nello stesso momento, al suo esterno? Il fatto stesso che la cultura hacker si sia trasferita dalle università alle comunità, di nuovo formate perlopiù da studenti medi, di hackers non accademici dalla seconda metà degli anni Ottanta è curioso e finora inspiegato. Davvero è bastata la popolarità del libro di Levy a impregnare intere generazioni di appassionati di computer con l'etica nata nello specifico contesto delle università americane?

Queste domande, unite alla mia esperienza di ricerca sulla divulgazione tecno-scientifica nel primo Novecento[27], mi hanno portato a formulare l'ipotesi che questo volume vuole dimostrare: se la parola hack riferita all'informatica è nata in contesto universitario, le caratteristiche della cultura hacker sono la manifestazione di un processo di più lunga durata che possiamo chiamare, con Constance Penley e Andrew Ross, la tecnocultura statunitense[28]. Come si vedrà nei capitoli seguenti, parte di questa tecnocultura sono la centralità dell'individuo nel processo di innovazione e l'accento posto sul ruolo positivo che l'esperienza diretta della tecnologia ha per i giovani. Questo immaginario, incarnato in riviste, pubblicità e romanzi, vede al proprio centro il valore dell'atto creativo operato su una tecnologia esistente per risolvere problemi contingenti. Difficile e forse inutile cercare di individuare la precisa data di nascita di questa concezione del rapporto tra tecnologia e società. Ciò che è certo, dal mio punto di vista, è che questo immaginario e il suo apparato valoriale sono già ravvisabili nelle riviste di divulgazione di massa che nascono nei primi vent'anni del Novecento e nella letteratura per ragazzi a cavallo tra i due secoli.

Questo libro intende dunque raccontare la storia dell'hacking in una prospettiva di lungo periodo e provare che è solo da questa prospettiva

che esso può essere storicamente compreso. Per farlo abbiamo bisogno di una definizione di hack che possa essere il punto di riferimento attraverso il quale osservare il cambiamento storico, abbastanza generica da soddisfare la maggior parte degli studiosi che si sono finora occupati dell'argomento ed abbastanza specifica da essere riconoscibile come un unico fenomeno, anche a scapito delle ovvie variazioni delle sue manifestazioni storiche.

Definiamo dunque hack come *qualsiasi interazione creativa e originale con una tecnologia preesistente volta a modificarne le funzioni rispetto a quanto previsto dal suo designer originale*. Aggiungendo l'importante corollario che, per essere considerato tale, l'hack deve essere comunicato all'interno di una comunità che possa valutarne il valore e metterlo in relazione con la reputazione di chi lo ha compiuto. Vale la pena sottolineare che, come nel caso degli studiosi che mi hanno preceduto e dell'autodefinizione di tutte le comunità hacker, non vi è riferimento alla legalità dell'atto o al campo dell'informatica.

Usando questa definizione tenteremo di superare la rigida divisione in «generazioni» di hackers (che in ogni caso sono estremamente permeabili e spesso sovrapposte) e di guardare a un unico fenomeno storico, che chiamiamo hacking perché questa è la sua definizione oggi più diffusa. Adotteremo dunque una prospettiva che possiamo chiamare, con Michel Foucault, genealogica: non cercheremo in primo luogo di provare relazioni tra fatti storici, siano esse cronologiche o causali, ma interpreteremo fenomeni storicamente distanti come diverse manifestazioni di un unico discorso sulla tecnologia.

Nel percorso vedremo che il rapporto creativo con la tecnologia è stato capace di riunire comunità di giovani e giovani adulti ben prima che il primo computer entrasse in un laboratorio universitario; scopriremo che alcune caratteristiche, pratiche e rappresentazioni che identifichiamo con la più recente modernità hanno in realtà una storia ben più lunga; e infine ripercorreremo la storia del computer hacking fino agli impetuosi cambiamenti che hanno caratterizzato la pratica (e la cultura digitale nel suo complesso) negli ultimi vent'anni.

Il volume si apre così con un capitolo dedicato alle prime comunità che all'inizio del Novecento si sono riunite attorno alla capacità individuale di interagire creativamente con la tecnologia: i radioamatori. Il capitolo

successivo affronta i phone phreaks dagli anni Settanta, evidenziando quella che, a mio modo di vedere, rimane la più importante eredità che essi hanno lasciato alla cultura hacker e a quella digitale: le modalità della comunicazione politica. Il capitolo 3 racconta la storia dei primi hackers non universitari e la reazione dell'opinione pubblica, ancora legata a una concezione largamente positiva del rapporto gioventù-tecnologia. Il capitolo 4 narra il processo di mediatizzazione e parallela criminalizzazione degli hackers avvenuta dalla fine degli anni Ottanta, in particolare attraverso le vicende di uno dei computer hackers più famosi di sempre, Kevin Mitnick. I due capitoli successivi narrano la storia dei movimenti Free Software e Open Source e li pongono all'inizio di una nuova risemantizzazione, da parte della società e degli stessi praticanti, della parola hacker. Il capitolo 7 tratta del cosiddetto «hacktivismo», l'hacking messo al servizio di cause e proteste politiche, di nuovo mettendo in evidenza le peculiari modalità della loro comunicazione in un ambiente, quello del web, dove la distinzione tra comunicazione e azione è spesso ambiguo. Il volume si chiude con uno sguardo al presente e con un commento sull'«esplosione dell'hacking» in una miriade di attività anche molto diverse tra loro e in alcuni casi solo ispirate o impropriamente associate alla definizione originale.

Uno dei principali fili conduttori del libro è il rapporto tra gli hackers e i media. Come vedremo, giornali, televisioni e, in seguito, siti web non si limiteranno a raccontare gli hackers, ma, seguendo le proprie logiche di spettacolarità e commerciabilità della notizia, contribuiranno a forgiare le comunità hacker, le loro azioni e le loro aspettative. Gli hackers stessi impareranno a relazionarsi con i media e ad operare, o tentare di operare, hacks su di essi. Gli articoli di giornale citati in questo saggio sono spesso messi a confronto con una realtà ben diversa da quella in essi raccontata. Può sembrare ingiusto usare il senno di poi per evidenziare gli errori di chi, in molti casi onestamente, tentava di spiegare in tempo reale fenomeni che ancora oggi presentano molte difficoltà di lettura e comprensione. Ma, di nuovo, non è questo l'obiettivo. L'obiettivo è evidenziare come la realtà reagisca a questi errori di comprensione e di descrizione e come la cultura hacker si sia gradualmente avvicinata al racconto, inizialmente errato, che di essa si faceva.

Il focus principale e quasi esclusivo del libro sono gli Stati Uniti. Ciò è

dovuto tanto alla natura delle mie ricerche quanto alla storia del fenomeno narrato: come il cinema hollywoodiano o il rock'n'roll, l'hacking ha origine negli Stati Uniti e offre alle tante e importanti re-interpretazioni globali caratteristiche proprie della cultura e della storia statunitense. Ciò non significa che la conoscenza del fenomeno sia esaurita dall'analisi del contesto d'origine o da questo volume. Se saprà offrire un punto di paragone, di partenza o di dibattito a chi voglia intraprendere studi storici dell'hacking in altri contesti geografici o su scala globale, il libro avrà raggiunto uno dei propri obiettivi.

A proposito di questo saggio

Le principali fonti che hanno nutrito le interpretazioni di questo saggio sono, in ordine di importanza, le pubblicazioni autoprodotte dalle culture tecniche prese in considerazione («QST», «YIPL/TAP», «Phrack», «2600. The Hacker Quarterly» e vari messaggi BBS perlopiù tratti dall'archivio textfiles.com), la copertura mediatica statunitense (generalmente attraverso i quotidiani, ma anche via web), gli scritti autobiografici, le esperienze raccolte da altri studiosi e le interviste rilasciate dai protagonisti in vari media.

Il lavoro storico su fonti web è solo agli inizi, ma chi vi si è cimentato ha fatto notare le sue inedite insidie, soprattutto in relazione alla loro facile falsificabilità e alla loro scarsa longevità[29]. Per il primo problema non vi è una reale soluzione che non sia l'abilità dello storico e la sua conoscenza del contesto in cui le fonti sono prodotte e della credibilità degli archivi nei quali sono contenute. Per il secondo si è scelto, ogniqualvolta sia stato possibile, di non citare il sito web «live», che potrebbe essere diverso a seconda del momento in cui lo si consulta, ma una versione archiviata su Wayback Machine, il meritorio servizio di archiviazione del web offerto gratuitamente da Internet Archive. Questo stesso servizio ha permesso la consultazione di siti web che sono ormai scomparsi dalla rete, ma che sono essenziali alla ricostruzione della storia hacker. Nell'atto di archiviare le pagine citate nel saggio e non già presenti su Wayback Machine (possibilità aperta a chiunque lo voglia fare) le si è rese disponibili per la futura ricerca storica, indipendentemente dai cambiamenti futuri dei singoli siti.

I link citati appariranno dunque in nota come nel seguente esempio:

http://web.archive.org/web/20220119031924/https://www.laterza.it/

I primi otto numeri dopo web/ rappresentano l'anno (2022), il mese (01) e il giorno (19) in cui la pagina è stata «fotografata», dando informazioni sulla fonte e non sulla – spesso inutile – data dell'ultimo accesso di chi la cita. L'indirizzo che inizia con https è l'URL originale, nel caso il sito citato sia ancora online e il lettore sia interessato a consultarne l'ultima versione. Se si troverà in nota la citazione tradizionale del sito «live» sarà perché il gestore del dominio non permette l'archiviazione, spesso per motivi di diritto d'autore.

Dato che il volume è rivolto a un pubblico che non abbia necessariamente conoscenze informatiche o di storia dell'informatica, alla sua fine si troverà un glossario dei termini tecnici.

Infine, brevemente, i ringraziamenti. Il primo a mio padre, Guido Mazzini, cui il libro è dedicato. Prima di andarsene ci ha lasciati in un porto sicuro.

Il secondo a mia moglie, Yusi Guo. Mi piace pensare che è anche grazie alla storia raccontata in questo libro che abbiamo avuto modo di conoscerci.

Il terzo a Carlotta Sorba che, nonostante si occupi di argomenti molto diversi dai miei, mi ha seguito e sostenuto in tutta la prima parte della mia carriera, mentre mi occupavo di soldati geertziani, tecnologie immaginarie e infine hacker. Senza la sua convinzione del fatto che la storia e lo storico possono e devono assumersi dei rischi, studiando campi inesplorati e a prima vista controintuitivi, questo libro letteralmente non esisterebbe.

In ultimo, ma non per importanza, a Enrico Francia, che ha seguito e aiutato la gestazione di questo libro, arricchendo il suo contenuto, la mia fiducia in esso e soprattutto le mie giornate.

1 J. Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation*, W.H. Freeman & Co, San Francisco 1976, p. 113 (trad. it. *Il potere del computer e la ragione umana: i limiti dell'intelligenza artificiale*, Gruppo Abele, Torino 1987). Qui e

in seguito le traduzioni sono mie. Le pagine indicate si riferiscono sempre all'edizione originale.

2 Ivi, p. 115.

3 Ivi, p. 118.

4 Ivi, p. 184.

5 S. Turkle, *The Second Self: Computers and the Human Spirit* (1984), The MIT Press, Cambridge (Mass.) 2004 (trad. it. *Il secondo io*, Frassinelli, Milano 1985).

6 Ivi, p. 213.

7 S. Levy, *Hackers: Heroes of the Computer Revolution* (1984), O'Reilly Media, Sebastopol (CA) 2010 (trad. it. *Hackers: gli eroi della rivoluzione informatica*, Shake, Milano 1994).

8 P. Samson, *An Abridged Dictionary of the TMRC Language*, https://web.archive.org/web/20171125003208/http://www.gricer.com/tmrc/dictionary1959.html.

9 S. Brand, *Keep Designing. Discussions from the Hackers' Conference, November 1984*, in «Whole Earth Review», 46, 1985, pp. 44-55.

10 Levy, *Hackers*, cit., pp. 27-38.

11 L'espressione è ripresa dal romanzo di D. Coupland, *Microserfs*, Flamingo, London 1995 (trad. it. *Microservi*, Feltrinelli, Milano 1996).

12 Levy, *Hackers*, cit., p. 26.

13 Ivi, p. 11.

14 Rop Gonggrijp, *Hacker Perspective*, in «2600. The Hacker Quarterly», XXIV, 2007, 4, pp. 26-28.

15 P. Taylor, *Hackers: Crime in the Digital Sublime*, Routledge, London 1999.

16 T. Jordan, P. Taylor, *A Sociology of Hackers*, in «The Sociological Review», 46, 1998, 4, pp. 757-780.

17 D. Thomas, *Hacker Culture*, University of Minnesota Press, Minneapolis 2002.

18 Ivi, pp. XIII-XIV.

19 Ivi, p. 50.

20 D. Hebdige, *Subculture. The Meaning of Style*, Routledge, London 1979 (trad. it. *Sottocultura. Il fascino di uno stile innaturale*, Costa & Nolan, Genova 1990).

21 Thomas, *Hacker Culture*, cit., pp. 175-176.

22 G. Coleman, *The Political Agnosticism of Free and Open Source Software and the Inadvertent Politics of Contrast*, in «Anthropological Quarterly», LXXVII, 2004, 3, pp. 507-519; G. Coleman, A. Golub, *Hacker Practice. Moral Genres and the Cultural Articulation of Liberalism*, in «Anthropological Theory», VIII, 2008, 3, pp. 255-277.

23 G. Coleman, *The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld*, in «Anthropological Quarterly», LXXXIII, 2010, 1, pp. 47-72.

24 G. Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking*, Princeton

University Press, Princeton 2013.

25 G. Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, Verso, New York 2014.

26 «L'età d'oro del cracking», come è stata definita da T. Jordan, *A Genealogy of Hacking*, in «Convergence: The International Journal of Research into New Media Technologies», XXIII, 2017, 5, pp. 528-544.

27 F. Mazzini, *Mechanical Vaudeville. Popularization of Science and the Trivialization of War in the US (1915-1918)*, in *The Mediatization of War and Peace: The Role of the Media in Political Communication, Narratives, and Public Memory (1914-1939)*, a cura di C. Cornelissen e M. Mondini, Walter de Gruyter, Berlin 2021, pp. 61-76.

28 *Technoculture*, a cura di C. Penley e A. Ross, University of Minnesota Press, Minneapolis 1991.

29 N. Brügger, *Web History and the Web as a Historical Source*, in «Zeithistorische Forschungen/Studies in Contemporary History», IX, 2012, 2, pp. 316-325; F. Musiani, C. Paloque-Bergès, V. Schafer, B.G. Thierry, *Qu'est-ce qu'une archive du web?*, OpenEdition Press, Marseille 2019.

1.
Radio ham, 1900-1920

Giovani e tecnologia nella tecnocultura statunitense

Un robot gigantesco solcava la prateria del Far West, alla velocità di un treno, emettendo fumo dalle orecchie e dalla bocca. «La faccia era fatta di ferro, verniciata di nero, con occhi spaventosi e una tremenda bocca sogghignante». Al posto del petto aveva una fornace, al posto del naso una sirena da locomotiva. Vestiva un cappello a tuba, anch'esso di metallo, e trainava un carrello che conteneva il carbone e l'acqua che alimentavano il suo motore a vapore.

La meravigliosa macchina era invenzione di Johnny Brainerd, un ragazzino esile, gobbo e basso. Ma

> Questo nano, piccolo e malformato, aveva il dono di una mente incredibile. La sua creatività meccanica si avvicinava al meraviglioso [...] Sembrava non esserci limite alla sua inventività. Aveva creato una locomotiva, e poi un vaporetto, perfetti in ogni loro parte, anche nel minimo dettaglio, usando solo il suo coltello, un martello e un cesello. [...] Era diventato un maestro nell'arte della telegrafia senza alcuna assistenza[30].

Con questa descrizione si apre un fortunato libro per ragazzi, *L'uomo-vapore delle praterie*, uscito nel 1867 a firma di Edward S. Ellis. Si trattava di uno dei primi esempi di fantascienza popolare e del primo esempio di un nuovo sottogenere letterario, che è stato definito «edisonade» dal critico letterario John Clute[31] e «la risposta statunitense a Jules Verne» e «l'antecedente del moderno steam-punk» dallo storico della letteratura Nathaniel Williams[32]. I protagonisti di tale genere erano invariabilmente dei teenagers che sapevano rapportarsi alla tecnologia in maniera creativa, usandola per superare mirabolanti peripezie e vivere incredibili avventure. Ma la creatività tecnica, l'età e l'etnia non erano le uniche

caratteristiche che questi giovani immaginari, ispiratori di giovani lettori in carne ed ossa, condividevano con il futuro hacker. Come i grandi inventori americani cui erano ispirati (Edison, Bell, Morse, Maxim...), questi precoci inventori non avevano avuto una formazione universitaria: il loro rapporto con la tecnologia non nasceva dai libri, da una guida adulta o dalla riflessione teorica, ma da un processo autodidatta di prova ed errore – quello che Levy avrebbe probabilmente definito un «hands-on imperative». Indipendenza e individualismo erano al centro di tutte le narrazioni. Il mondo degli adulti, con la loro istruzione formalizzata, era intenzionalmente ridicolizzato dal genio innato del giovane inventore, «suggerendo ai lettori che la conoscenza tecnica può dare il diritto a un giovane di comandare gli adulti»[33].

L'edisonade avrebbe raggiunto il proprio apice di popolarità alla fine del XIX secolo, ma avrebbe in varie forme accompagnato l'intera storia culturale della tecnologia statunitense nel XX. Frank Reade (la cui serie inizia nel 1876, anch'essa con un automa a vapore nel Far West[34], e avrebbe visto più di 180 uscite) e Tom Swift (la cui prima serie inizia nel 1910[35] e ancora continua)[36] sono solo due dei più famosi «piccoli Edison» che, nel corso dei decenni, avrebbero inventato o creativamente migliorato motociclette, radio, aeroplani, carri armati e persino, negli anni Cinquanta, armi atomiche[37]. Il rapporto privilegiato tra maschio bianco, tecnologia, creatività e indipendenza dall'autorità adulta, che l'edisonade incarnava e volutamente propagandava[38], avrebbe parallelamente percorso l'idea popolare di scienza e tecnologia fino ai giorni nostri.

La letteratura non era peraltro l'unico medium che, a cavallo dei due secoli, promuoveva il mito del genio individuale e dell'apprendimento tramite la pratica, nonché il ruolo formativo che la tecnologia poteva avere per i più giovani. La divulgazione tecno-scientifica di inizio XX secolo veicolava gli stessi temi, in riviste riccamente illustrate e pensate per un pubblico di massa e non particolarmente colto o in manuali espressamente scritti per «tutti i ragazzi svegli che, nel vero spirito Yankee, prendono l'iniziativa e scoprono quello che sono capaci di fare»[39]. In un momento in cui l'impeto dell'innovazione scientifica si stava spostando dai singoli inventori a laboratori di ricerca industriali e

universitari, le riviste di divulgazione popolare si impegnavano a difendere il ruolo dell'individuo nel processo di innovazione. I lettori, e in particolare i più giovani, erano così incoraggiati a fare esperimenti con la radio, l'elettricità, la modifica di automobili e motociclette, e a creare modellini che imitavano gli ultimi ritrovati della tecnica. Il «boy genius», che grazie alla propria intelligenza riusciva a creare qualcosa di nuovo o a imitare una complessa tecnologia, era una figura centrale di questa narrazione. I lettori erano inoltre spinti a creare delle comunità che, attraverso la mediazione delle riviste e in particolare delle rubriche dedicate alle lettere, permettevano loro di scambiarsi informazioni tecniche, conoscere chi condivideva le loro passioni, dimostrare la propria capacità tecnica e sentirsi parte di un gruppo che trascendeva i limiti geografici e copriva l'intero territorio nazionale statunitense. Tra queste comunità nessuna aveva tante caratteristiche in comune con i futuri hackers quanto quella dei radioamatori, o «radio hams».

La radio da comunicazione a medium

La radio fu portata all'attenzione del grande pubblico sul finire del XIX secolo. Nel 1899 Guglielmo Marconi dimostrava, in un evento mediatico accuratamente preparato, la capacità della «sua» tecnologia di «parlare» a distanza in assenza di fili, comunicando a terra la cronaca in diretta dell'America's Cup, una competizione velistica, mentre le imbarcazioni erano ancora in mare e appena visibili dalla riva. La radio di Marconi era molto diversa dalla tecnologia che sarebbe diventata popolare solo vent'anni più tardi. L'inventore bolognese, al pari di tutti gli scienziati che negli anni precedenti avevano perfezionato la comunicazione attraverso onde elettromagnetiche, pensava infatti alla radio come a una sostituzione del telegrafo, da usarsi in tutte quelle situazioni nelle quali non era possibile stendere un filo (come la comunicazione tra navi o in zone particolarmente impervie). Come il telegrafo, la prima radio non trasmetteva voce o musica, ma codice Morse. Come il telegrafo essa doveva, almeno in teoria, mettere in comunicazione due punti: il fatto che le onde radio fossero captabili da qualsiasi apparecchio ricevente era visto come un difetto (che Marconi avrebbe instancabilmente tentato di risolvere) e non come la caratteristica

che avrebbe determinato il successo della tecnologia come mass medium. Come il telegrafo, infine, la radio doveva essere utilizzata, nella concezione di Marconi, da operatori altamente specializzati, per trasmettere messaggi abbastanza importanti da giustificare la spesa che l'assunzione di un telegrafista comportava. L'idea di Marconi era quella – per usare termini che al tempo non esistevano – di una tecnologia estremamente «chiusa» e proprietaria. Marconi avrebbe concesso i propri apparati e i propri operatori sotto licenza e questi avevano il mandato di comunicare soltanto con altri operatori Marconi – almeno fino a che la legislazione internazionale non costrinse la Marconi Company a rispondere perlomeno ai casi di emergenza.

L'apparato necessario per la trasmissione era in realtà semplice, relativamente economico e, per gli standard di solo pochi anni dopo, rudimentale: una scintilla creata da un generatore o da una batteria in uno spinterometro produceva oscillazioni del campo elettromagnetico che circondava un'antenna e le proiettava in tutte le direzioni, come le onde di un sasso lanciato in uno stagno. Il mittente, aprendo e chiudendo un circuito tramite un *clicker* da telegrafo, attivava e disattivava la scintilla, trasmettendo le linee e i punti del codice Morse. La stazione ricevente, tramite un coesore o un cristallo di silicone, captava le onde elettromagnetiche e le traslava in forma sonora, una serie di «beep» più o meno lunghi che venivano annotati e tradotti dall'operatore, da Morse a caratteri latini. Ma la difficoltà nell'apprendere il codice Morse e l'assunto che nessuno avrebbe avuto interesse a comunicare attraverso di esso al di fuori dei pochi grandi attori istituzionali che già usavano il telegrafo erano visti come garanzie sufficienti del fatto che la radio non sarebbe diventata una tecnologia domestica e di uso quotidiano.

A sfidare questa concezione della tecnologia intervennero, quasi immediatamente, i giovani appassionati e autodidatti che erano stati preparati, sul finire del secolo precedente, dalla letteratura e dalla divulgazione scientifica. Come scrive Clinton B. DeSoto negli anni Trenta, essi

> si trovavano soprattutto negli Stati Uniti, dove l'arte della sperimentazione elettrica aveva già [al momento delle dimostrazioni di Marconi] raggiunto una considerevole popolarità. Negli ultimi anni del XIX secolo esisteva un gruppo consistente di questi sperimentatori, di tutte le età, che facevano piccoli elettromagneti, motori, batterie,

generatori elettrostatici, che erigevano linee telegrafiche, e che costruivano tutti gli altri apparati sperimentali a loro portata – solo come hobby, senza alcun interesse commerciale[40].

A partire dagli anni Dieci del Novecento questi «appassionati disordinati, pazienti, dagli occhi avidi, animati da una curiosità insaziabile e non scoraggiati da mille fallimenti»[41], si sarebbero riuniti in club e associazioni, spesso su base locale. Le riviste di divulgazione scientifica e anche alcune pubblicazioni generaliste cominciarono a includere articoli sul funzionamento della radio e istruzioni tecniche su come costruirsi un apparecchio in casa. Hugo Gernsback, uno dei padri della moderna fantascienza letteraria, fondava nel 1908 «Modern Electrics», che nel 1913 sarebbe diventata «Electrical Experimenter», rivista perlopiù dedicata all'hobby della «telegrafia senza fili». Nello stesso anno nasceva «Wireless Age», organo semi-ufficiale della Marconi Company. La radio sembrava così avviata, negli Stati Uniti, su due strade parallele: quella delle comunicazioni marittime e transoceaniche (già nel 1901 Marconi aveva, in un altro evento sapientemente pubblicizzato, trasmesso la lettera S attraverso l'Atlantico) e quella dell'hobby di nicchia, intrapreso da un appassionato ma relativamente sparuto gruppo di giovani «tinkerers»[42].

Le due attività sarebbero però presto entrate in conflitto. Fin dagli anni Dieci le autorità lamentavano il fatto che gli amatori potevano ascoltare le comunicazioni ufficiali e in alcuni casi persino intervenire, con scherzi, provocazioni o false richieste di soccorso[43]. Varie proposte di legge erano state avanzate per limitare l'uso ricreativo della radio, ma avevano incontrato l'opposizione di club, riviste specializzate e soprattutto della stampa nazionale. Per la prima volta uno Stato si trovava a voler regolare uno spazio immateriale come lo spettro elettromagnetico. La regolamentazione dell'«aria» nella quale viaggiavano i messaggi radio sembrava ai più un'ingerenza ingiustificata del governo nelle libertà individuali. Gli stessi sostenitori del controllo statale riconoscevano peraltro il legame, ormai ritenuto indissolubile, tra sperimentazione tecnologica e gioventù statunitense e si impegnavano a non «privare i tanti brillanti ragazzini americani con inclinazione alla scienza di un passatempo innocuo e costruttivo, dal quale il paese può ricavare il

beneficio di future invenzioni». I vantaggi della regolamentazione erano però sostenuti con metafore ben più allarmistiche: dopotutto «in tutte le grandi città è necessario un permesso perché un ragazzino possa avere un revolver che può sparare a una singola persona [...] Il wireless usato dagli amatori può interferire con messaggi di soccorso da una nave con centinaia di vite a bordo»[44].

Nell'aprile 1912 affondava, nel suo viaggio inaugurale da Southampton a New York, il transatlantico Titanic, causando la morte di circa 1.500 passeggeri. L'impressione sull'opinione pubblica statunitense e mondiale fu immensa. L'intensa copertura giornalistica del tempo evidenziò che i soccorsi erano stati in qualche modo ostacolati dall'intrusione degli amatori. In realtà non esistevano al tempo stazioni amatoriali in grado di raggiungere il luogo dove il transatlantico era affondato. Ma la confusione che regnava nella comunicazione radio costiera in corrispondenza della tragedia, e insieme il sospetto, mai provato ma incessantemente denunciato dai giornali, che gli amatori avessero interferito con le notizie che arrivavano dall'Atlantico, furono sufficienti a convincere la stampa (che dipendeva dalla comunicazione telegrafica e radio per il proprio approvvigionamento di notizie), e di conseguenza l'opinione pubblica, della necessità di un intervento legislativo.

A pochi mesi dalla tragedia del Titanic passava così al Congresso il *Radio Act*[45]. La legge prevedeva che gli amatori che volessero non solo ascoltare, ma anche trasmettere, ottenessero una licenza dal Dipartimento del Commercio e potessero usare soltanto onde sotto i 200 metri di ampiezza e stazioni che non superassero la potenza di 1 Kw. Alla Marina e alle compagnie di radiotelegrafia era riservata la parte ritenuta più efficiente dello spettro elettromagnetico. Come fa notare Susan Douglas, la legge segnava la fine della libera esplorazione della frontiera dell'etere e l'inizio della gestione e dello sfruttamento da parte di governo e corporations. Gli amatori sembravano condannati alla riserva dei 200 metri, e forse a scomparire[46].

La limitazione fu tuttavia interpretata come uno stimolo all'inventività e alla sperimentazione. Laddove la distanza era raggiunta dagli operatori commerciali semplicemente costruendo stazioni più potenti ed antenne più alte, «gli amatori dovevano cavarsela con molto meno, rivolgendosi al

perfezionamento delle proprie piccole stazioni e all'affinamento della loro tecnica»[47]. A soli dieci anni dal passaggio del *Radio Act* le onde corte (sotto i 100 metri) sarebbero state utilizzate per il primo contatto amatoriale attraverso l'Atlantico[48]. Il superamento della difficoltà tecnica imposta dal governo sarà rivendicato con orgoglio dai radioamatori per tutto il XX secolo.

Non era però tutta questione di ingegno e passione. Nel 1912 la diffusione dell'audion, un vacuum tube utilizzato per la ricezione e trasmissione delle onde radio, rese gli apparecchi amatoriali più potenti e meno costosi e l'imposizione dei 200 metri meno limitante. L'invenzione è generalmente attribuita all'imprenditore Lee De Forest, che l'avrebbe brevettata e inizialmente distribuita. Ma l'opinione degli amatori era che il merito andasse a Edwin Armstrong, un radioamatore che fin dall'età di quindici anni «si era lanciato nell'affascinante gioco del wireless» e che aveva modificato l'audion per renderlo più efficiente, inserendovi un circuito rigenerativo. Al di là delle dispute di attribuzione, che le corti decisero in favore di De Forest[49], è interessante notare che Armstrong è descritto negli stessi termini in cui saranno descritti gli hackers della fine del Novecento: aveva sperimentato, nel proprio attico di casa e con mezzi limitati, spinto dalla passione per l'hobby e dalla fiducia che ogni apparecchiatura può essere migliorata.

> Un giovane amatore ventiduenne avrebbe fatto la scoperta che avrebbe rivoluzionato l'intera arte della radio, una scoperta a lungo cercata dai migliori scienziati del tempo in questo paese e in Europa. [...] Il resto del mondo degli amatori si mise al lavoro per trasformare in pratica il frutto delle ricerche, ormai di importanza storica, di Armstrong e di tanti altri[50].

La tragedia del Titanic aveva per la prima volta messo in cattiva luce il giovane appassionato che si interessava di tecnologia. Ma aveva anche provato l'importanza della radiotelegrafia e messo sotto i riflettori gli operatori che avevano permesso, anche a costo della propria incolumità, di salvare quasi metà dei passeggeri del transatlantico. Nonostante il *Radio Act* la comunità dei radioamatori continuò così a crescere: nel 1913 erano state rilasciate appena 507 licenze[51]; nel 1916 il numero sarebbe salito a più di diecimila, ma gli operatori abusivi erano stimati in cifre dieci volte

superiori[52] (si ricordi inoltre che per ascoltare e per trasmettere all'interno del proprio Stato non era necessaria la licenza).

Nel 1914 Hiram Percy Maxim (figlio dell'inventore della mitragliatrice) fondò l'American Radio Relay League (ARRL), che sarebbe diventata la più importante associazione di radioamatori negli Stati Uniti e nel mondo. L'obiettivo era, almeno in parte, quello di superare il limite dei 200 metri e della potenza delle stazioni, organizzando una sorta di network di comunicazione distribuito che permettesse l'invio di un messaggio in tutti gli Stati Uniti. Il network rimarrà perlopiù un'aspirazione, ma la Lega, grazie anche alla sua rivista («QST», pubblicata dalla fine del 1915), sarebbe diventata, come vedremo a breve, uno dei principali luoghi di ritrovo e confronto degli amatori.

L'entrata degli Stati Uniti nella prima guerra mondiale, nell'aprile del 1917, determinò la chiusura di tutte le stazioni non governative e l'interruzione delle attività amatoriali fino al 1919. Ma la guerra portò anche a una rivalutazione dell'hobby, grazie all'importanza della comunicazione wireless in trincea e al vantaggio rappresentato dall'ampia disponibilità di potenziali reclute già addestrate all'uso del Morse e della radio. Alla riapertura delle stazioni il numero dei radioamatori negli Stati Uniti avrebbe continuato a salire.

La rivoluzione dell'uso della radio era però ancora da compiersi. L'audion permetteva, al contrario del sistema a scintilla, di trasmettere onde continue e perciò voce e musica. I primi esperimenti nel campo furono fatti prima della guerra dallo stesso Lee De Forest, che trasmetteva musica, notizie e messaggi pubblicitari[53]. Dopo la guerra un altro amatore, Franz Conrad, impiegato di una compagnia di hardware radiofonico, la Westinghouse, decise di usare l'attrezzatura dell'azienda per trasmettere, ogni sabato sera, concerti preregistrati e anche musica dal vivo – per l'unico pubblico allora in grado di ricevere onde radio, quello dei radioamatori. La dirigenza dell'azienda si accorse del successo dell'esperimento e soprattutto del fatto (risaputo dagli amatori ormai da quindici anni) che la comunicazione interpersonale non era l'unico uso della radio. Franz Conrad ricevette un'attrezzatura più potente ed ebbe la possibilità di trasmettere con regolarità. Nel 1920 nasceva così KDKA, la prima stazione di radio broadcasting al mondo. L'anno successivo le

stazioni sarebbero diventate 28, quello ancora successivo 550. Era l'inizio di quella che è stata definita «la mania della radio» («radio craze») degli anni Venti, un processo di rapidissima diffusione degli apparecchi riceventi che avrebbe rivoluzionato, tra le altre cose, la comunicazione politica, l'intrattenimento, l'informazione. Gli amatori ebbero in questo processo un ruolo centrale, sia come primo pubblico sia come facilitatori nei confronti di aspiranti ascoltatori meno capaci tecnicamente. Ma il loro ruolo fu ancora più importante nel chiudere il periodo di «flessibilità interpretativa»[54] della radio, trasformandola dallo strumento di comunicazione interpersonale immaginato da Marconi nel mezzo di comunicazione di massa che oggi conosciamo. Questo fu il risultato non di uno sforzo conscio e pianificato, ma di mille sperimentazioni volte ad esplorare, per divertimento, passione e volontà di appartenere a una specifica comunità, le possibilità della tecnologia e i confini di uno spazio immateriale. Fu il risultato di una cultura che vedeva tra i propri valori fondanti il rapporto creativo con la tecnologia. Nel seguente paragrafo esamineremo alcune delle caratteristiche di questa cultura e il suo rapporto con la futura cultura hacker.

Cultura ham

È dalle pagine di «QST», la rivista della ARRL pubblicata dal 1915 e ancora oggi in stampa[55], che è possibile intravedere cosa significasse essere un radioamatore nel primo quarto del XX secolo. L'appassionato doveva costruirsi la propria apparecchiatura da solo, in special modo prima che si sviluppasse, dalla metà degli anni Venti, un mercato di pezzi di ricambio e di apparecchi pronti per l'uso. Anche quando i pezzi erano venduti come finiti o semi-finiti essi dovevano essere assemblati, spesso in mancanza di precise istruzioni da parte del produttore. Queste dovevano essere ricavate dalla sperimentazione e dal confronto con altri amatori e con le riviste specializzate.

Un radioamatore ricorda, nel 1917, cosa aveva dovuto fare, appena quattordicenne, per placare la propria «malattia» (*bug* – il modo in cui i radioamatori del tempo indicavano il proprio bisogno insopprimibile di interagire con la tecnologia): «Sono andato in una biblioteca pubblica e ho preso un libro che parlava dei primi esperimenti di Marconi. Il libro

menzionava i pezzi necessari, ma non essendo possibile comprarli dovevo per forza costruirmeli». Il primo elemento era il ricevitore: «Ho preso una piccola bottiglia, spezzato il collo, inseriti due tappi nel tubo e ho coperto il tutto con un foglio d'alluminio. Poi sono andato di nuovo a cercare nella spazzatura»[56]. Dopo aver ricavato i fili di argento da una moneta l'amatore passò all'antenna, ricavata da un palo stenditoio sul tetto di casa sua, isolata tramite un copertone da bicicletta. Nel suo apparecchio sarebbero in seguito stati aggiunti pali da tenda, barattoli da cucina, uncini e chiodi. Può darsi che l'appassionato, nello spiegare ai lettori di «QST» la propria esperienza, esagerasse il proprio talento e la propria capacità di convertire oggetti domestici in apparecchiatura radiofonica. Ciò che è certo è che già dall'inizio del secolo una comunità di giovani appassionati vedeva nella modifica creativa della tecnologia e nell'apprendimento attraverso l'esperienza dei valori fondamentali: «A quei tempi nulla poteva essere comprato – tutto doveva essere fatto in casa. [...] Dover costruire una cosa è il modo migliore di capire come quella cosa funziona»[57].

Dopo il lavoro sull'«hardware» veniva l'effettiva comunicazione via radio. La maggior parte delle attività aveva luogo di notte, poiché le onde si propagavano più facilmente, e d'inverno, poiché le frequenze erano meno disturbate. Cuffie sulle orecchie, dito sul *clicker* da telegrafo (almeno nei casi in cui l'apparecchio poteva sia ricevere che trasmettere), il radioamatore si trovava infine nell'«etere». Il concetto di etere, una sostanza invisibile e impalpabile nella quale le onde elettromagnetiche si sarebbero propagate come le onde nel mare, era stato scartato dai circoli scientifici già all'inizio del Novecento. Ma la parola continuava ad essere usata dagli amatori e dalla stampa come mezzo per dare materialità a un mondo che si esplorava con l'udito, fatto di suoni esotici e misteriosi, accessibile solo a pochi fortunati iniziati.

L'amatore si metteva prima di tutto in ascolto, annotando il codice Morse che gli capitava di sentire e traducendolo al meglio delle proprie capacità, con particolare attenzione alle informazioni riguardanti il luogo dal quale il suono proveniva: la sfida, chiamata in gergo «DXing», era quella di raggiungere stazioni il più lontano possibile, prova sicura della qualità dell'apparecchio ricevente e delle capacità di chi lo aveva

costruito. Ad ogni stazione era attribuito, al momento del rilascio della licenza, un codice che conteneva informazioni sull'area in cui essa si trovava. In questo modo chi avesse sentito un messaggio di «W1MK» poteva essere sicuro che esso proveniva dal New England. In aggiunta, la ARRL mandava ai propri iscritti dei «Blue Books», elenchi che associavano al nome della stazione quello del suo proprietario e il suo indirizzo postale. Una volta che il contatto tra due amatori fosse stato stabilito nell'etere, esso veniva spesso sancito dall'invio di una cartolina (detta «QSL card», a volte personalizzata dal singolo amatore) che indicava la posizione della stazione raggiunta e andava a far parte della collezione di trofei dell'ham.

Dato che non vi era modo di contattare una singola stazione se non chiamando ripetutamente e pubblicamente il suo codice, l'amatore doveva, prima di trasmettere, attendere che vi fosse silenzio. L'esperienza dell'etere, basata com'era sull'auto-moderazione di hams spesso molto giovani, entusiasti e dalle capacità diseguali, poteva essere caotica, in special modo nei centri cittadini, dove si concentravano diverse stazioni amatoriali, o in prossimità dei porti, dove più intensa era la comunicazione radio «ufficiale»:

> Ora, proprio mentre scrivo, quel vecchio cretino di 2AGJ a York State sfarfalla con quella sua scintilla che sembra un uccello in gabbia. 8YO strilla come un matto cercando di contattare qualcuno nella costa del Pacifico, 8HN sta facendo del suo meglio per rimanere cortese a scapito di un'intera ora di tribolazioni [...], ho sentito distintamente 4DI dire una parolaccia, e per quello che posso vedere, nessuno ha concluso niente[58].

Ma quando tutto andava per il meglio la sensazione era quella di superare magicamente la distanza, proiettandosi, grazie alle proprie competenze tecniche e dalla comodità della propria casa, in luoghi prima inaccessibili:

> Dopo aver pianificato tutta l'estate e aver lavorato nel tempo libero, avevo finalmente completato il mio apparecchio ed ero pronto per un test. Ho ascoltato e ho avuto il piacere di sentire 8FJ e 8YL per due ore e mezza prima di poter intervenire. Infine è arrivato il mio turno e ho provato a contattare 8TI a Tuffin, Ohio, a sessanta miglia di distanza. Mi ha risposto immediatamente [...] Sono andato a letto pensando che era un ottimo inizio. Provate a immaginare la mia estasi quando, pochi giorni dopo, ho ricevuto una cartolina da 9BD, a Superior in Wisconsin, che diceva di aver ascoltato la

mia conversazione con 8TI e che il mio segnale era chiaro a quella distanza, 600 miglia[59].

Tale ebbrezza poteva somigliare a una dipendenza. Gli amatori di inizio secolo chiamavano la propria passione «bug» (che in inglese vuol dire sia «malattia», «lieve malanno», che «insetto») e, di conseguenza, sé stessi «bugs» (insetti). La parola «ham» si sarebbe imposta solo negli anni Venti. La descrizione, pur scherzosa, di questa dipendenza ricorda la figura, dipinta da Weizenbaum e riprodotta incessantemente dagli anni Ottanta, dell'hacker ossessionato, socialmente inetto, dai vestiti raffazzonati e dalla scarsa igiene:

> Il «Bug» [...] ti morde quando meno te lo aspetti. Tra i sintomi più evidenti che possono essere notati dopo un morso possono essere menzionati: insonnia, dilapidazione del portafogli, perdita della futura Salvezza, scolorimento delle mani, favella non comprensibile, occasionale rigonfiamento della testa, cleptomania nei confronti del filo di rame senza casa e a volte persino cessazione delle relazioni diplomatiche con la famiglia. [...]

Anche l'ostilità verso le aziende che si occupavano di comunicazione, tipica dei phreaks e degli hackers dagli anni Settanta, trova un occasionale parallelo nella percezione ham. La citazione precedente continua: «Il Wireless Bug come ogni altra cosa ha i suoi nemici naturali, tra i quali i più importanti sono Electric Lighting Co., la Compagnia Telefonica, le Interferenze»[60].

La stessa esplorazione dell'etere, per come emerge dalle pagine di «QST», ha molti punti in comune con l'esplorazione dei sistemi informatici così come è stata descritta dagli hackers e da chi li ha studiati. La curiosità e la volontà di imparare sperimentando erano, in entrambi i casi, le motivazioni esplicitamente addotte per spiegare a sé stessi e agli altri il perché si intraprendeva la pratica. Ma, appena sotto la superficie, vi erano due motivazioni altrettanto importanti: da una parte la volontà di appartenere a una comunità di iniziati, definita da specifiche competenze, da uno specifico gergo, da valori e miti propri e da sfide collettive; dall'altra la volontà di distinguersi all'interno di questa comunità, mostrando agli altri membri la propria capacità tecnica e l'efficienza del proprio apparecchio.

Le comunità ham esibiscono, fin dai primi anni del Novecento, un

particolare rapporto tra estremo individualismo e offerta volontaria dei risultati delle proprie scoperte e azioni individuali alla comunità. Il merito (della capacità tecnica, dell'inventività) era individuale, ma acquistava valore solo nel momento in cui veniva volontariamente condiviso e riconosciuto dalla comunità dei pari. Lo spiega Clinton DeSoto in un passaggio risalente agli anni Trenta, ma che potrebbe perfettamente essere applicato ai phone phreaks degli anni Settanta (vedi capitolo seguente) e agli hackers degli anni Ottanta e Novanta, in particolare quelli che hanno fondato i movimenti Free Software e Open Source (vedi capp. 5 e 6):

> La rivalità per fare qualcosa che non è mai stato fatto prima è intensa, ma è una rivalità amichevole, e non appena qualcuno riesce a stabilire un nuovo record vuole immediatamente far vedere ai propri fratelli amatori non solo come lo ha fatto, ma come può essere replicato. Tutti capiscono che un nuovo record nel campo della radio non è un risultato personale, ma un risultato della radio. Se un amatore contatta una stazione distante telefona a tutti i suoi amici e prende appuntamenti per loro [perché anch'essi si possano mettere in contatto con la stazione]. Se un nuovo collegamento si sviluppa, o un nuovo aggiustamento è scoperto, che migliora l'efficienza e la performance, esso è immediatamente condiviso con il radio club locale o sulle pagine di una rivista per amatori. Il minimo avanzamento della tecnica, ogni scoperta individuale, ogni osservazione promettente è immediatamente proprietà di tutti[61].

La formazione dei neofiti e la coesione della comunità passano dunque per la continua discussione del medium che permette la comunicazione stessa, in una manifestazione *ante litteram* di quella che Christopher Kelty ha chiamato «pubblico ricorsivo» (vedi prossimo capitolo)[62]. È difficile sopravvalutare l'importanza che, all'interno di queste comunità, rivestiva l'esistenza di riviste cartacee e autoprodotte. Attraverso di esse avvenivano la formazione e il reclutamento dei neofiti. Quasi tutti gli articoli erano scritti da amatori, che mettevano in comune le proprie esperienze e le proprie capacità, consigliavano letture, rispondevano a domande dei meno esperti, esprimevano raccomandazioni e rimbrotti sulla corretta etichetta da tenere nell'etere. Tra le regole di cortesia vi erano il non eccedere nell'uso dell'appellativo «OM» (Old Man, vecchio mio) o altre espressioni ricorrenti, l'indicare con chiarezza l'inizio e la fine di un messaggio, l'astenersi dall'usare apparecchiature scadenti che potevano creare interferenze per tutti gli altri. Ma al contempo si

consigliava di non essere eccessivamente severi con chi sgarrava, poiché «anche l'interferer [chi crea interferenze] può diventare un buon operatore se non è cacciato dal gioco»[63].

Grazie alle riviste gli amatori potevano far mostra delle proprie capacità tecniche, pubblicando foto dei propri apparecchi circondati dalle cartoline che provavano il numero e la distanza delle stazioni raggiunte, scrivendo articoli che descrivevano le proprie scoperte, pubblicando lunghe liste dei codici che si erano sentiti nell'etere, nella speranza che un lettore si riconoscesse e volesse inviare una cartolina. «QST», come la rivista «Phrack» settant'anni dopo, avrebbe anche pubblicato profili biografici di alcuni radioamatori, con la lista dei loro successi e la foto del loro apparecchio.

Soprattutto le riviste permettevano a un pubblico disperso geograficamente, e che aveva contatti sporadici e spesso aleatori (basati come erano sui capricci del tempo, della stagione e di apparecchi fatti in casa), di sentirsi parte di una comunità nazionale e internazionale, fatta di individui che condividevano passioni, attitudini e valori (oltre che genere e classe sociale). Una comunità «virtuale» era resa possibile dallo spazio immateriale dell'etere e dalla materialità di una rivista che veniva recapitata ogni mese nella casella della posta.

«QST», «Electrical Experimenter» e le tante riviste a diffusione locale avevano anche un'ulteriore funzione: quella di coordinare gli sforzi della comunità in sfide collettive. La più importante, nei primi anni di vita della pratica, era quella dalla quale la American Radio Relay League prendeva il proprio nome: la creazione di un «passaparola» (*relay*) che potesse trasmettere un messaggio in maniera affidabile da costa a costa.

Il sistema prevedeva la creazione di sei linee dorsali («trunk lines», espressione presa dalla telefonia, che indica le direttive di maggiore traffico) tra le città principali, nelle quali amatori particolarmente devoti e capaci assicuravano la propria presenza e la trasmissione dei messaggi. Le stazioni più affidabili sarebbero state nominate «Star Stations» e sarebbero state raccomandate dalla ARRL per ricevere dal governo una licenza speciale che permettesse loro di trasmettere con maggiore potenza[64]. Ogni dorsale avrebbe avuto un quartier generale, locato nei punti di congiunzione delle diverse linee, e uno o più coordinatori, che

avrebbero gestito il servizio di passaparola non solo con la radio ma anche attraverso lettere e telefoni. Un messaggio di test di ogni singola linea avrebbe dovuto essere mandato almeno una volta alla settimana, tra le 10 e le 11 di sera. Questo doveva essere una password segreta e sempre diversa, in modo da poter verificare gli amatori che lo avessero effettivamente ricevuto[65]. Dal luglio 1916 «QST» avrebbe pubblicato ogni mese i rapporti dei coordinatori delle linee, per aggiornare i soci sullo stato della sfida collettiva.

Un esperimento avvenne alla fine del febbraio 1916, nell'anniversario della nascita di George Washington e prima ancora che le linee dorsali fossero stabilite. In un momento in cui il paese era assorbito dai dibattiti sulla necessità di essere preparati all'ingresso nella guerra mondiale, «l'obiettivo era quello di mostrare al governo degli Stati Uniti che gli amatori statunitensi sono nella posizione di poter cooperare nel campo della radio», inviando un messaggio relativamente complesso dall'Illinois all'intera nazione e chiedendo di farlo arrivare alle autorità politiche dei vari Stati. Il testo, firmato dal colonnello W.P. Nicholson, recitava: «Una Democrazia richiede che un popolo si governi ed educhi sé stesso perché sia armato e disciplinato per proteggere sé stesso» e raggiunse dopo un'ora entrambe le coste. Il messaggio fu un successo mediatico, riportato come fu da diversi giornali.

Il progetto di più lungo periodo era quello di creare una sorta di «network distribuito», nel quale ogni nodo (corrispondente a una stazione amatoriale) avesse multiple connessioni agli altri nodi, in modo che, nel caso uno dei nodi fosse stato fuori gioco (ad esempio se l'operatore non era davanti alla radio), il messaggio avrebbe potuto intraprendere altri percorsi. Il parallelo con i moderni networks distribuiti digitali è solo casuale (quando essi si svilupperanno lo faranno a partire da altre preoccupazioni e con altre ispirazioni)[66], ma è tuttavia evidente ed evocativo. Nonostante le affermazioni della ARRL (il network sarebbe stato di grande utilità per raggiungere aree remote e in caso di emergenza), è impossibile non notare che già esisteva un network capace di comunicare da costa a costa: quello telefonico. L'enorme sforzo organizzativo non aveva, in ultima analisi, un obiettivo utilitaristico: come nel caso di altre sfide tecniche collettive che vedremo nei prossimi

capitoli, lo scopo era principalmente quello di impegnare gli amatori in una causa comune, rinsaldando i legami interni, evidenziando una gerarchia basata sulle capacità tecniche e caratterizzando l'intero hobby come qualcosa che andava al di là del semplice diletto. Questo è evidente nell'orgoglio che segue all'esperimento del febbraio 1916 («È stata una causa comune: ricchi, poveri, giovani, vecchi, due donne, una legione di ragazzini e diversi preti») e negli aneddoti che sono associati all'episodio (un uomo malato si era messo alla radio contro gli ordini del suo dottore, pur di non interrompere il passaparola; un cittadino di Washington si era presentato alla Casa Bianca per portare il messaggio trascritto; un altro, impossibilitato a portare fisicamente il messaggio al governatore della Virginia, aveva addirittura fatto ricorso al «vecchio e fuori moda sistema del telegrafo»)[67], ma anche nelle discussioni che seguono ai vari esperimenti, volte a correggere gli errori tecnici e a deprecare quelli sociali (come l'eccessivo protagonismo di alcuni amatori).

La comunità dei radioamatori aveva, come abbiamo brevemente visto, un proprio specifico argot («bug», «junking», a indicare la pratica di usare nei propri apparecchi materiali di recupero, «rag-chewing» – masticare lo straccio – per indicare una lunga conversazione via radio, «raise» – evocare – per indicare il contatto con una stazione). Ma a questo si aggiungeva, e nell'etere si sostituiva, il linguaggio del codice Morse e delle sue abbreviazioni. Uno scambio poteva dunque apparire come in questo esempio risalente al 1931, citato e tradotto dal Morse da Richard Bartlett:

W9FYK DE VK7HL R = TKS For CALL OM = UR SIGS QSA5R7 HR IN WEST HOBART TASMANIA? WEST HOBART TASMANIA = HW? AR W9FYK DE VK7HL K

A W9FYK da VK7HL, ricevuto. Grazie per la chiamata vecchio mio. Il tuo segnale ha forza eccellente ed è facilmente leggibile qui a West Hobart in Tasmania [il luogo è ripetuto poiché è la parte più importante della comunicazione]. Come è il mio segnale? A W9FYK da VK7HL passo.

VK7HL DE W9FYK R = TKA OM FOR CMG BACK = UR SIGS QSA4R5 XDC HR BOULDER COLORADO? BOULDER COLORADO = VY PSED TO QSO = UR MY FIRST VK7 ES WUD LIKE A QSL = MY QRA OK IN CALL BOOK AR VK7HL DE W9FYK K

A VK7HL da W9FYK, ricevuto. Grazie vecchio mio per la risposta. Il tuo segnale ha

forza buona ed è leggibile a velocità moderata qui a Boulder in Colorado [ripetuto]. Molto contento di questo contatto. Sei il mio primo VK7 [cioè il primo contatto dall'Australia] e vorrei una QSL Card. Il mio indirizzo è corretto nell'elenco. A VK7HL da W9FYK passo[68].

Conversazioni di questo tipo avvenivano, almeno fino agli anni Venti inoltrati, non oralmente, ma attraverso combinazioni di suoni più o meno lunghi che simboleggiavano le singole lettere, che dovevano essere pazientemente trascritte e riunite in parole, a scapito delle interferenze, del sovrapporsi delle voci e dei possibili errori della propria controparte. Per questo la capacità di usare il codice Morse in maniera veloce ed efficiente aveva, nei circoli amatoriali, un'importanza pari alla capacità di costruire il proprio apparecchio. Come nel caso degli hackers, parti del linguaggio tecnico entravano nel parlato e nella scrittura quotidiana, come provato dal titolo di «QST» (abbreviazione Morse per «chiamata a tutte le stazioni»), ma anche dalla citata pratica del DXing (DX è abbreviazione di «distanza») o dall'onnipresenza di OM nelle pagine delle riviste. Il codice rivestiva un ruolo simile a quello che la conoscenza dei linguaggi di programmazione avrebbe avuto nelle comunità informatiche: un linguaggio altamente specialistico, che richiedeva dedizione e talento per essere appreso e il cui uso marcava il confine tra la comunità di iniziati e il resto del mondo e quello tra un ham di successo e uno mediocre.

La conoscenza del Morse non era peraltro soltanto un requisito informale per appartenere alla comunità ham. Per ottenere la licenza ogni amatore doveva passare, come abbiamo detto, un esame. Questo testava la capacità di costruzione e riparazione di un apparecchio, la comprensione della tecnologia e della scienza della radiofonia, la conoscenza delle leggi nazionali e internazionali sulla radiotelegrafia e la velocità con la quale il candidato inviava e riceveva un messaggio Morse. A seguito del suo superamento e di una eventuale ispezione dell'apparecchiatura sarebbero stati rilasciati la licenza e l'agognato codice della stazione, che sarebbe divenuto anche il nome con il quale l'amatore sarebbe stato chiamato all'interno del circolo di appassionati. L'acquisizione della licenza, dapprima avversata e spesso aggirata, divenne così un evento importante, un rito di passaggio che non di rado

comportava il viaggio in una grande città per raggiungere un ispettore radio[69] e che segnava l'ingresso ufficiale nella comunità[70].

L'importanza della licenza rilasciata dallo Stato evidenzia una differenza tra i radioamatori di inizio Novecento e i phreaks e hackers che li avrebbero seguiti. Laddove i secondi, come si vedrà, mostreranno una spiccata diffidenza verso ogni forma di potere costituito, e troveranno nell'autorità più un polo attraverso il quale definirsi per differenza che non un possibile alleato, i primi cercavano incessantemente l'approvazione delle autorità e il riconoscimento pubblico del proprio hobby. La fondazione dell'ARRL e il suo progetto di creare un network di comunicazione nazionale erano stati comunicati al Department of Commerce e alla Marina, in quanto «impegni patriottici». Le autorità in cambio avevano concesso che alcuni nodi della rete, indicati dalla Lega, potessero operare oltre i limiti di potenza e di frequenza imposti dalla legge[71].

Al momento dell'entrata degli Stati Uniti nella prima guerra mondiale e della chiusura di tutte le stazioni amatoriali la reazione degli hams non fu di oltraggio o di ostilità, ma di sostegno alla decisione, perlomeno nelle comunicazioni ufficiali. Hiram Maxim firmò una risoluzione nella quale impegnava la ARRL non solo a mettere fuori uso tutte le stazioni dei suoi membri, ma anche a scovare e denunciare le stazioni illegalmente mantenute in funzione. Il fondatore del club esortava i suoi tremila membri a donare le loro radio alle autorità e ad essere pronti a mettere le loro capacità al servizio dello sforzo bellico[72]. Nel settembre 1917 la rivista chiuse temporaneamente i battenti per l'arruolamento della redazione e di molti lettori.

> La condizione presente non può andare avanti per sempre e lo spirito dell'amatore wireless è vivo in questi giorni morti come è sempre stato. Sia che la legge ci chiuda le stazioni o ci sequestri persino l'equipaggiamento, sia che ci disperda ai quattro venti, sia che siamo nell'esercito in Francia, o in Marina su mari tempestosi, saremo sempre Amateur Wireless Bugs, e niente ci cambierà. [...] Il richiamo della «scintilla» sarà sempre nei nostri cuori[73].

Alla fine del conflitto il ruolo degli amatori nella Grande Guerra sarebbe stato prontamente rivendicato come prova del fatto che ulteriori

limitazioni alla loro capacità di comunicare e sperimentare non erano solo inopportune, ma pericolose per la sicurezza nazionale.

La «cultura ham» esiste ancora oggi e molti phone phreaks e hackers negli anni Ottanta e Novanta si sarebbero considerati ham (uno tra tutti Kevin Mitnick, vedi cap. 4), a testimonianza del fatto che in una «cultura tecnica» ciò che conta non è l'efficienza in senso assoluto (quanto facile, veloce o chiara sia la comunicazione) ma l'efficienza relativa alla tecnologia prescelta (quanto sofisticato, creativo e profondo sia il rapporto tra l'utente e la macchina). Per la ricostruzione della cultura ham negli anni successivi alla sua genesi si rimanda all'ottimo libro di Kristen Haring[74].

Ciò che importa sottolineare qui è che svariate caratteristiche che sono state attribuite alla cultura hacker e che abbiamo menzionato nell'Introduzione (dalla sua composizione sociale alle sue pratiche, dai suoi valori agli stereotipi attorno ad essa creati) erano presenti in maniera del tutto riconoscibile già dai primi anni del Novecento. Questo non deve suggerire necessariamente una filiazione diretta degli hackers dagli amatori. Il caso dei radioamatori prova piuttosto l'esistenza, già all'inizio del secolo scorso, di un particolare discorso sulla tecnologia, che era proprio della cultura statunitense e che si basava su due assunti principali. Da una parte vi era la convinzione, incarnata come si è visto fin dalla letteratura per ragazzi di fine Ottocento, che vi fosse un rapporto privilegiato e quasi naturale tra giovane e tecnologia e che questo rapporto implicasse un approccio creativo e proattivo da parte dell'adolescente. Dall'altra vi era la convinzione che questo rapporto non potesse fiorire se non all'interno di una comunità, capace di coordinare gli sforzi individuali e di darvi valore.

Nel prossimo capitolo osserveremo sia la lunga storia di questo discorso tecno-culturale sia i cambiamenti che gli furono imposti dal suo incontro con l'ideologia della tarda controcultura americana.

30 E.S. Ellis, *The Steam Man of the Prairies*, American Novel Publishing Company, New York 1867.

31 J. Clute, *Edisonade*, in «The Encyclopedia of Science Fiction»,

https://web.archive.org/web/20211004213630/http://www.sf-encyclopedia.com/entry/edisonade.

32 N. Williams, *War Machines and Child Geniuses: American Edisonades*, in *The Cambridge History of Science Fiction*, a cura di G. Canavan e E.C. Link, Cambridge University Press, Cambridge 2019, pp. 86-100.

33 Ivi, p. 94.

34 Noname, *Frank Reade and His Steam Man of the Plains. Or, The Terror of the West*, F. Tousey, New York 1883.

35 V. Appleton, *Tom Swift and His Motor Cycle*, Grosset & Dunlap, New York 1910.

36 *Tom Swift Inventors' Academy*, in «Simon & Schuster», https://web.archive.org/web/20190713050412/https://www.simonandschuster.ca/series/Tom-Swift-Inventors-Academy?intcmp=np_series_link.

37 V. Appleton, G. Kaye, *Tom Swift and His Atomic Earth Blaster*, Grosset & Dunlap, New York 1954.

38 F.J. Molson, *The Boy Inventor in American Series Fiction: 1900-1930*, in «Journal of Popular Culture», XXVIII, 1994, 1, pp. 31-48.

39 A.N. Hall, *Home Handicraft for Boys: Learning Through Doing*, J.B. Lippincott, Philadelphia 1935, citato in K. Haring, *Ham Radio's Technical Culture*, The MIT Press, Cambridge (Mass.) 2007, p. 9.

40 C.B. DeSoto, *200 Meters and Down*, American Radio Relay League, West Hartford (Conn.) 1936, p. 14.

41 Ivi, p. 15.

42 La parola *tinkerer* ha in inglese un significato vicino a quello che avrebbe assunto la parola hacker. Con essa si intende una persona che lavora con la tecnologia, per ripararla o modificarla ai propri fini, spesso attraverso un processo di prova ed errore. Significativamente, non esiste una parola del tutto analoga in italiano. La traduzione forse più fedele è «smanettone», ma nell'accezione inglese manca il tono lievemente negativo che ha la parola italiana.

43 K.H. von Wiegand, *Stop It, Kid! Cries Congress to the American Boy*, in «The San Francisco Call», 29 marzo 1908.

44 Citato in S.J. Douglas, *Inventing American Broadcasting: 1899-1922*, The Johns Hopkins University Press, Baltimore 1989, p. 224.

45 H.G.J. Aitken, *Allocating the Spectrum: The Origins of Radio Regulation*, in «Technology and Culture», XXXV, 1994, 4, pp. 686-716.

46 DeSoto, *200 Meters*, cit., p. 32.

47 W. Silver, *A History of QST. Volume 1: Amateur Radio Technology 1915-2013*, American Radio Relay League Inc., Newington 2013, p. 1.

48 K.B.W., *Transatlantic Amateur Communication Accomplished!*, in «QST», VII, 1924, 6, pp. 9-12.

49 S. Hong, *Wireless: From Marconi's Black-Box to the Audion*, The MIT Press, Cambridge (Mass.) 2001, p. 188.

50 DeSoto, *200 Meters*, cit., p. 37.

51 Department of Commerce - Bureau of Navigation, *Radio Stations of the United States*, Government Printing Office, Washington 1913.

52 DeSoto, *200 Meters*, cit., p. 48; H.R. Slotten, *Radio and Television Regulation: Broadcast Technology in the United States, 1920-1960*, The Johns Hopkins University Press, Baltimore 2000, p. 7.

53 *A Concert by Wireless*, in «QST», II, 1917, 11, p. 26.

54 T.J. Pinch, W.E. Bijker, *The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other*, in *The Social Construction of Technological Systems*, a cura di W.E. Bijker, T.P. Hughes, T.J. Pinch, The MIT Press, Cambridge (Mass.) 2012, pp. 11-44.

55 *QST*, in «ARRL - The National Association for Amateur Radio», https://web.archive.org/web/20220303052146/http://www.arrl.org/qst.

56 Il termine qui utilizzato è «junking», che vuol dire «buttare via», ma nello slang degli amatori significa cercare nella spazzatura per trovare pezzi utili al proprio apparecchio. Questa pratica ha un parallelo nel «dumpster diving» (immersione nella spazzatura) dei futuri hackers, in cerca di pezzi di computer o di informazioni riservate.

57 L. Manuel, *Thoughts of the Good, Old Palmy Days*, in «QST», I, 1916, 4, pp. 47-48.

58 The Old Man, *Rotten QRM*, in «QST», II, 1917, 2, pp. 8-10.

59 M.B. West, *Who Is Who in Amateur Wireless*, in «QST», I, 1916, 10, pp. 262-263.

60 A. Nony Mous, *Wireless Spirit*, in «QST», I, 1916, 12, p. 358.

61 DeSoto, *200 Meters*, cit., p. 8.

62 C.M. Kelty, *Two Bits: The Cultural Significance of Free Software*, Duke University Press, Durham 2008, p. 3.

63 Experience, *Successful Control of QRM*, in «QST», I, 1916, 10, p. 250.

64 H.P. Maxim, *Practical Relaying*, in «QST», I, 1916, 3, pp. 19-22.

65 H.P. Maxim, *Practical Relaying*, in «QST», I, 1916, 4, pp. 45-46.

66 T. Detti, G. Lauricella, *Le origini di Internet*, Mondadori, Milano 2013.

67 9XE, *Washington Birthday Amateur Relay Message*, in «QST», I, 1916, 5, pp. 45-46.

68 R.A. Bartlett, *The World of Ham Radio, 1901-1950: A Social History*, McFarland & Company, Jefferson (N.C.) 2007, p. 6.

69 A. Powell Morgan, *Wireless Telegraph Construction for Amateurs*, Van Nostrand Company, New York 1914, p. 187.

70 Little Willie, *Taking an Examination*, in «QST», I, 1916, 5, pp. 71-73.

71 *National Defense. Our Services Offered to Government*, in «QST», 1915, 1, p. 4.

72 H.P. Maxim, A. Hebert, *War!*, in «QST», II, 1917, 6, pp. 3-4.

73 *Another Season Opens, But*---, in «QST», II, 1917, 10, p. 16.

74 E dal quale è tratta la definizione di «cultura tecnica» («una cultura che si costruisce e crea un'ideologia attorno a una tecnologia»): Haring, *Ham Radio's Technical Culture*, cit., p. XV e cap. 1.

2.
Phone phreak, 1971-1984*

«Youth International Party Line»

Nel maggio 1971 Abbie Hoffman marciava a Washington, insieme agli Yippies di cui era co-fondatore[75] e a 35.000 dimostranti, contro la guerra in Vietnam. La manifestazione fu l'occasione per distribuire 10.000 volantini che pubblicizzavano una nuova newsletter cartacea, la «Youth International Party Line» («YIPL»), che avrebbe visto la luce nel mese successivo sotto la direzione dello stesso Hoffman e di Al Bell (pseudonimo di Alan Fierstein). La pubblicazione si sarebbe occupata di «educare» i propri lettori riguardo all'«illegittimo controllo del sistema di comunicazione di questo paese» esercitato dalla compagnia telefonica Bell[76] (come era ancora familiarmente chiamata l'azienda fondata da Alexander Graham Bell, nonostante avesse cambiato il proprio nome in American Telephone and Telegraph Company, AT&T, già nel 1899). Il primo numero fu inviato ai 50 attivisti che avevano pagato i 4 dollari dell'abbonamento annuale, ma chi avesse dichiarato di non poterselo permettere avrebbe in futuro ricevuto gratuitamente le informazioni. All'editoriale (il cui testo è disposto in modo da formare una campana, il simbolo della Bell) seguono le istruzioni per ricavare i numeri delle carte di credito telefonico (e ottenere così chiamate gratuite), lo schema tecnico per modificare l'apparecchio telefonico domestico e permettere l'installazione (illegale) di ulteriori apparecchi, una sezione dedicata alle lettere dei lettori, notizie sulla legislazione riguardante la telefonia e su iniziative di protesta contro la guerra in Vietnam.

Come ha ben documentato Phil Lapsley[77], le tecniche di modifica degli apparecchi telefonici e di interazione creativa con la rete non sono, nel

1971, una novità. Fin dall'inizio degli anni Sessanta, infatti, la security Bell era a conoscenza dell'esistenza della cosiddetta «blue box», un apparecchio (il cui schema tecnico sarebbe stato pubblicato nel secondo numero di «YIPL») di facile costruzione che riproduceva le frequenze sonore usate dal sistema telefonico a toni per l'indirizzamento delle chiamate e per il calcolo delle bollette. Accostando la blue box alla cornetta del telefono ed emettendo una frequenza di 2.600 hz si poteva «far credere» al sistema che il ricevitore fosse stato riagganciato, rendendo la successiva chiamata di lunga distanza gratuita.

Altre «scatole» di svariati colori erano al centro degli interessi sia della rivista che della comunità dei suoi lettori, che si autodefiniva «phreaker», «phone phreak», o semplicemente «phreak»[78]. La «cheese box», i cui primi usi risalgono probabilmente agli anni Cinquanta[79], reindirizzava le chiamate a un numero diverso da quello inizialmente composto, rendendo la conversazione non tracciabile e gratuita. La «black box» era una modifica che, manipolando il flusso di energia elettrica nell'apparecchio telefonico casalingo, faceva «credere» al sistema telefonico che la cornetta fosse stata riagganciata, mentre la conversazione era ancora in corso, rendendo gratuite le chiamate in entrata; la «red box» simulava i toni che segnalavano il pagamento nei telefoni pubblici, rendendo le chiamate gratuite; la «beige box» era un apparecchio telefonico dotato di connettori, del tutto simile a quello in dotazione ai tecnici Bell, che permetteva di collegarsi direttamente alle linee telefoniche, effettuando chiamate o ascoltando quelle altrui. Tutte queste «scatole» erano autoprodotte dagli appassionati, che dovevano perciò avere conoscenze estremamente dettagliate e specifiche sul funzionamento degli apparecchi e del sistema telefonico nel suo complesso, così come sulla legislazione che li riguardava e sulle politiche di Bell e del suo servizio di sicurezza[80]. La costruzione di circuiti e dispositivi era, come nel caso dei radioamatori, almeno tanto importante quanto la comunicazione che essi permettevano. «YIPL» si occupava di diffondere queste informazioni, tratte dai manuali tecnici della Bell, da riviste di settore e soprattutto dall'esperienza dei lettori.

La possibilità di effettuare chiamate a costo ridotto o nullo, garantita dalle scatole e da altri espedienti, permetteva la composizione di numeri

in sequenza nel tentativo di mappare il sistema telefonico della Bell. Si trattava di un'esplorazione che molto aveva in comune con l'esperienza dell'etere avuta dai radioamatori fin da inizio Novecento: condotta con l'udito, piuttosto che con la vista, essa traeva parte del proprio fascino dall'inaspettato, dalla ricerca di suoni insoliti e di voci senza volto e dal tentativo di connettere quanto si sentiva con le conoscenze collettive della comunità. Lo *scanning* richiedeva costanza, conoscenze approfondite dei suoni del sistema telefonico e, ovviamente, creatività: «Se trovi qualcosa di strano, giocaci! [...] Prendi ogni piccolo pezzo e scombinalo! Dopo che lo hai fatto a pezzi cercane degli altri. Usa la tua immaginazione, intuizione e buon senso» («YIPL», marzo 1978).

La gratuità permetteva d'altra parte la creazione di piccole comunità «virtuali», composte da appassionati sparsi su tutto il territorio statunitense. Strumento importante nella creazione di queste comunità furono le cosiddette «party lines» (dalle quali «YIPL» prendeva il proprio nome)[81]: chiamando allo stesso tempo numeri di servizio non più in uso, svariati utenti potevano parlare in contemporanea, scambiandosi informazioni tecniche, notizie sulle imprese di phreaks particolarmente talentuosi o su nuovi numeri telefonici di interesse, e semplici chiacchiere[82]. Nel corso degli anni «YIPL/TAP»[83] si occuperà di discutere, perfezionare e diffondere questi e altri hacks del sistema telefonico e di tenere al passo i propri lettori con l'innovazione tecnologica. Ben presto gli interessi della rivista si amplieranno fino a coprire campi diversi, come la manifattura di fuochi d'artificio o di droghe, la modifica di contatori domestici (cosiddetto «gas raiding», gennaio-febbraio 1974), parchimetri o decoders televisivi, la scassinatura dei lucchetti e, dalla fine degli anni Settanta, l'accesso illecito ai sistemi informatici. Lo stesso Abbie Hoffman aveva dato alle stampe un manuale di «sopravvivenza nella giungla elettronica», scritto come una parodia dei libri di auto-aiuto e ironicamente intitolato *Ruba questo libro*, nel quale si trovavano consigli su come procurarsi servizi e beni gratuiti, costruire armi e bombe e falsificare documenti[84].

La composizione sociale, generazionale e di genere dei lettori di «YIPL/TAP» non è di difficile identificazione: gli appelli della redazione a diffondere la pubblicazione nelle scuole superiori e nelle università

(gennaio 1972), i riferimenti alla vita quotidiana che si trovano nelle lettere, il costante richiamarsi, nei soprannomi e nei commenti, a personaggi dei fumetti, della televisione e della letteratura di fantascienza, indicano un pubblico di lettori perlopiù bianco, maschile, di classe media e di un'età compresa fra i 13 e i 25 anni. Se all'inizio gli studenti medi sembrano essere preponderanti, con il passare del tempo i lettori e gli articolisti arriveranno a comprendere laureati e tecnici (in alcuni casi anche della Bell). La sottocultura che si raccoglieva intorno a «YIPL/TAP» era, al pari di gran parte della controcultura statunitense di quegli anni e della cultura hacker studiata da Douglas Thomas negli anni Novanta, una cultura giovanile, caratterizzata da «dominio sulla tecnologia, indipendenza e scontro con l'autorità adulta»[85].

Sebbene non vi siano dati precisi, la circolazione della newsletter fu indubbiamente ampia all'interno della comunità dei phone phreaks, ma limitata in termini assoluti. La redazione incoraggiava attivamente i propri lettori a fotocopiare la rivista e diffonderla nelle scuole e nei luoghi pubblici. Le conventions organizzate da «YIPL/TAP» videro la partecipazione di diverse centinaia di persone; la natura tecnica delle informazioni fornite, presentate in molti casi in ordine di complessità, favoriva la vendita di arretrati ai novizi che, venuti tardivamente a conoscenza della pubblicazione, dovevano mettersi al passo. Ciò nonostante è lecito inferire che il numero di copie direttamente spedite fu, per tutto l'arco di vita della pubblicazione, ridotto: quando, nel gennaio 1977, Tom Edison, l'allora caporedattore, segnalava la perdita di 238 abbonati, il colpo era definito «fatale». Eppure la rivista e la pratica acquisirono, tanto nella percezione della security Bell e delle autorità di polizia, quanto all'interno delle successive culture hacker, una centralità sproporzionata rispetto alla loro effettiva diffusione. AT&T fece più volte uso della frode telefonica operata dai phone phreaks per giustificare l'aumento delle proprie tariffe. Già nell'ottobre 1972 un documento interno della Bell, ottenuto da «YIPL» e pubblicato il mese successivo sotto l'ironico titolo *AT&T Papers*[86], indicava la newsletter come la principale fonte di informazioni per la frode telefonica e sollecitava la raccolta di testimonianze che potessero incriminare la redazione. Dal 1974 l'FBI aprì un file dedicato alla newsletter e cominciò a far uso di

informatori per conoscere la composizione della redazione e i suoi obiettivi[87].

Cultura phreak

Prima ancora che un mezzo di educazione tecnica o politica, «YIPL/TAP» era uno strumento di smistamento di informazioni segrete o difficilmente reperibili. A volte queste erano trovate in cataloghi, libretti di istruzioni o pubblicazioni ufficiali di scarsa circolazione, come il «Bell System Technical Journal» del novembre 1960, che incautamente forniva informazioni dettagliate sui *Sistemi segnaletici per il controllo degli scambi telefonici*[88], necessari alla costruzione delle blue box[89], e che sarebbe diventato oggetto di culto tra i phreaks. Nella maggior parte dei casi le informazioni erano raccolte tramite l'esperienza diretta dei sistemi tecnologici, in uno sforzo collettivo che «YIPL/TAP» rendeva possibile e celebrava.

Come nel caso di altre pubblicazioni controculturali, quali «People's Yellow Pages»[90] (fondata nel 1971 e immediatamente pubblicizzata da «YIPL») e «Whole Earth Catalogue», lo scambio di informazioni tecniche e servizi altrimenti irreperibili serviva a fare di un gruppo di interesse geograficamente disperso una comunità che si definiva alternativa al mercato e alla cultura dominante. E come nel caso di queste pubblicazioni, gli articoli pubblicati nei tredici anni di vita della rivista provenivano per la maggior parte dai lettori stessi ed erano scelti per la loro originalità, sia rispetto a tecniche già conosciute sia rispetto a quella che era percepita come la morale dominante. La richiesta di contributi si trovava in quasi ogni numero:

> Tutti hanno qualcosa da offrire a una newsletter scritta dai lettori. Imbrogli, ricette, codici di carta di credito telefonica, numeri per chiamate gratuite, numeri di test, notizie oltraggiose, passwords di computer, prefissi internazionali, inchieste giudiziarie in corso, e qualsiasi cosa vogliate condividere (gennaio 1973).

La redazione manteneva un servizio di scambio di schemi tecnici via posta (chiamato ironicamente «Destructory Assistance», assistenza distruttiva) e cercava di favorire l'incontro faccia a faccia dei lettori e la loro organizzazione in piccoli gruppi locali. Dalla metà degli anni

Settanta «TAP» compilava una lista di contributori affidabili e delle loro competenze per metterli in contatto con chi avesse specifiche esigenze tecniche e per diffondere informazioni ritenute troppo pericolose per la pubblicazione. Quanto effettivamente pubblicato non è che uno squarcio sulla creazione di un sapere collettivo ben più ampio: buona parte di quest'ultimo si affidava senza dubbio alle conversazioni via telefono ed è ovviamente di difficile ricostruzione.

I lettori erano invitati a fornire le proprie risposte a specifici problemi tecnici non ancora di pubblica conoscenza o a testare collettivamente ipotesi sul funzionamento del sistema telefonico e, negli anni Ottanta, dei networks digitali. Come nel caso delle future comunità hacker, il compenso per questo sforzo individuale (e per i rischi legali che in alcuni casi esso comportava) spesso non andava al di là della pubblicazione del pezzo sotto pseudonimo e della consapevolezza di aver contribuito, con il proprio ingegno, alla conoscenza del gruppo di appassionati a spese di un'autorità centrale. Come nel caso dei radioamatori, il culto della capacità tecnica e l'accento posto sulla formazione attraverso l'esperienza pratica non si traducevano in elitismo. Grande attenzione era riservata alla formazione dei neofiti e all'allargamento della comunità, in particolare attraverso ripetute spiegazioni di nozioni che dovevano essere ben conosciute dai phreaks più esperti, il richiamo a numeri arretrati (sempre ristampati e disponibili per l'acquisto) per spiegare gli articoli più complessi, workshops pubblici tenuti nel corso delle conventions e persino la pubblicazione di un corso di elettronica per principianti. Non vi è traccia del disprezzo che molte comunità hacker successive avrebbero nutrito per gli «script kiddies», ovvero chi usa, come si è detto, hacks inventati da altri senza aggiungervi nulla di originale. Al contrario, i neofiti erano invitati ad emulare gli esperti anche in mancanza di capacità tecniche: nel corso delle conventions erano addirittura distribuite audiocassette con la registrazione dei toni della blue box per chi non era in grado di costruirne una in proprio.

Oltre alla formazione propriamente tecnica, «YIPL/TAP» impartiva regolarmente lezioni di quello che sarà chiamato dalle comunità hacker «social engineering»: la capacità di sfruttare le convenzioni sociali e i rapporti di potere per ottenere accesso a informazioni riservate o altri vantaggi tecnici, nella convinzione che l'elemento umano sia sempre il

punto più debole di ogni sistema tecnologico (vedi cap. 4). Il buon phreak doveva essere capace di inserirsi in ogni falla lasciata dalla burocrazia e dal grande volume di informazioni che il sistema Bell doveva gestire, impersonando di volta in volta un dipendente della compagnia telefonica, un cliente sprovveduto o insoddisfatto, uno studente che stava facendo una ricerca sul sistema telefonico: «Ricorda. Devi sempre apparire, agire e parlare con sicurezza» (dicembre 1971). Lo sfruttamento dei rapporti di genere è parte integrante delle capacità di ogni «ingegnere sociale»[91]. Nel rivolgersi alle operatrici telefoniche della Bell, sempre donne – consigliava «YIPL/TAP» –, «Cercate di suonare di mezza età, di fretta e arrabbiati con le operatrici, ma disponibili a dar loro un'ultima possibilità» (novembre 1972). I dieci comandamenti del phreaker, pubblicati nel 1983, raccomandavano, oltre alla cautela in ogni conversazione telefonica e alla discrezione nel parlare delle proprie attività, la diligenza a scuola e nel lavoro, poiché «le autorità ben sanno che gli studiosi non infrangono mai la legge» (luglio-agosto 1983).

Parte fondamentale del processo di *community building* era la creazione di un avversario. L'ostilità verso AT&T, il monopolio sanzionato dallo Stato che controllava il principale terreno di esplorazione e di incontro tra i phreaks, teneva insieme e definiva la comunità dei lettori di «YIPL/TAP». Bell acquisiva, sulle pagine della newsletter, i caratteri di un vero e proprio antagonista fumettistico: a essa si attribuiva, direttamente o indirettamente, ogni possibile nefandezza, ivi compresa, in un caso particolarmente paradossale, la responsabilità della stagflazione[92] agli inizi degli anni Settanta (maggio 1973). Le pratiche monopolistiche di AT&T – criticate da più parti, non solo dalla controcultura – e la (percepita) scarsa qualità del servizio autorizzavano le azioni illegali dei phreaks e permettevano di caratterizzare l'hobby come una scelta etica e le chiamate gratuite come una difesa della libertà di parola. «Ma Bell» (Mamma Bell, come era familiarmente chiamata AT&T) era di volta in volta definita come un onnisciente Grande Fratello che si approfittava dell'ignoranza della popolazione non tecnicamente informata[93] o come un ottuso gigante ridicolizzato dall'ingegnosità della piccola comunità phreak. Il volto visibile di questo colosso erano gli impiegati, i tecnici (generalmente visti come ignoranti vittime essi stessi) e soprattutto la

security Bell, il corpo incaricato di indagare sulle frodi telefoniche: tutte queste categorie erano oggetto di costanti analisi e scambio di informazioni, che miravano a registrarne il comportamento per permettere, insieme alla minuziosa conoscenza delle leggi e delle politiche Bell, il social engineering. Per evitare una perquisizione, ad esempio, Tom Edison consigliava di far aprire la porta a un minorenne: «La politica Bell non permette ai loro agenti di sicurezza di entrare in una casa occupata soltanto da un bambino. Questo è dovuto alla diffusa voce che tutti gli agenti di sicurezza Bell siano pervertiti molestatori di bambini» (settembre 1979). L'ostilità continuamente ribadita si accompagnava tuttavia a un ambiguo fascino per l'avversario: l'innovazione tecnica messa in campo da Bell era un ostacolo alle tecniche dei phreakers, ma anche occasione di nuove sfide che mantenevano in vita la comunità. Al pari dei molti hackers che hanno legittimato la propria passione diventando esperti di cybersicurezza, molti phreaks aspiravano (e in alcuni casi riuscivano) a lavorare per la Bell. Gli strumenti e i gadgets della compagnia telefonica (dagli attrezzi in dotazione ai tecnici autorizzati a indumenti con il logo della campana) erano oggetti di culto tra gli appassionati, al pari del famoso «Bell System Technical Journal» del novembre 1960.

Se il costante rincorrersi con la security Bell era un indubbio oggetto di fascino, nulla aiutava a serrare i ranghi come una sfida tecnica comunemente intrapresa. Lo sforzo collettivo poteva essere applicato a obiettivi banali, come lo studio comparato dei distributori automatici per capire quali accettassero gettoni contraffatti (febbraio 1973), o a vere e proprie imprese tecnologiche, come la penetrazione nel sistema telefonico dell'esercito statunitense, AUTOVON (settembre-ottobre 1977). La costante innovazione tecnica di AT&T assicurava che la ricerca collettiva del sapere fosse un'impresa senza fine. L'introduzione del «fortress phone», un telefono pubblico «blindato», scatenò la discussione su come scassinarne i lucchetti. L'invenzione di un apparecchio per individuare le blue boxes portò al raffinamento della loro costruzione e a nuove regole di cautela nel loro utilizzo, così come al tentativo, sempre collettivo, di verificare quali linee fossero controllate (giugno 1979). «Qualsiasi sofisticata tecnologia Ma Bell inventi per scovarci – affermava Tom Edison in un'intervista rilasciata a 'The Village Voice' del 1975 –

uno di noi inventa sempre un modo per aggirarla, lo condivide attraverso la rivista e presto i phreaks sono di nuovo in pista». Quando infine il superamento del sistema a toni per l'indirizzamento delle chiamate rese le blue boxes obsolete, la reazione della newsletter dimostrava l'entusiasmo con cui la nuova sfida era accolta: «Come siamo soliti dire, i vecchi phreaks non muoiono mai, ma costruiscono una scatola di colore diverso»; dopotutto, «il telefono è solo un apparecchio elettronico e come ogni apparecchio elettronico PUÒ ESSERE SCONFITTO!!!» (marzo 1976).

Un terzo strumento della costruzione identitaria del gruppo è la creazione di celebrità. Chi si è occupato di phreaking, sia allora sia in seguito[94], è stato colpito dalla preponderanza di ragazzini non vedenti tra le fila dei phreaks, e in particolare dalla figura di Joybubbles (Josef Engressia), cieco dalla nascita e capace di zufolare all'esatta frequenza necessaria a effettuare chiamate gratuite sul sistema telefonico pubblico. I riferimenti a phreaks non vedenti sono tuttavia rari in «YIPL/TAP» ed è probabile che la loro centralità nelle ricostruzioni successive sia dovuta più alla loro atipicità che non al loro numero. Ben più centrale è la figura di Captain Crunch (John Draper), «il leggendario phone phreak che Ma Bell ha inseguito per tutto il continente»[95]. Ciò che rese celebre Draper fu la sua estrema attenzione nella costruzione della propria figura attraverso interviste e lettere a «TAP» e altre pubblicazioni, secondo un modello di autopresentazione del sé che sarebbe diventato familiare sui social networks nel nuovo millennio[96]. Elementi ugualmente importanti furono senza dubbio la sua capacità di operare un «tandem attorno al mondo» (vale a dire chiamare un telefono che gli era a fianco facendo sì che la chiamata attraversasse il globo prima di far squillare il telefono in questione), la sua estesa conoscenza del sistema telefonico (nel 1975 Crunch offriva un corso residenziale di phone phreaking di una settimana ai lettori di «TAP») e l'attenzione che FBI e Bell gli riservavano. Dal 1972 la newsletter seguì costantemente le disavventure legali di Draper – perseguitato, secondo «YIPL/TAP», per intimidire ogni phreak e perché «sa abbastanza da ridurre Ma Bell in macerie» – e più volte aprì raccolte di fondi a suo sostegno. L'annuncio della sua volontà di cessare ogni rapporto con i phreaks per dedicarsi alla

programmazione, comunicato attraverso una lettera pubblicata da «TAP» nel 1979 e dopo tre condanne per frode telefonica, non fu sufficiente a rovinare il suo status di celebrità. Nel 1984 Steven Levy lo includerà tra gli «ultimi veri hackers»[97] e Steve Wozniak, fondatore di Apple ed egli stesso una delle massime celebrità hacker, lo citerà tra le proprie fonti di ispirazione.

Un ultimo, fondamentale, strumento per la costruzione identitaria del gruppo è la designazione di un obiettivo comune. Che si trattasse di ingannare un operatore telefonico per avere accesso a informazioni riservate, apporre un francobollo su una busta in modo che non fosse vidimato dal timbro dell'ufficio postale, usare il sistema di comunicazione a toni per ottenere chiamate gratuite, l'obiettivo pratico era sempre quello di usare informazioni specifiche, dettagliate, segrete e illecitamente ottenute su un sistema tecnologico o sociale per far sì che questo funzionasse a vantaggio dell'individuo che vi interagiva creativamente e contro la volontà di chi gestiva il sistema o lo aveva creato. In molti casi i rischi corsi, le competenze che era necessario acquisire o le tribolazioni cui bisognava sottoporsi appaiono del tutto spropositate rispetto al risultato ottenuto. A conclusione di un articolo su come derubare un «fortress phone» (l'operazione richiedeva una complessa e dispendiosa procedura, con il solo guadagno della manciata di monete contenute in un telefono pubblico), «Mr. Phelps» ammetteva: «Solo l'aspirante perpetratore può decidere se ne vale la pena, dato il carico di lavoro e il rischio in cui si incorre» (novembre 1975). Anche l'ottenimento di chiamate gratuite di lunga distanza è difficilmente giustificabile da un punto di vista utilitaristico: in molti casi si ammetteva che, nonostante tutte le nozioni raccolte e il tempo speso, semplicemente non si avevano conoscenti da chiamare in altre città. Lungi dallo scoraggiare l'hobby, la mancanza di interesse pratico era usata come prova della sua innocenza e purezza intellettuale: «Per quanto riguarda [l'argomento che] i phreaks starebbero truffando il pubblico, non è evidente per noi di 'TAP', poiché sappiamo che la maggior parte dei phreaks trae piacere dall'esplorazione elettronica del sistema, senza far male a nessuno e facendo chiamate che altrimenti non avrebbero fatto» (marzo 1975). Quando, negli anni Ottanta, il sistema da esplorare

diventerà quello informatico, questo proclamato disinteresse per ogni fine che non sia esclusivamente intellettuale e di intrattenimento si riverserà nella «cultura hacker». Come spiega «Ben Dump» in uno dei primi articoli dedicati all'esplorazione illegale dei computer: «Entrare in un computer di una corporation può essere pericoloso, perché pensano tu stia cercando dei segreti industriali (chi se ne frega?)» (gennaio 1980). Gli fa eco «The Magician», anticipando la distinzione tra «veri hackers» e «crackers» più volte ribadita nelle culture hacker:

> Certo, c'è chi trae il proprio piacere solo dalle chiamate gratuite, ma quelli non sono veri phone phreaks. I veri phone phreaks sono «appassionati di telecomunicazioni» che sperimentano, giocano e imparano dal Sistema telefonico. A volte questo [...] implica chiamate gratuite. Ma le chiamate gratuite non sono che una piccola parte delle attività dei VERI phone phreaks (maggio 1982).

Monkey theatre

La principale e più duratura novità introdotta da «YIPL/TAP» non è tanto la politicizzazione di un inusuale hobby e il suo inserimento all'interno della tradizione controculturale della tecnologia antisistema, quanto il suo accostamento con le specifiche modalità di comunicazione politica adottate dagli Yippies. La strategia comunicativa teorizzata da Hoffman e da lui chiamata «monkey theatre» (una variazione ironica sul «guerrilla theatre»)[98] nasceva dalla sua insoddisfazione per il movimento pacifista, ritenuto troppo noioso e perciò incapace di parlare ai giovani, e per la sinistra controculturale, troppo intellettuale e preoccupata più dell'esattezza del messaggio che non della sua efficacia. Il segreto della comunicazione moderna risiedeva, secondo Hoffman, nello stimolare la fantasia e la voglia di divertimento del pubblico[99]. Come un trailer cinematografico o una pubblicità televisiva, una dichiarazione mediatica doveva essere breve nella formulazione, dal forte impatto emotivo ed esagerata nei contenuti, in modo da creare aspettative nel pubblico, uno «spazio vuoto» che esso potesse riempire con le sue fantasie. I media televisivi e giornalistici avrebbero inseguito questo spazio vuoto, formulando congetture e dando visibilità al messaggio politico di chi lo aveva creato: «I media non mentono mai se ti rivolgi a loro in una maniera mitica e non lineare». La scelta stessa di un nome senza senso,

Yippies, era un espediente per suscitare la curiosità del pubblico e dei media: «La precisione era sacrificata per ottenere un maggior grado di suggestione [...] I reporters avrebbero giocato i loro ruoli prestabiliti: 'Qual è la differenza tra un hippie e un Yippie?'. Sarebbero state date cento risposte diverse, costringendo il reporter a creare la propria risposta; a distorcere. E la distorsione era diventata la linfa vitale degli Yippies»[100].

Dal punto di vista pratico il monkey theatre consisteva nella messa in scena di spettacoli o proclami volutamente provocatori, per dimostrare l'assurdità dell'indignazione dell'opinione pubblica e della reazione delle forze dell'ordine, ma anche per serrare i ranghi tra chi ne capiva l'ironia. Si trattava di «sbarazzarsi [...] delle analisi prolisse, degli slogan a pugno chiuso, delle proteste ordinate – che erano state una costante della Sinistra dal XIX secolo. Invece, [gli Yippies] organizzavano eventi umoristici fatti per la televisione e guardati da milioni di giovani, ribelli in potenza che avevano ben poco interesse per una politica che non fosse intrattenimento»[101]. La tecnica richiedeva, come un hack, un'istintiva comprensione del sistema mediatico (delle sue paure, delle sue prerogative, dei suoi mezzi) per piegarlo a usi non previsti o desiderati dal sistema stesso: in particolare dare visibilità al movimento e ai suoi leaders.

La più compiuta dimostrazione del potere del monkey theatre ebbe luogo durante la manifestazione contro la convention del Partito democratico nel 1968 a Chicago, dove i delegati del partito avrebbero dovuto scegliere il candidato presidenziale per le imminenti elezioni. L'evento di protesta, battezzato «Festival of Life», fu accuratamente preparato da Hoffman e Jerry Rubin, con roboanti comunicati stampa e apparizioni televisive. Un maiale (chiamato «Pigasus») fu nominato candidato Yippie alle presidenziali e portato alla manifestazione. Gli Yippies minacciarono di travestirsi da tassisti e di rapire i delegati, di fare sesso per le strade, di tuffarsi nudi nel lago Michigan, di marciare vestiti da Vietcong. Come dei «super villains» avrebbero versato LSD nell'acquedotto di Chicago, intossicando l'intera cittadinanza. L'assurdità delle minacce, evidente per i simpatizzanti Yippie e per chiunque avesse mai letto un fumetto, non impedì che i media vi dessero ampia visibilità,

presentandole come possibili o perlomeno come prova della perversione di questa particolare branca della nuova controcultura americana[102]. Appena prima dell'inizio della convention Hoffman promise provocatoriamente di lasciare Chicago se gli avessero dato 100.000 dollari[103]. Il «Chicago Tribune», immune da ogni ironia, titolò indignato: *Gli Yippies pretendono soldi dalla città*. Ben consapevole di questa intensa attenzione, all'inizio della convention, il 25 agosto 1968, Hoffman distribuì volantini, prontamente riprodotti dai giornali, con un «Piano Yippie Top Secret» che prevedeva, all'interno del parco dove erano ospitati i manifestanti, corsi di karate, «snake dancing», «comunicazione underground» (quasi certamente phone phreaking), Olimpiadi Yippie, un concorso di bellezza Miss Yippie e un corso «in stupidità della polizia». In maniera più preoccupante per le forze dell'ordine, i volantini contenevano informazioni sulle stanze di hotel dove erano alloggiati alcuni delegati, con tanto di mappe dei diversi piani e l'esplicito invito, ripetuto ossessivamente (BREAK-IN BREAK-IN BREAK-IN), a entrarvi[104]. Nessuna invasione degli hotel o interazione con i delegati fu tentata nel corso della manifestazione.

Ciò nonostante la reazione delle forze dell'ordine fu brutale. Il sindaco di Chicago dimostrò di aver preso sul serio le minacce, non solo presidiando l'acquedotto della città, ma mobilitando 12.000 poliziotti, 6.000 soldati della guardia nazionale e 7.500 dell'esercito regolare – a fronte di 10.000 manifestanti stimati[105]. In quella che le stesse fonti governative hanno in seguito definito una «rivolta della polizia»[106] e che gli storici hanno visto come uno dei momenti topici della storia della controcultura statunitense, le forze dell'ordine andarono ben oltre gli ordini ricevuti, attaccando manifestanti pacifici, giornalisti e semplici passanti, sotto gli occhi delle telecamere attirate da Hoffman e dal suo monkey theatre.

Chicago fu un successo mediatico, perlomeno nel breve termine. La protesta fu raccontata come un'iniziativa Yippie, nonostante la partecipazione di gruppi controculturali ben più numerosi, affermati e moderati. Hoffman, anche grazie al seguitissimo processo che lo avrebbe visto protagonista nei mesi successivi (e che lo Yippie avrebbe reso un nuovo evento surrealista)[107], sarebbe diventato una figura pubblica

nazionale. Ben meno positivo il risultato di lungo periodo: se Chicago aveva portato per la prima volta in televisione la violenza della polizia – creando inevitabili paralleli con le immagini che arrivavano dal Vietnam –, le elezioni presidenziali del 1968 furono vinte di misura da Nixon con la promessa di «ristabilire l'ordine» dopo le rivolte che avevano avuto luogo in quell'anno.

Il tentativo di politicizzare il phreaking ebbe un successo ugualmente limitato. Nonostante sporadici tentativi dei redattori di «YIPL» di ribadire il valore politico della pratica, su insistenza dei lettori il contenuto esplicitamente attivista fu presto limitato in favore della comunicazione tecnica, tanto che nell'agosto 1973 il titolo della rivista abbandonò il riferimento agli Yippies per diventare «Technological American Party» («TAP») e, nel 1979, semplicemente «Technological Assistance Program». A solo un anno di distanza dal primo numero Hoffman lasciò la direzione della rivista, pur continuando a contribuirvi in maniera anonima. La posizione politica della newsletter oscillò, per tutti gli anni Settanta e a seconda della mutevole composizione della redazione, tra un libertarianesimo individualista e un generico anarchismo avverso a ogni tipo di restrizione della libertà di parola e a ogni tipo di regola, dalle tasse (febbraio-marzo e settembre-ottobre 1976) all'imposizione di un limite di velocità per gli autoveicoli (novembre-dicembre 1978). Come è reso esplicito in un editoriale del febbraio 1974, la creazione di una linea politica coerente non era tra le priorità della pubblicazione e ogni posizione politica esplicita doveva essere presa come espressione del singolo articolista: l'obiettivo di «TAP» dalla metà degli anni Settanta si era ormai spostato sulla libertà di informazione, lasciando ai lettori la responsabilità di come questa sarebbe stata utilizzata. La natura del coinvolgimento politico dei phreaks è forse meglio compresa attraverso la categoria di «pubblico ricorsivo»: «un pubblico che è vitalmente interessato al mantenimento pratico e materiale e alla evoluzione dei mezzi legali, pratici e concettuali della sua esistenza come pubblico»[108]. Come le comunità Free Software di cui parla Kelty, i phreaks si accostavano alla politica non con un piano ideologico coerente, ma attraverso il coinvolgimento pratico nel sistema che permetteva la loro esistenza e la discussione sulle forme (aperte, non

autoritarie, tecnologicamente efficienti) che questo avrebbe dovuto avere. L'avversione per le restrizioni alla libertà di informazione e per le pratiche monopolistiche di AT&T, del governo e delle corporations erano denunciate non con un'analisi organica o una linea ideologica univoca o rivoluzionaria, ma con interventi tecnici che permettevano un uso alternativo del sistema.

Ciò che rimane dell'accostamento tra phreaking e Yippies sono in primo luogo le forme della comunicazione politica. Scrive Al Bell nel gennaio 1973: «Il nostro obiettivo è che la gente si chieda: 'Perché [i phreaks] stanno truffando la compagnia telefonica?' [...] i membri di 'YIPL' sono attori e il mondo sta guardando». Lo scherzo e le azioni di piccolo sabotaggio («monkey warfare»: settembre 1971) nei confronti delle figure di autorità, dall'ufficio postale alla polizia, dall'Internal Revenue Service (l'Agenzia delle entrate) alla Bell, costituiscono una parte importante del contenuto tecnico di «YIPL/TAP»: ridicolo e irriverenza sono usati per dimostrare l'ottusità dell'avversario e la rigidità dei sistemi tecnologici e sociali che si intendono criticare. Ben presto il sabotaggio indiscriminato proposto da Hoffman sarà moderato da sollecitazioni a non distruggere telefoni che possono essere usati da altri phreaks, a non mettere in eccessiva difficoltà gli innocenti operatori telefonici e a non impedire chiamate di emergenza. Come nel monkey theatre, le capacità tecniche dei phone phreaks e la loro minaccia alla società o al sistema telefonico sono sistematicamente esagerate, con l'obiettivo di celebrare la comunità dei phreaks e il loro dominio sul «sistema», ma anche di attirare l'attenzione dei media. Il tentativo ebbe successo, con effetti a volte indesiderati. Un articolo su «Ramparts», una delle principali riviste della New Left statunitense, dichiarava senza mezzi termini: «Con il giusto equipaggiamento, sembra, un manipolo di persone può mettere fuori combattimento i circuiti di comunicazione a lunga distanza in tutto il mondo»[109]. Il ricordato file dell'FBI fu riaperto nel 1979, quando un informatore comunicò che durante una riunione di redazione erano state distribuite le istruzioni (mai pubblicate sulla newsletter) per costruire una bomba atomica. Agli schemi tecnici (che il Department of Energy giudicherà informazioni riservate ma non segrete) si accompagnava un commento di questo tenore: «Sii l'invidia dei tuoi

vicini e rispettato dai tuoi nemici [...] Portala ovunque tu vada. Al primo segno di problemi fai partire il timer e scappa come se ne andasse della tua vita», e una garanzia che prometteva un rimborso entro trenta giorni dalla detonazione nel caso questa non fosse stata di almeno cinque chilotoni[110]. La pubblicazione di informazioni potenzialmente pericolose (la newsletter offriva a più riprese istruzioni su come procurarsi o costruirsi armi ed esplosivi, su come svaligiare una casa, su come produrre e vendere droghe pesanti) era giustificata dalla convinzione che «l'informazione vuole essere libera»[111] e promossa dall'orgoglio di essere riusciti a scovare e a mettere in comune informazioni segrete, nascoste e invise alle autorità. In nessun caso la presentazione di tali informazioni equivaleva a un invito alla violenza organizzata o interpersonale. Una nota editoriale del settembre 1978 metteva in chiaro che la rivoluzione anti-sistema di «TAP» si raggiungeva attraverso il «sabotaggio di migliaia di parchimetri e le torte in faccia» più che attraverso una violenza vista come propria di «elementi più barbarici della nostra società (come poliziotti, politici...)». Lo strumento di offesa più utilizzato era limitato ai confini «virtuali» della rete telefonica e consisteva nel diffondere il numero di telefono o di carta di credito telefonica di figure pubbliche per esporle agli scherzi della comunità phreak – una pratica che prefigura il sarcasmo del charivari delle prime comunità virtuali informatiche[112] e il doxing praticato dai trolls contemporanei (vedi cap. 7).

Il monkey theatre sarebbe passato dalla cultura phreak a quella hacker e da questa si sarebbe riversato nella più ampia «cultura digitale». Lo scherzo come strumento politico, l'esagerazione strumentale della minaccia rappresentata dal gruppo, l'uso sovversivo ed esperto delle regole di sistemi tecnologici, mediatici e sociali, sono tutte caratteristiche che saranno tramandate, attraverso pubblicazioni direttamente ispirate da «YIPL/TAP» quali «Phrack Magazine» e «2600. The Hacker Quarterly»[113], alle culture hacker dei nostri giorni. Le pagine che seguono proveranno che l'eredità di Hoffman è stata raccolta, in maniera inconsapevole, da gruppi tanto diversi quanto il movimento Open Source, gli hacktivisti del Cult of the Dead Cow e di Anonymous e i trolls di LulzSec.

⋆ Una versione più breve di questo capitolo è apparsa in F. Mazzini, *Linee condivise. Il 'phone phreaking' e la storia culturale dell'hacking (1971-1984)*, in «Passato e Presente», XXXVI, 2018, 103, pp. 47-69.

75 Lo Youth International Party fu fondato da Hoffman e altri nel 1967. Il termine Yippie è una deformazione ironica di hippie ed ha un significato più onomatopeico (YIP! come urlo di liberazione) che letterale. «Cosa significa Yippie? Energia – eccitazione – divertimento – fierezza – punto esclamativo!». A. Hoffman, *Revolution for the Hell of It* (1968), Thunder's Mouth Press, New York 2005.

76 «YIPL», giugno 1971. Data la sua pubblicazione e numerazione a volte incostante, la newsletter sarà citata con mese e anno di edizione e non con il numero. Ogni numero consiste di quattro facciate fittamente stampate e in rari casi manoscritte. Tutti i numeri sono consultabili online: «Index of /tap», https://web.archive.org/web/20220411124953/http://www.textfiles.com/tap/.

77 P. Lapsley, *Exploding the Phone. The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell*, Groove Press, New York 2013, p. 113.

78 «Freak» in inglese significa «mostro», ma anche «ossessionato». I phreaks sostituiscono ph alla f per fare riferimento al telefono (*phone*) e perché ph e f si leggono in inglese entrambe come *f*.

79 Lapsley, *Exploding the Phone*, cit., p. 101.

80 Per avere un'idea del livello di dettaglio tecnico si veda l'antologia di scritti sul phone phreaking presentata da E. Goldstein, *The Best of 2600: A Hacker Odyssey*, Wiley Pub, Indianapolis 2008, cap. 2.

81 Youth International Party Line è un gioco di parole che allude ironicamente agli interessi tecnici della newsletter (party line in quanto chiamata condivisa), ai suoi scopi politici (party line in quanto «linea di partito») e al suo tono ironico (party line in quanto «linea della festa»).

82 Una rarissima registrazione di una party line del 1971 è ascoltabile in rete, con i commenti del phreak che l'ha messa a disposizione: E. Doorbell, *Phreaks & Folks on the Hempstead NY '5166' Vacant Code Conference, pgm. 1, June 1971*, https://www.youtube.com/watch?v=XZa8TRD3f4s.

83 Nel 1973 la newsletter cambierà il proprio nome in «TAP» (vedi *infra*). Per questo, quando si parlerà della pubblicazione nel suo complesso si userà l'espressione «YIPL/TAP».

84 A. Hoffman, *Steal This Book*, Grove Press, New York 1971.

85 Thomas, *Hacker Culture*, cit., pp. IX-X.

86 Il riferimento era ai *Pentagon Papers*, i documenti riservati pubblicati dal «New York Times» l'anno precedente, che svelarono al pubblico tempi e modalità del coinvolgimento statunitense in Vietnam e che molto fecero per consolidare l'opposizione interna alla guerra.

87 *FBI File 100-NY-179649 - Technological American Party (TAP), Subversive Matter*,

testo consultabile all'indirizzo https://web.archive.org/web/20211030215318/http://www.historyofphonephreaking.org/docs/yipl-fbi.pdf.

88 C. Breen, C.A. Dailbom, *Signaling Systems for Control and Telephone Switching*, in «The Bell System Technical Journal», XXXIX, 1960, 6, pp. 1381-1444.

89 Lapsley, *Exploding the Phone*, cit., p. 9.

90 S. Binkley, *Getting Loose: Lifestyle Consumption in the 1970s*, Duke University Press, Durham 2007, p. 196.

91 Thomas, *Hacker Culture*, cit., pp. 62-63.

92 Una situazione economica che vede in contemporanea alta inflazione, recessione economica e alti tassi di disoccupazione.

93 «Questo Sistema universale, che in questo paese chiamiamo Mamma, fu davvero il creatore di noi tutti. [...] Il moderno sistema telefonico fu il creatore dell'Universo [...] Ecco perché, amici miei, non dovete giocare col vostro telefono. Ecco perché la Madre si adirerà se lo farete», recita ironicamente il phreak «Mark Bernay» in una registrazione dei tardi anni Sessanta intitolata *Reverend Mark Bernay Explains the True Nature of the Universe*, https://web.archive.org/web/20210821185427/http://www.wideweb.com/phonetrips/revbernay.mp3.

94 R. Rosenbaum, *Secrets of the Little Blue Box*, in «Esquire», ottobre 1971, pp. 117-125 e 217-226; G. Genosko, *When Technocultures Collide: Innovation from Below and the Struggle for Autonomy*, Wilfrid Laurier UP, Waterloo 2013, cap. 6.

95 R. Sherman, *Phone Phreaks in Phun City*, in «Ramparts», ottobre 1972, pp. 12-13.

96 P.D. Marshall, *The Promotion and Presentation of the Self: Celebrity as Marker of Presentational Media*, in «Celebrity Studies», 1, 2010, 1, pp. 35-48.

97 Levy, *Hackers*, cit., pp. 253-255.

98 Il «teatro di guerriglia» era la messa in scena, da parte di gruppi controculturali quali i Diggers, di performances improvvisate, politicamente motivate e oltraggiose per i temi trattati, il luogo in cui avvenivano o il linguaggio e il vestiario degli attori. Il gioco di parole si basa sulla similitudine tra «guerrilla» e «gorilla», che diventa «monkey» (scimmia) nella variazione di Hoffman.

99 J.R. Urgo, *Comedic Impulses and Societal Propriety: The Yippie! Carnival*, in «Studies in Popular Culture», X, 1987, 1, pp. 83-100.

100 A. Hoffman, *Revolution for the Hell of It*, Pocket Books, New York 1970, cap. 4.

101 M. Isserman, M. Kazin, *America Divided: The Civil War of the 1960s*, Oxford University Press, New York 2000, p. 233.

102 M. Jezer, *Abbie Hoffman, American Rebel*, Rutgers University Press, New Brunswick (N.J.) 1992, cap. 7; S.E. Shawyer, *Radical Street Theatre and the Yippie Legacy: A Performance History of the Youth International Party, 1967-1968*, tesi di

dottorato, University of Texas 2008, cap. 3, https://repositories.lib.utexas.edu/bitstream/handle/2152/17999/shawyers56058.pdf?sequence=2&isAllowed=y.

103 A. Hoffman, *Soon To Be A Major Motion Picture*, Putnam, New York 1980, p. 152.

104 Tutti i volantini sono raccolti e commentati in Hoffman, *Revolution*, cit.

105 Isserman, Kazin, *America Divided*, cit.

106 D. Walker, *Rights in Conflict: The Violent Confrontation of Demonstrators and Police in the Parks and Streets of Chicago during the Week of the Democratic National Convention of 1968*, Braceland Brothers, Philadelphia 1968.

107 Urgo, *Comedic Impulses*, cit.

108 Kelty, *Two Bits*, cit., p. 29.

109 Sherman, *Phone Phreaks*, cit.

110 *FBI File 100-NY-179649* cit.

111 S. Brand, *The Media Lab: Inventing the Future at MIT*, Viking, New York 1987, pp. 202-228.

112 F. Brunton, *Spam: A Shadow History of the Internet*, The MIT Press, Cambridge (Mass.) 2013, pp. 43-48.

113 Le due principali pubblicazioni hacker furono fondate non a caso tra il 1984 e il 1985, appena dopo la chiusura di «TAP». Il nome «2600. The Hacker Quarterly» è un chiaro omaggio alla frequenza in hertz usata dai phreaks per effettuare chiamate gratuite, mentre il PH in «Phrack» è un riferimento all'uso che delle due lettere facevano i phreaks. Lo stesso uso si trova nella parola «phishing», derivante da «fishing», a ulteriore testimonianza del lungo corso dell'influenza phreaker sulla cultura digitale.

3.
Whiz-kid, 1983-1990

Tre testi

L'emergere dell'hacking dall'accademia e dai ristretti circoli di appassionati di telefoni e il suo insediarsi nella coscienza collettiva e nel dibattito pubblico possono essere sintetizzati in tre testi. Tutti e tre emergono negli Stati Uniti tra il 1983 e il 1984.

Del primo si è già parlato: il saggio *Hackers: Heroes of the Computer Revolution* di Steven Levy. La descrizione della «nascita della cultura hacker» e dei punti fondamentali della sua etica è stata accettata non solo dalla gran parte degli accademici che si sono occupati della storia dell'hacking, ma anche dagli hackers stessi, e in particolare da chi, avvicinatosi alla pratica dopo la metà degli anni Ottanta, non conosceva nel dettaglio le vicende dei phreaks e la loro «etica». Il successo del libro nella comunità hacker è facilmente spiegabile: si tratta di una narrazione accessibile ed estremamente elogiativa, che permetteva ai neofiti di sentirsi parte di una cultura non solo di lunga e prestigiosa tradizione, ma ormai al centro della modernità. Levy annoverava infatti tra i «veri hackers» protagonisti della rivoluzione informatica, come Steve Wozniak e Steve Jobs, fondatori di Apple, Steve Russell e Alan Kotok, che lavorarono a uno dei primi videogiochi, *Spacewar!*, e Lee Felsenstein, designer del primo computer portatile[114].

Il secondo è un film di fantascienza, *WarGames*, uscito nel 1983 e subito di grande successo. La pellicola racconta le avventure di David Lightman (Matthew Broderick), un teenager geniale, ribelle e appassionato di informatica che, esplorando la rete, riesce a guadagnarsi l'accesso a un computer del NORAD (North American Aerospace Defense Command). Lightman è convinto di essere incappato in un videogioco

che simula una guerra tra Stati Uniti e Unione Sovietica. In realtà si tratta di Joshua, un'avanzata intelligenza artificiale che controlla l'arsenale nucleare statunitense e che minaccia di far scoppiare la terza guerra mondiale. Dopo svariate peripezie (Lightman deve scappare dai militari che lo credono una spia russa e rintracciare il programmatore dell'intelligenza artificiale) il ragazzino, grazie alla sua perspicacia e alla sua capacità di pensare fuori dagli schemi rigidi delle autorità adulte, riesce a disinnescare il conflitto, convincendo Joshua che l'unico modo per vincere il gioco della guerra termonucleare è non giocare.

La parola hacking non compare nel film, ma i giovani che al tempo si dilettavano nella pratica non avevano difficoltà a riconoscere che le azioni del protagonista erano quelle di un hacker/phone phreak: Lightman usava un modem per comporre automaticamente numeri di telefono in sequenza e individuare computer connessi alla rete; tentava di immaginare le passwords a partire da quelle più usate o dai pochi indizi a disposizione; modificava gli apparecchi hardware che lo circondavano per servire i propri fini; addirittura usava una tecnica phreak (non del tutto verosimile) per ottenere chiamate gratuite. Il messaggio del film, evidentemente pensato per un pubblico di teenagers, era esso stesso in linea con i valori della comunità dei phone phreaks e della nascente comunità hacker extrauniversitaria. La genialità, la curiosità e l'intraprendenza valgono più dell'educazione formale e dei titoli accademici. Gli eredi della rivoluzione informatica non erano le autorità adulte (ritratte nel film come comicamente ottuse), ma i giovani che comprendevano la logica e il potenziale liberatorio dei computer, soprattutto se usati come strumenti personali. Il film fu criticato dagli hackers del tempo per le sue imprecisioni tecniche, ma è costantemente citato, a volte con un qualche imbarazzo, come fonte di ispirazione per chi si accostava alla pratica dalla metà degli anni Ottanta ai primi anni Novanta[115]. Come si vedrà nelle pagine seguenti, esso ebbe un effetto profondo anche sulla percezione pubblica dell'hacking in quegli stessi anni, arrivando ad avere un ruolo non solo in innumerevoli caratterizzazioni giornalistiche, ma anche nell'iter che porterà alle prime leggi statunitensi sui crimini informatici.

Il terzo testo è un romanzo, *Neuromancer*, di William Gibson (1984),

oggi noto principalmente per due ragioni. La prima è che in esso è coniato il termine «cyberspazio»:

> Un'allucinazione consensuale di cui avevano esperienza quotidiana miliardi di operatori legittimi, in ogni nazione [...] Una rappresentazione grafica dei dati tratti da ogni computer nel sistema umano. Complessità impensabile. Linee di luce tracciate nel nonspazio della mente, gruppi e costellazioni di dati[116].

Come sappiamo, il neologismo sarebbe stato usato, dagli anni Novanta in poi, per indicare lo spazio immateriale del web; ma nell'immediato esso dava un nome e soprattutto un orizzonte immaginario a una pratica di nicchia, la navigazione in networks digitali attraverso computer, che allora coinvolgeva soltanto specialisti e giovani hackers.

Il secondo motivo di notorietà è il fatto che il romanzo dava i natali al nuovo genere fantascientifico del «cyberpunk»[117]. *Neuromancer*, come i tanti romanzi e film che si sarebbero ad esso ispirati, descriveva un mondo in cui enormi corporations governavano su masse abbrutite da una feroce lotta per la sopravvivenza in disumane megalopoli. La tecnologia era, in questo futuro distopico, ampiamente disponibile, nella forma di droghe, armi e soprattutto protesi in grado di aumentare le capacità umane. Allo squallore del mondo «reale» faceva da contraltare la libertà e la maestosità di Matrix, una realtà virtuale a cui era possibile collegarsi per via neurale. Il protagonista di *Neuromancer* è Case, un hacker (o «cowboy» nel gergo del libro) tanto inebriato dall'esperienza della rete quanto incapace di vivere nella realtà materiale. Assunto dal misterioso Armitage, Case si troverà a organizzare una serie di hacks (la parola non appare tuttavia nel libro e a quanto pare Gibson aveva scarsa dimestichezza con l'informatica)[118] che lo porteranno in contatto e in contrasto con cyborg, ninja e intelligenze artificiali.

Se Lightman rappresentava un *whiz-kid*[119], l'archetipo dell'intraprendenza e della perspicacia giovanile in chiara continuità con il genere delle edisonades (vedi cap. 1), il nichilista Case era un anti-eroe che sceglieva il cyberspazio come alternativa a un mondo corrotto, mettendo a rischio la propria incolumità psichica e fisica in nome di una vocazione insopprimibile, una vera e propria dipendenza, verso il mondo digitale. Entrambi i personaggi, accomunati dal disprezzo per le

regole e dall'estraneità al mondo delle autorità, ebbero ampio successo nelle comunità hacker extra-accademiche[120].

La realtà dell'hacking era ovviamente molto più mondana rispetto a quella immaginata in *WarGames* o *Neuromancer*. Un'efficace descrizione di cosa significasse essere un hacker negli anni Ottanta è fornita da The Mentor (Loyd Blankenship) in un file di testo (un *t-file*, secondo il gergo hacker del tempo) dedicato alla formazione dei neofiti e diffuso alla fine del 1988[121]. Il testo inizia con le regole di comportamento: non danneggiare mai i sistemi in cui si entra; non alterare i files se non è strettamente necessario a coprire le proprie tracce o ad assicurarsi un futuro accesso; stare alla larga dai computer governativi. L'infrazione della legge è spesso una conseguenza dell'hacking, ma non è il suo scopo: il «vero hacker» penetra nei sistemi per esplorare e raccogliere conoscenza.

Il luogo più sicuro dove cominciare la propria carriera di hacker erano, secondo The Mentor, le università, che spesso fornivano accesso alle aule informatiche anche a chi non era studente, dietro un piccolo pagamento. La sicurezza informatica nei colleges era notoriamente debole e gli amministratori erano abituati alle piccole infrazioni commesse dagli utenti. Difficile dunque che si rivolgessero alle autorità, se l'hacker non causava danni eccessivi.

Il passaggio successivo era lanciarsi nei networks informatici, preferibilmente quelli al tempo più estesi (Internet, il network che avrebbe connesso tutti i networks, era ancora di là da venire), perché assicuravano un grande numero di computer connessi (e perciò più possibilità di trovare falle di sicurezza) e perché erano ben mappati da hackers più esperti, che potevano aiutare il neofita. Le istruzioni diventano poi più tecniche, ma è utile riassumerle per comprendere cosa significasse, nella pratica, esplorare i sistemi informatici prima dell'avvento del web. Il primo passo era connettersi alla rete attraverso un modem, componendo un numero telefonico sul proprio computer. Una volta connesso, l'hacker si trovava davanti a un terminale, una stringa di testo che richiedeva all'utente di inserire comandi. Per connettersi a un qualsiasi computer era necessario conoscere il suo indirizzo, o *Network User Address* (NUA): non esistevano siti web o motori di ricerca. L'aspirante hacker poteva tuttavia fare riferimento alle liste di NUA

compilate dalla comunità. In alternativa poteva inserire numeri in sequenza, manualmente o attraverso un software, sperando di indovinare, a partire da vari indizi, il codice identificativo. Da notare che, una volta connesso a un altro computer della rete, l'hacker incorreva nei costi di una normale chiamata telefonica, locale o di lunga distanza, a seconda di dove era fisicamente il computer di destinazione. Di particolare interesse erano dunque le macchine che accettavano chiamate a carico, o i codici che permettevano di addebitare i costi della chiamata su accounts a pagamento o istituzionali. Dato che nella maggior parte dei casi ci si atteneva alla regola di non causare danni ai sistemi, questi costi di connessione 'rubati' avrebbero costituito la maggior parte dei danni che sarebbero stati imputati agli hackers nei processi degli anni Ottanta e primi Novanta.

Una volta connessi era necessario indovinare il login e la password per accedere ai files sul computer. Siccome la sicurezza non era, almeno fino alla fine degli anni Ottanta, un problema considerato pressante, le passwords erano spesso facili da indovinare e la comunità hacker si scambiava informazioni su quelle più comunemente usate.

Quello che si faceva una volta guadagnato l'accesso a un computer dipendeva dalla coscienza del singolo hacker e dal sistema in cui si era imbattuto. La casualità di quello che si poteva trovare era, come nel caso dell'etere o del sistema telefonico, parte integrante del divertimento e ciò che permetteva di caratterizzare l'esperienza come esplorazione. Dato che, nella maggior parte dei casi, i computer connessi non avevano files di particolare interesse pratico, esplorare era spesso l'unica attività: si cercavano files che garantissero un futuro accesso o trofei che potessero essere mostrati alla comunità per provare che si era riusciti ad entrare. Questo è peraltro confermato dal risultato di molti dei processi che seguirono alle vicende raccontate in questo capitolo: nessuno dei suoi protagonisti ha avuto significativi vantaggi economici dal proprio hobby – un fatto che rimarrà inspiegabile e sospetto per le autorità di polizia e giudiziarie. «Se ti stai chiedendo 'Perché fare hacking?' – conclude The Mentor – allora hai probabilmente perso un sacco di tempo a leggere tutto questo, perché non lo capirai mai».

La sociabilità hacker, come la maggior parte della sociabilità in rete negli anni Ottanta e primi Novanta, avveniva sui *Bulletin Board Systems* (BBS),

dei computer connessi alla linea telefonica che ospitavano bacheche elettroniche. L'utente esterno poteva chiamare, tramite modem, il numero del BBS di suo interesse e visualizzare sul proprio schermo tutti i messaggi che su questo avessero lasciato altri utenti. Già agli inizi degli anni Ottanta si assistette alla nascita di centinaia di BBS, spesso dedicati a interessi specifici, dai computer alla medicina, dallo sport alla fantascienza. Alcuni BBS permettevano di inviare email agli utenti registrati e di scaricare software, a volte anche software «piratati».

La connessione, in assenza di tariffe forfettarie, aveva i costi di una normale chiamata telefonica. Per questo molti BBS mantenevano una dimensione locale: gli utenti tendevano ad evitare i costi di una chiamata di lunga distanza. C'erano però dei modi per aggirare questo limite. I phone phreaks e gli hackers sapevano come effettuare chiamate di lunga distanza gratuite, usando «boxes» colorate o clonando carte di credito telefonico. Ma esistevano anche metodi più legittimi: i t-files, che sono fonti importanti per questo capitolo, erano files di testo che uscivano con regolarità, come una rivista, e che venivano numerati e riprodotti in BBS di diverse aree. Se un messaggio era giudicato abbastanza interessante era facile che venisse raccolto e riprodotto in diversi BBS. Le comunità hacker degli anni Ottanta nascevano dunque con più facilità su basi locali, ma sempre più, con l'avanzare del decennio, acquisivano carattere nazionale e in alcuni casi internazionale. In questo processo di diffusione importanza cruciale ebbero, come vedremo nel corso del capitolo, i media «tradizionali»: la stampa e la televisione.

The 414s

Il 5 settembre 1983 la copertina di «Newsweek» presentava un giovane sorridente davanti a un computer. Il titolo recitava *Computer Capers* («Marachelle con il computer») e la didascalia identificava il teenager come «Neil Patrick, hacker del gruppo 414». Il lungo articolo all'interno raccontava come i «414s», un gruppo di giovani hackers di Milwaukee (tra questi Gerald Wondra, Timothy Winslow e Neil Patrick), fossero riusciti a penetrare in diversi sistemi informatici, compresi quelli della base militare di Los Alamos e quelli che gestivano i pagamenti allo Sloan-Kettering Cancer Center di New York. I giovani si erano conosciuti nei

Boy Scouts e avevano cominciato ad appassionarsi ai computer in occasione di una gita presso un centro IBM. Erano venuti a conoscenza dell'esistenza di una pratica chiamata hacking da OSUNY, un BBS al tempo molto famoso per lo scambio di informazioni hacker e phreak, e avevano deciso di fondare un proprio BBS.

Il sistema utilizzato dai 414s ricordava quello usato da David Lightman in *WarGames*: un computer collegato a un modem chiamava una serie di numeri telefonici casuali. Dopo una nottata lo schermo presentava i numeri che avevano risposto e ai quali corrispondeva perciò un computer connesso alla rete. Gli hackers provavano dunque a inserire passwords in successione, nella speranza che una di queste permettesse l'accesso al computer. Secondo le stime di Gerald Wondra il sistema aveva permesso, nel corso di poco più di un anno, di penetrare in una dozzina di computer negli Stati Uniti e in Canada, con privilegi da amministratore[122]. In molti casi le passwords di successo erano quelle di fabbrica, riportate nei manuali di istruzioni delle macchine, mai cambiate dagli amministratori dei sistemi e diffuse nei BBS hacker.

Cosa fare una volta entrati nel sistema era di secondaria importanza. In un caso i ragazzini fecero stampare tutti i files presenti nei computer di un'industria di cemento, inondandone gli uffici di carta. In altri casi lasciarono sui computer citazioni da *WarGames*. Se c'erano videogiochi installati nel computer penetrato, gli hackers passavano qualche ora a giocare, associando il nome «414» al punteggio raggiunto in classifica[123]. Fu proprio grazie a un videogioco, lasciato di proposito dagli investigatori su uno dei computer in cui gli hackers erano già penetrati, a permettere il loro tracciamento e il loro arresto nei primi mesi del 1983.

Il caso dei 414s, per quanto banale se messo a confronto con gli hacks che avrebbero avuto luogo negli anni successivi, è importante per l'intensa attenzione mediatica che ricevette, molto probabilmente perché i giovani hackers guadagnarono notorietà nella stessa estate in cui *WarGames* usciva nelle sale cinematografiche.

L'articolo di «Newsweek», il primo nel quale degli hackers ricevevano un'attenzione nazionale, aveva un tono simpatetico e a tratti ammirato. Il pezzo dava voce a personaggi rispettati come Steve Wozniak («Spero che i miei figli diventino come [i 414s]») e Richard Stallman («[noi hackers]

non crediamo al diritto di proprietà») e dava credito al fatto che le «marachelle» erano state compiute solo per curiosità e come prova di intelligenza. I giovani erano messi in continuità sia con gli Yippies, con la loro «gioviale mancanza di rispetto per le regole», sia con i ben più esperti e affermati hackers universitari. *WarGames* era correttamente definito «una fantasia senza fondamento»: i computer del NORAD non erano collegati alla rete e non avevano controllo sui missili nucleari. Questo non impediva agli articolisti di comparare i giovani hackers a David Lightman, con il quale i 414s sembravano condividere genialità, intraprendenza e precocità. Il pezzo si concludeva con un commento di un accademico che accostava gli hackers a moderni Robin Hood: «I media si sono innamorati [dei giovani hackers], forse perché ci mostrano che abbiamo ancora controllo sui computer. Inconsciamente vediamo dei ragazzini penetrare in questi mostri e vendicare la nostra perdita di privacy, individualità o qualsiasi cosa temiamo di aver perso a causa dei computer»[124].

Dopo un certo sensazionalismo legato alla provenienza dei computer penetrati (gli hackers potevano lanciare un attacco missilistico? Potevano cambiare le cartelle cliniche o appropriarsi di conti bancari?)[125] e una volta verificato che i danni causati dal gruppo erano minimi, anche per altri media nazionali la notizia divenne il fatto che David Lightman esisteva nella realtà e si chiamava Neil Patrick. Unico del gruppo a non essere ancora diciottenne, Patrick poteva permettersi di raccontare le imprese del gruppo a un sistema mediatico avido di ascoltarle, senza paura di essere perseguito legalmente. Dopo «Newsweek», Patrick fu ospite di svariati talk shows, fu oggetto di numerosi articoli e soprattutto fu invitato a testimoniare davanti al Congresso in relazione al nuovo fenomeno del crimine informatico[126].

Non vi è dubbio che le «marachelle» dei 414s e il successo del film *WarGames* costituirono un punto di svolta nella storia dell'hacking, nonostante i primi fossero praticamente sconosciuti alle comunità hacker e il secondo fosse un'opera esplicitamente fantascientifica. Fino ad allora la legislazione statunitense mancava di mezzi specifici per punire i crimini informatici, in special modo se questi non riguardavano minacce o furti di documenti di valore. Il semplice ingresso illecito in uno spazio

virtuale non costituiva in sé un crimine e i tentativi di applicare le leggi sulla violazione di domicilio andavano spesso a vuoto una volta raggiunti i tribunali. Allo stesso modo, le leggi sul furto di beni materiali mal si adattavano all'accesso non autorizzato a files, oggetti infinitamente riproducibili che non venivano in effetti sottratti al loro legittimo proprietario, anche quando illecitamente copiati[127]. Ma a seguito del dibattito pubblico sui 414s il Congresso statunitense emanava, tra il 1984 e il 1986, il *Computer Fraud and Abuse Act*, che rendeva crimini l'ingresso non autorizzato nei sistemi informatici e il traffico illecito di passwords.

L'influenza di *WarGames* percorre l'intero iter legislativo[128]. L'udienza dell'aprile 1984, cui fu invitato Neil Patrick in qualità di testimone, era stata aperta dalla proiezione di un pezzo del film, «ad illustrare – come recita il verbale ufficiale – la facilità con la quale i computer sono vulnerabili all'accesso da parte di individui non autorizzati». La stessa pellicola (nella quale, si ricordi, un computer senziente gestiva, senza alcun controllo umano, l'intero arsenale nucleare statunitense) era citata nella discussione sulla nuova legge come «una rappresentazione realistica della composizione automatica dei numeri telefonici e delle capacità di accesso del personal computer»[129].

La svolta non sfuggì peraltro agli stessi hackers. Il primo articolo del primo numero di quella che sarebbe diventata la più importante rivista dell'underground informatico, «2600. The Hacker Quarterly», notava che «Molto è cambiato rispetto ai nostri primi giorni. È uscito *WarGames*. E poi i 414s sono stati catturati. Improvvisamente tutti parlavano di phreaks e hackers»[130]. L'attenzione non era sempre benvenuta. Poco dopo essere stata menzionata su «Newsweek» OSUNY fu chiusa[131]. Molti scritti retrospettivi individuano nell'arresto dei 414s e nell'uscita di *WarGames* il momento in cui l'hacker si era trasformato da una «persona che può fare cose magnifiche con il computer» in una persona che «fa cose criminali con un computer»[132]. Tra la fine degli anni Ottanta e l'inizio dei Novanta alcuni hackers mostrarono per questo motivo una certa ostilità verso i 414s, ragazzini inesperti e incauti che, per giocare a videogiochi e imitare un film, avevano portato l'attenzione della legge anche sui veterani:

> Infine è successo, il film *WarGames* è uscito e masse di undicenni sono andati a

vederlo. Il problema non era che il film era brutto, ma che da allora TUTTI vogliono diventare un hacker/phreak. Spuntavano neofiti da tutte le parti, le bulletin boards cominciavano a essere intasate 24 ore al giorno. Ad oggi [nel 1987] non si sono ancora riprese. Altri problemi sono emersi, i neofiti indovinavano passwords semplici su grandi computer governativi e cominciavano a giocarci... Beh, non ci è voluto molto perché fossero beccati, penso tutti ricordino gli hackers 414. Sono stati così stupidi da rispondere «sì» quando il computer ha chiesto se volevano giocare a videogames[133].

Tra il 1983 e il 1984 l'hacking era passato da impenetrabili laboratori universitari e oscure bacheche digitali alla fiction hollywoodiana, alle pagine della stampa e ai talk shows televisivi, per approdare infine nelle aule dei legislatori. La caratterizzazione dell'hacker era, in questo primo periodo e come abbiamo visto, ancora largamente positiva ed ispirata alle narrazioni che a suo tempo avevano glorificato l'intraprendente radioamatore e il ragazzino prodigio che sperimentava in prima persona le possibilità della scienza e della tecnologia. Come testimonia Sherry Turkle, che nel 1984 aveva intervistato alcuni newyorkesi in merito a un hack operato da dei teenagers, la prima reazione dell'opinione pubblica fu di ammirazione per dei giovani che avevano «battuto il sistema», rappresentato da macchine che erano ancora percepite come di dominio del governo e delle grandi corporations. Venticinque anni dopo la stessa Turkle commentava che, con la crescente importanza dei computer per la sicurezza personale e finanziaria, il confine tra bravata ingegnosa e crimine era meno netto e che «è ora raro trovare simpatia per gli scherzi via computer, o che essi siano visti come resistenza innocua al fatto che 'ci sono troppi computer'»[134].

La nuova legge segnava infatti l'inizio di una graduale criminalizzazione dell'hacking. «È ora di instillare la paura divina in questa gente», aveva minacciato un funzionario governativo sulle pagine di «Newsweek». «Pretendiamo la privacy, eppure glorifichiamo chi entra illegalmente nei computer», lamentava uno dei deputati firmatari della proposta della nuova legge[135]. I fatti degli anni successivi avrebbero risolto questo paradosso.

Internet worm

Nel 1988 Internet era un «luogo» molto diverso da oggi o da quello che

sarebbe stato anche solo cinque anni dopo. Al tempo vi erano connessi circa 60.000 computer, collocati soprattutto negli Stati Uniti. Non esistevano il web o i motori di ricerca: entrambi sarebbero stati inventati l'anno dopo e avrebbero conosciuto una certa diffusione solo dalla metà degli anni Novanta. La navigazione non avveniva dunque attraverso elementi grafici (le finestre, i link, i siti web), ma attraverso comandi alfanumerici. Lo stesso si poteva dire dei computer connessi alla rete: questi montavano perlopiù diverse versioni di UNIX, un sistema operativo che non aveva al tempo alcuna interfaccia grafica. La comunità di utenti di Internet era relativamente ristretta ed omogenea, composta da ricercatori universitari, governativi o militari e pochi attori aziendali, perlopiù coinvolti nello sviluppo dell'infrastruttura informatica.

È in questa Internet primordiale che, il 2 novembre 1988, per la prima volta si diffuse un «worm»[136]. Entrato nella rete da un computer del Massachusetts Institute of Technology (MIT), si sarebbe in poche ore riprodotto in migliaia di macchine. Una volta installato, il worm esplorava le connessioni che il computer aveva con il mondo esterno e, usando svariati bugs di UNIX, inviava sé stesso ai contatti del proprio ospite, installandosi automaticamente nella nuova macchina e ricominciando il processo di ricerca di contatti esterni. Il programma non aveva altro obiettivo che riprodursi: non raccoglieva informazioni, non intaccava gli applicativi o i dati già presenti sui calcolatori[137]. Svelava le passwords di accesso dei sistemi, ma con il solo obiettivo di replicarsi, senza insediarsi nel sistema operativo, senza prendere controllo delle macchine e senza registrare le passwords per assicurarsi un futuro accesso.

Tuttavia l'attività di ricerca delle connessioni, ripetuta incessantemente da più copie del programma installate contemporaneamente, era sufficiente a mandare in arresto le macchine. Inoltre, soprattutto nelle prime ore dell'attacco, non vi era alcuna certezza sulle capacità del worm, sul suo autore o sul modo migliore per fermarlo. Le sue funzioni sembravano innocue dal punto di vista della sicurezza delle informazioni, ma la scala stessa dell'attacco e il fatto che riguardava anche Milnet, la porzione di rete dedicata alle basi militari, scatenarono il panico nei centri di ricerca. La soluzione più semplice e immediata era scollegare i computer dalla rete. Tuttavia molte analisi successive hanno evidenziato

come questo sia stato in realtà controproducente[138]: già nel 1988 chi aveva accesso a Internet comunicava prevalentemente via mail. La disconnessione impediva l'installazione di nuove copie del worm, ma anche lo scambio di informazioni e di soluzioni che avevano avuto un qualche successo in altri centri di ricerca.

L'identità dell'autore del worm fu svelata grazie a una chiamata anonima a John Markoff, un giornalista del «New York Times» specializzato in informatica che, come vedremo, è stato una presenza costante nella storia dell'hacking negli anni Novanta e che contribuì significativamente, con i suoi articoli e con svariati libri, alla costruzione dell'immagine pubblica degli hackers in quanto banditi. Come racconta lo stesso Markoff, l'informatore anonimo si tradì, indicando con le lettere *rtm* l'autore del worm. Una ricerca di questo acronimo su una directory di nomi utente di chi aveva al tempo accesso a Internet rivelò che *rtm* corrispondeva al login di Robert Tappan Morris, uno studente di informatica della Cornell University. L'identità fu confermata, secondo Markoff, dallo stesso padre di Morris, che conosceva il giornalista e lavorava, come crittografo e matematico, per la National Security Agency (NSA), l'agenzia statunitense preposta al controllo delle comunicazioni elettroniche[139].

L'obiettivo di Morris, come riconosciuto dalla corte che lo condannò per infrazione del *Computer Fraud and Abuse Act*, non era ostile. Si trattava anzi di uno dei primi casi, per quanto maldestro, di quello che in seguito sarebbe stato definito «white hat hacking», la pratica di penetrare in sistemi informatici non per semplice curiosità o volontà di esplorazione, né per raccogliere illecitamente informazioni o per vandalismo, ma per evidenziare falle di sicurezza nei sistemi e permettere agli amministratori di colmarle prima che un hacker malintenzionato se ne avvantaggiasse. Sconosciuta al tempo, la pratica sarebbe divenuta fondamentale per l'industria della sicurezza informatica ed è il motivo per il quale molti dei suoi addetti si definiscono oggi hacker (vedi il paragrafo su L0pht, cap. 7).

L'Internet worm (o Morris worm, come sarebbe stato conosciuto dopo l'identificazione del suo autore) aveva infatti un sistema di sicurezza che avrebbe dovuto impedire qualsiasi danno ai sistemi. Ad ogni nuova

connessione il programma avrebbe «chiesto» alla macchina di destinazione se avesse già una copia del virus installata. Se la risposta fosse stata positiva il worm non si sarebbe trasferito, per evitare installazioni multiple che avrebbero bloccato i sistemi. Se tutto avesse funzionato come previsto il software sarebbe stato del tutto invisibile, almeno fino a che Morris non lo avesse rivelato, svelando al contempo le falle di sicurezza che gli permettevano di funzionare.

Morris, come tanti hackers prima e dopo di lui, era animato da uno spirito competitivo, sia nei confronti delle macchine sia nei confronti dei propri pari. Preoccupato che un programmatore avversario potesse scoprire il worm e fermare la sua diffusione semplicemente simulando una risposta positiva da parte della macchina di destinazione, fece sì che, ogni sette risposte positive, il virus si installasse ugualmente. Ma Morris aveva sottovalutato enormemente il numero di computer connessi alla rete e conseguentemente il numero di «domande» di installazione che ogni singola macchina avrebbe ricevuto contemporaneamente, anche a scapito del dispositivo di sicurezza: abbastanza per mandare fuori uso anche il miglior computer del tempo[140]. Sebbene involontariamente, Morris aveva lanciato il primo «denial of service attack»[141] della storia di Internet.

Quando Morris si rese conto di quanto stava succedendo, confessò l'accaduto al padre e, con l'aiuto di un amico di Harvard (l'informatore di Markoff), cercò di inviare a diversi centri universitari le istruzioni per debellare il virus e impedire nuove installazioni. Era già troppo tardi: molti dei nodi della rete che non erano stati messi fuori uso si erano disconnessi per precauzione. Internet era, per la prima e fino ad oggi ultima volta, in larga parte offline. Le macchine infettate furono quantificate in circa 6.000 e i danni causati furono stimati dalle autorità giudiziarie come compresi tra 200 e 53.000 dollari *per ogni computer*[142].

Se si eccettuano però questi costi, legati al ripristino dei sistemi e al tempo di calcolo perso, gli effetti pratici del worm furono molto ridotti. In pochi giorni diversi gruppi di ricerca al MIT, a Berkeley e alla Purdue University avevano disassemblato[143] il codice e prodotto una patch che impediva il suo funzionamento. In una ulteriore dimostrazione della competitività hacker i programmatori universitari arrivarono persino a

pubblicare i bugs del Morris worm, suggerendo ironicamente come avrebbe potuto essere reso più letale[144].

Le conseguenze legali per Robert Morris furono limitate se confrontate ai danni stimati: tre anni di prigione con la condizionale, 400 ore di servizio comunitario e 10.000 dollari di multa. La narrazione mediatica, per quanto spesso eccessivamente allarmista rispetto al virus e alle sue conseguenze, non demonizzò il suo autore[145]. In alcuni casi la stampa arrivò anzi a lodarlo, ringraziando Morris per aver allertato la società sui rischi legati alla sicurezza informatica. Questa relativa benevolenza era certo dovuta all'immagine sostanzialmente positiva che l'opinione pubblica americana aveva fino ad allora del whiz-kid: il fatto che uno studente fosse stato capace, da solo e solo scrivendo alcune righe di codice, di mettere in ginocchio il sistema informatico governativo, universitario e industriale rafforzava l'ideale di tecnologia dal basso proprio della cultura statunitense almeno dalla fine dell'Ottocento (vedi cap. 1). La buona fede di Morris fu riconosciuta tanto dall'opinione pubblica quanto dalle autorità giudiziarie[146]. Ma è probabile che la sua posizione al centro del sistema universitario e governativo (promettente studente di Cornell e figlio del capo del servizio di sicurezza informatica della NSA) abbia avuto un ruolo nelle conseguenze relativamente miti dei suoi atti e nel fatto stesso che le autorità giudiziarie fossero disposte a credere all'involontarietà dei danni causati. L'impressione è rafforzata dal duro trattamento mediatico e giudiziario riservato a Kevin Mitnick, un hacker esterno ai centri di ricerca istituzionali, solo pochi anni dopo e in assenza di danni economici comparabili (vedi capitolo seguente).

Le conseguenze psicologiche dell'evento furono in ogni caso profonde. L'applicazione del *Computer Fraud and Abuse Act* fu resa più severa nella sua interpretazione di cosa significassero intenzionalità punibile e accesso autorizzato[147]. A pochi giorni dalla diffusione del worm la NSA aveva già cominciato a discutere di possibili soluzioni di lungo periodo. Meno di un mese dopo il Dipartimento della Difesa finanziava la fondazione di una task force di risposta alle crisi di sicurezza informatica, il CERT (Computer Emergency Response Team, ancora oggi esistente presso la Carnegie Mellon University).

Non meno importanti furono le ripercussioni del worm sulla comunità

degli specialisti di informatica. Nel dicembre 1989 Joyce Reynolds pubblicava un messaggio dal titolo *L'elmintiasi di Internet*[148] nella newsletter del Network Working Group, il team di specialisti che, dal 1969 ad oggi, ha deciso gli standard tecnici e le politiche di Internet[149]. In esso si constatava che il worm aveva risvegliato la comunità dei programmatori sul tema della sicurezza informatica: dopo di esso chiunque si fosse occupato di sistemi e di networks avrebbe dovuto assumersi la responsabilità della loro vulnerabilità. La collaborazione tra i membri del ristretto gruppo di chi aveva accesso alla rete (l'«old boy network», come lo definisce Reynolds) era stata essenziale. La disponibilità del codice sorgente era il primo dispositivo di sicurezza, in quanto avrebbe reso superfluo il laborioso e lungo lavoro di disassemblaggio.

L'incidente aveva inoltre provato che l'informatica comportava ormai seri problemi etici, che i centri di ricerca dovevano dibattere, esplicitare e tradurre in codici di condotta ufficiali[150]. Il disvelamento pubblico di falle informatiche giustifica il danno causato e il rischio che attori malintenzionati si possano avvantaggiare di questa conoscenza? D'altra parte, se le falle non sono rese pubbliche, non vi è il rischio che gli amministratori di sistema e i produttori di software le ignorino, volontariamente o meno, offrendo servizi meno sicuri? Sono domande che attraversano tutta la storia dell'hacking, che ancora oggi dividono gli esperti e che acquisiranno particolare urgenza nel nuovo millennio (vedi cap. 7).

Ma la conseguenza probabilmente più importante del Morris worm si ebbe a livello mediatico. Il caso dei 414s aveva per la prima volta mostrato alla stampa che i sistemi informatici non erano per soli specialisti, ma erano alla base di aspetti essenziali della vita quotidiana, come la gestione delle cartelle cliniche e i conti bancari. Il Morris worm dimostrava la fragilità di questi servizi fondamentali, ora digitalizzati. La minaccia dei virus informatici, fino ad allora meramente teorica e discussa solo dagli specialisti, si era infine realizzata: era solo un caso, secondo molti osservatori, che l'attacco fosse partito da uno studente e non da un agente straniero.

Al contempo gli organi di informazione ebbero la conferma del fatto

che mettere un hacker in prima pagina a pochi giorni da un'elezione presidenziale (quella che l'8 novembre 1988 vide vincitore George H.W. Bush) non era stato un errore. La metafora del virus, per quanto nata in ambiente informatico, aveva, nel bel mezzo della crisi dell'AIDS, una particolare efficacia in ambito giornalistico e una particolare risonanza presso l'opinione pubblica[151]. Il crimine informatico, nonostante il pubblico avesse poca familiarità con i computer (o forse proprio in ragione dell'aura misteriosa che ancora li circondava), richiamava lettori e spettatori. I tempi erano maturi per un'attenzione ancora più vorace e per un trattamento ben meno simpatetico.

114 Levy, *Hackers*, cit., p. 437.

115 Come si apprende, ad esempio, dalle interviste a personaggi della comunità hacker pubblicati da «Phrack»: n. 28, file 2; n. 33, file 2; n. 38, file 3; n. 51, file 4; n. 53, file 4. Dato che «Phrack» non ha una versione cartacea si citano qui il numero della raccolta di files e quello del file a cui si riferisce. Tutti i files sono reperibili all'indirizzo https://web.archive.org/web/20211009005852/http://www.Phrack.org/archives/issues/.

116 W. Gibson, *Neuromancer* (1984), Ace Books, New York 2004, p. 51 (trad. it., *Neuromante*, Editrice Nord, Milano 1986).

117 *Cyberpunk*, in *The Encyclopedia of Science Fiction*, a cura di J. Clute e D. Langford, 2015, https://web.archive.org/web/20210731154556/http://www.sf-encyclopedia.com/entry/cyberpunk. Tra i pionieri del genere, il racconto *Do Androids Dream of Electric Sheep?* (Philip Dick, 1968) e la sua trasposizione filmica *Blade Runner* (1982), e soprattutto il romanzo *The Shockwave Runner* di John Brunner (1975), esso stesso con protagonista un hacker.

118 S. Bukatman, *Gibson's Typewriter*, in *Flame Wars: The Discourse of Cyberculture*, a cura di M. Dery, Duke University Press, New York 1994, pp. 71-90.

119 Letteralmente «ragazzo mago» (whiz è abbreviazione e alterazione di wizard); in italiano può essere approssimativamente tradotto come «bambino prodigio».

120 «Phrack», n. 30, file 8.

121 The Mentor, *A Novice Guide to Hacking*, dicembre 1988, https://web.archive.org/web/20211202033434/http://textfiles.com/hacking/lodhbasi.hac.

122 Intervista a Gerald Wondra in M.T. Vollmann, *The 414s: The Original Teenage Hackers*, 2021, https://vimeo.com/502242358.

123 Intervista a Timothy Winslow, *The Kid Hackers Who Starred in a Real-Life*

WarGames, in «The Telegraph», 16 settembre 2015.

124 *Beware: Hackers at Play*, in «Newsweek», 5 settembre 1983.

125 P. Elmer-DeWitt, *Computers: The 414 Gang Strikes Again*, in «Time Magazine», CXXII, 1983, p. 9.

126 Subcommittee on Transportation, Aviation and Materials, *Computer Communications Security and Privacy*, U.S. Congress, Washington, 1984.

127 A. Burstein, *A Survey of Cybercrime in the United States*, in «Berkeley Technology Law Journal», XVIII, 2003, 1, pp. 313-338.

128 C. Andoh, A. Godderis, *The Virtual Wall of the Fourth Amendment*, in «IEEE Annals of the History of Computing», XLI, 2019, 1, pp. 47-50.

129 *House of Representatives Report 98-894*, in *United States Congressional Serial Set. Nos. 892-952*, U.S. Government Printing Office, Washington, D.C. 1986.

130 *AHOY!*, in «2600. The Hacker Quarterly», I, 1984, 1, p. 1.

131 *Ibid*.

132 «Phrack», n. 21, file 9; il punto di svolta è confermato da Cheshire Catalyst (Robert Osband), ultimo redattore di «YIPL/TAP», in *TAP: The Legend Is Dead*, in «2600. The Hacker Quarterly», IV, 1987, 1, pp. 4-5, e da Richard Stallman in D.E. Denning, *Concerning Hackers Who Break into Computer Systems*, 1990, https://web.archive.org/web/20160806014912/http://insecure.org/stf/Denning_concerning_hackers.html.

133 Jack The Ripper, The Jammer, *The Official Phreaker's Manual v. 1.1*, febbraio 1987, https://web.archive.org/web/20090426035234/http://www.textfiles.com/phreak/PHREAKING/manual1.txt. Simili sentimenti, in forma più colorita, sono espressi in un altro t-file da Jolly Roger, *The Basics of Hacking II*, https://web.archive.org/web/20150727021016/http://cd.textfiles.com/group42/ANARCHY/COOKBOOK/BHT2.HTM.

134 Turkle, *The Second Self*, cit., p. 215.

135 Bill McCollum, citato in «Phrack», n. 7, file 9.

136 Un worm si distingue dagli altri virus informatici per la sua capacità di riprodursi automaticamente sul sistema infettato, laddove un semplice virus richiede l'installazione da parte di un utente, per quanto spesso ignaro. Un worm è un software indipendente, mentre un virus, come il suo analogo biologico, si insedia di norma in un programma già esistente.

137 B. Page, *A Report on the Internet Worm. The Virus We Were All Waiting For. Chaos in the Computer Networks*, in «2600. The Hacker Quarterly», V, 1989, 4, pp. 4-9.

138 J.A. Rochlis, M.W. Eichin, *With Microscope and Tweezers: The Worm from MIT's Perspective*, in «Communications of the ACM», XXXII, 1989, 6, pp. 689-698.

139 K. Hafner, J. Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon & Schuster, New York 1991, pp. 261-262.

140 *US v. Morris, 928 F. 2d 504*, Court of Appeals, 2nd Circuit 1990.

141 Un attacco cioè che, attraverso il sovraccarico delle risorse di un sistema, ne impedisce temporaneamente il funzionamento. È oggi tipicamente usato per oscurare siti internet, simulando un numero di visite superiore a quello che il server bersaglio può gestire (vedi cap. 7).

142 *US v. Morris*, *928 F. 2d 504*, cit.

143 Programmare significa nei fatti scrivere dei comandi leggibili da un essere umano che saranno poi automaticamente tradotti (assemblati) in codice macchina, gli 0 e gli 1 che costituiscono il linguaggio dei computer. Disassemblare è il processo contrario: partire dal codice binario per ricavare i comandi che sono stati usati per programmare un software, gli unici utili per comprenderne il funzionamento e, nel caso, modificarlo o impedirlo.

144 «Phrack», n. 22, file 8.

145 Tanto che Morris è ora un professore nello stesso Massachusetts Institute of Technology da dove il worm era per la prima volta entrato nella rete.

146 J. Markoff, *Student, after Delay, Is Charged in Crippling of Computer Network*, in «The New York Times», 27 luglio 1989.

147 Questo avrebbe portato, negli anni a venire e con la diffusione dei personal computers e dei servizi online, a un'applicazione estremamente ampia, che è arrivata a coprire anche l'infrazione dei termini di servizio delle piattaforme. P. Higgins, *Critical Fixes for the Computer Fraud and Abuse Act*, in «Electronic Frontier Foundation», https://web.archive.org/web/20211209153750/https://www.eff.org/deeplinks/2013/01/these-are-critical-fixes-computer-fraud-and-abuse-act.

148 J. Reynolds, *The Helminthiasis of the Internet. RFC 1135*, IETF Tools, 1989, https://web.archive.org/web/20220411130805/https://datatracker.ietf.org/doc/html/rfc1135. Elmintiasi significa infestazione da vermi ed è un ovvio riferimento al «worm».

149 L. Gitelman, *Always Already New: Media, History and the Data of Culture*, The MIT Press, Cambridge (Mass.) 2006, pp. 108-111.

150 Il citato RFC 1135 stimava con ottimismo «Lo sviluppo di standard etici obbligatori e condivisi dall'intera comunità degli informatici, insieme a leggi apposite, dovrebbe aiutare a eliminare definitivamente il crimine informatico»: Reynolds, *The Helminthiasis of the Internet*, cit.

151 Hafner, Markoff, *Cyberpunk*, cit., pp. 261-262.

4.
Dark-side hacker, 1990-1995

Operation Sun Devil e la Electronic Frontier Foundation

Il 15 gennaio 1990 il sistema telefonico di lunga distanza di AT&T smise improvvisamente di funzionare. Per nove ore 60.000 utenti persero il servizio. I disagi sarebbero continuati per giorni. Sebbene una portavoce di AT&T si fosse affrettata a specificare che la causa non era «un virus, un worm o niente di così pericoloso»[152], l'incidente, dovuto a un bug nei software dei centri di smistamento chiamate, dimostrava nuovamente la fragilità dei sistemi informatici e all'inizio fu erroneamente attribuito agli hackers. In maniera forse ancora più importante, il blackout metteva la popolazione a conoscenza del fatto che anche un atto quotidiano e dato ormai per scontato come la telefonata dipendeva da un software. Il sistema non era stato messo in ginocchio da degli hackers, ma poteva esserlo. La pressione per un intervento delle forze dell'ordine, sia da parte dell'opinione pubblica sia, soprattutto, da parte delle compagnie telefoniche, stava diventando irresistibile.

Il 9 marzo 1990 150 agenti federali operavano 27 perquisizioni in tutti gli Stati Uniti, arrestando sette teenagers e sequestrando 42 computer e più di 20.000 floppy disks. Era il punto apicale di Operation Sun Devil, un'indagine iniziata nel 1988 che vedeva la collaborazione dei servizi segreti, dell'FBI e dei servizi di sicurezza di tutti i maggiori operatori telefonici del tempo.

Il principale bersaglio del raid era un gruppo di hackers che chiamava sé stesso «Legion of Doom» (LoD), come il gruppo di super villains dei fumetti di Superman. Fondato nel 1984, il gruppo raccoglieva all'inizio degli anni Novanta circa una ventina di hackers extrauniversitari e curava la pubblicazione elettronica di t-files celebri nell'underground

elettronico, raccolti sotto il nome di «The LoD Technical Journal», oltre a un BBS riservato ai membri (150 gli invitati) in cui si scambiavano esplicitamente informazioni illegali[153].

Gli arresti rappresentavano in primo luogo un messaggio ai giovani che manomettevano computer, linee telefoniche e carte di credito: l'hacking era un crimine serio e l'anonimato non li avrebbe protetti. La retorica dei comunicati stampa che accompagnarono la retata era altisonante («L'hacking illegale dei computer mette in pericolo la salute e il benessere di individui, corporations e agenzie governative negli Stati Uniti [...] l'uso improprio e probabilmente illegale del computer può diventare il crimine principale dei colletti bianchi negli anni Novanta»)[154], le capacità degli hackers erano decisamente esagerate e i danni stimati erano altissimi, per quanto mai precisamente quantificati (una giornalista di «Newsweek» parlò di 50 milioni di dollari in sole chiamate gratuite). Le basi legali degli arresti, al contrario, erano molto deboli. Certo, i giovani hackers avevano commesso un crimine nel raccogliere codici telefonici e penetrare nei sistemi informatici dei centri di smistamento telefonico, ma l'entità dei danni causati o il guadagno economico dei perpetratori non erano chiari. Ben presto le autorità dovettero contemplare la possibilità che, incomprensibile per quanto potesse a prima vista apparire, questi ragazzini avessero accumulato la conoscenza necessaria ai propri hacks e si fossero assunti il rischio di portarli a termine per solo divertimento o, per dirla con Eric Bloodaxe (pseudonimo di uno dei perquisiti), per un «gran miglioramento [big boost] della [loro] reputazione nell'underground»[155].

Tra i computer sequestrati più della metà ospitavano dei BBS, i *fora* online che, prima del web, costituivano il principale mezzo di incontro telematico. La chiusura forzata di questi luoghi poneva per la prima volta questioni legislative e morali ancora oggi aperte. La libertà di parola doveva essere protetta online quanto lo era sulla stampa? Il codice di programmazione era protetto dalle leggi sulla libertà di parola? I gestori dei BBS (o, oggi, dei social networks) erano responsabili di quanto pubblicato sulle loro piattaforme, come nel caso di pubblicazioni cartacee? O, come le compagnie telefoniche, dovevano essere considerati

fornitori di servizi, non responsabili nel caso questi fossero stati usati illegalmente?

La questione della libertà della parola digitale si era già posta un anno prima, nel 1989, quando le autorità avevano rivelato di aver tenuto sotto controllo le comunicazioni della rivista elettronica «Phrack», di aver arrestato i suoi due fondatori, Knight Lightning (Craig Neidorf) e The Prophet (Robert Riggs), e averli spinti a rivelare i nomi degli altri redattori e degli iscritti alla loro mailing list. L'accusa principale era quella di aver illegalmente ottenuto e pubblicato un documento che spiegava in dettaglio il funzionamento del sistema telefonico per le chiamate di emergenza, il 911. Le informazioni in esso contenute mettevano in pericolo, secondo l'accusa, vite e proprietà, permettendo a malintenzionati di manomettere la comunicazione tra cittadini e forze dell'ordine. Il valore del file rubato era stato stimato in quasi 80.000 dollari e i due hackers, appena ventenni, rischiavano decenni di prigione. Il processo avrebbe rivelato che il documento incriminato era in realtà ottenibile legalmente per pochi dollari, che nessuna penetrazione del sistema 911 poteva essere provata e che non vi era stato nessun danno effettivo per la compagnia telefonica[156]. Neidorf e Riggs sarebbero stati assolti con formula piena.

Tale rivelazione arrivava in concomitanza con i racconti dei sequestri e delle perquisizioni di Operation Sun Devil e metteva in primo piano la questione della libertà della parola elettronica. I redattori di «2600» fecero correttamente notare in un editoriale che quello che era successo a «Phrack» (le cui comunicazioni erano state controllate, i cui computer erano stati confiscati e i cui redattori si trovavano penalmente implicati per aver pubblicato un'informazione in loro possesso) non sarebbe potuto accadere a «2600», per il semplice fatto che quest'ultima era pubblicata su carta: «Se una rivista stampata fosse stata chiusa in questa maniera, dopo aver aperto e letto tutta la sua corrispondenza, anche i media più ottusi e sensazionalistici se ne sarebbero accorti: ehi, non è una violazione del Primo Emendamento?»[157].

Il caporedattore Emmanuel Goldstein (Eric Corley) discuteva nello stesso numero di «2600» i dettagli del documento incriminato[158] e la

rivista ironicamente offriva di venderlo ai lettori per «soli» 20.000 dollari.

Un altro fenomeno che i raid del 1989-1990 rendevano evidente era l'imbarazzante incompetenza informatica delle autorità e della stampa generalista. Le pubblicazioni hacker del periodo riportavano con incredulo sprezzo gli episodi più paradossali emersi dai primi contatti tra l'underground digitale e le forze dell'ordine. Un poliziotto aveva spiegato alla madre di un membro di LoD che suo figlio aveva causato danni per un miliardo di dollari[159]. Un altro agente era convinto che un programma di editing grafico «piratato» permettesse di entrare nei sistemi informatici Apple.

La confisca di beni che nulla avevano a che vedere con i crimini informatici (stampanti, segreterie telefoniche, audioregistratori, audiocassette) suggeriva un'analoga ignoranza e una non necessaria invasione della privacy e dei diritti personali. In un caso famoso e, come vedremo, gravido di conseguenze, le autorità federali avevano confiscato da Steve Jackson Games, la casa editrice dove lavorava The Mentor, un file di testo contenente le regole di un gioco di ruolo a tema fantascientifico, scambiandolo per un manuale di crimine informatico. Questi episodi contribuivano alla percezione, da parte delle comunità hacker, di un mondo esterno del tutto incapace di comprendere il «cyberspazio» e di certo non qualificato per scriverne le regole[160].

Le comunità giovanili hacker non erano le uniche ad avere questa impressione. L'intensificarsi dei raid contro gli hackers e Operation Sun Devil in particolare attirarono l'attenzione dell'industria informatica e della controcultura californiana, comunità che non di rado si sovrapponevano. Molti dei protagonisti della Silicon Valley degli anni Ottanta e Novanta si definivano d'altra parte hacker e guardavano con preoccupazione all'evidente incompetenza di media e legislatori in materia di crimine informatico e gestione dei networks. Lo stesso poteva dirsi dei tecno-libertari e dei reduci della controcultura statunitense, che avevano per primi riflettuto sul possibile potere liberatorio e democratizzante dei computer e dei networks: alcune delle comunità avevano spostato la propria sociabilità dalle comuni rurali alle reti informatiche[161] e avevano un interesse immediato nella difesa della libertà

di parola e di associazione nel cyberspazio. Sebbene nessuno dei due gruppi fosse stato direttamente toccato da Operation Sun Devil, gli eventi dei primi anni Novanta li spinsero a unire le forze per creare un'organizzazione per la difesa dei diritti online, la Electronic Frontier Foundation (EFF).

John Perry Barlow, una delle figure centrali del tecno-libertarianesimo statunitense, della controcultura degli anni Settanta e della prima cultura digitale, ricorda l'incontro virtuale con due membri di LoD, Phiber Optik (Mark Abene) e Acid Phreak (Elias Ladopoulos), come una rivelazione. In occasione di un forum online organizzato da «Harper's Magazine» Barlow ebbe l'occasione di notare quanto i giovani hackers si distanziassero dall'idea di «tecno-hippy» che era stata popolare nei circoli controculturali: questi «cyberpunks» erano «irritabili, volgari, immaturi, immorali». Su di loro pesava inoltre una narrazione mediatica che li associava alla manomissione delle carte di credito e dei telefoni e persino alla collaborazione con la mafia. Il punto più basso del rapporto tra techno-hippies e hackers si raggiungeva quando la discussione virava sulla sicurezza dei sistemi informatici. I due membri della Legion of Doom erano del parere che qualsiasi sistema che non fosse adeguatamente protetto meritasse di essere violato. Barlow faceva notare che, per principio e per fiducia nel prossimo, non chiudeva a chiave nemmeno la porta di casa sua. Acid Phreak suggerì allora di comunicare a tutti il proprio indirizzo di casa e Barlow, provocato, lo fece. Il giorno dopo Phiber Optik pubblicava sul forum l'intero storico delle transazioni bancarie di Barlow, facendo intendere (falsamente) di poterlo modificare a proprio piacimento. L'effetto su Barlow, che pure partiva estremamente ben disposto verso gli hackers, fu profondo: «la mia valutazione delle capacità di magia nera del cracker era simile a una reverenza superstiziosa. Erano streghe digitali che stavano per zombificare la mia anima economica».

La sua reazione avrebbe avuto importanti conseguenze sul seguito della cultura digitale: invece di abbandonare la conversazione Barlow scrisse una email a Phiber, sfidandolo a trovare il suo numero di telefono e a chiamarlo. L'hacker lo fece senza alcuna difficoltà:

> In questa conversazione e nelle altre che sono seguite ho incontrato un ragazzino di 18

anni intelligente, civile e sorprendentemente animato da principi etici che sembrava, e continua a sembrare, ben poco pericoloso per chiunque, uomini o dati. [...] I personaggi terrificanti che Optik e Acid interpretavano sullo schermo erano un esempio amplificato dai media di una forma di adattamento umano che avevo già incontrato: si diventa quello che si è creduti essere. Stavano semplicemente recitando quello che io e, soprattutto, i redattori di «Harper's» ci aspettavamo da loro. Come le lacrime televisive delle vittime dei disastri naturali, il loro ringhiare si adattava facilmente alla distribuzione di massa[162].

Grazie al rapporto con il mondo hacker Barlow si rese conto, allo scoppiare di Operation Sun Devil, delle implicazioni che le retate avevano per la libertà di parola online: confiscare interi servers perché su di essi erano presenti dei files ottenuti illegalmente equivaleva a sequestrare un'intera casa perché un ospite vi aveva lasciato un videoregistratore rubato. D'altra parte, anche la posizione delle forze dell'ordine era a suo modo di vedere comprensibile: «Per loro tutta questa roba è come magia. Se stessi cercando di chiudere le attività di un covo di streghe probabilmente anche io sequestrerei tutto quello che c'è. Come distinguere una semplice scopa casalinga da un veicolo che poteva essere usato per scappare?»[163].

L'effettiva visita di un agente dell'FBI, che, nonostante la completa incomprensione dei fenomeni informatici su cui stava investigando, intendeva interrogarlo sulle sue connessioni con il mondo hacker, spinse Barlow a pubblicare le proprie riflessioni su The Well, il principale BBS della controcultura americana e, al tempo, uno dei più frequentati luoghi di incontro online. Qui furono lette da Mitch Kapor, imprenditore milionario e creatore di Lotus 1-2-3, uno dei primi software di fogli di calcolo per personal computer. Anche Kapor aveva ricevuto una visita dall'FBI per verificare le sue (inesistenti) relazioni con il crimine informatico. Nel giro di pochi giorni Kapor aveva messo in contatto Barlow, Acid e Optik con un importante studio legale newyorkese. Nell'arco di pochi mesi Kapor e Barlow avrebbero fondato con John Gilmore (attivista e dirigente di Sun Microsystems) la Electronic Frontier Foundation.

L'iniziativa trovò, secondo il racconto di Barlow, un deciso sostegno da parte di svariate figure eminenti della Silicon Valley (tra queste Steve Wozniak, cofondatore di Apple, e Stewart Brand, fondatore di The Well

e in seguito della rivista «Wired»), preoccupate che le azioni unilaterali del governo potessero inibire lo sviluppo dell'innovazione e dell'industria informatica[164]. Ben più ostile, almeno inizialmente, la reazione dei media nazionali, che vedevano sfidata la narrazione dell'hacker come minaccia e bandito della frontiera digitale e interpretavano la fondazione come un semplice fondo di difesa legale per gli hackers[165].

Nell'immediato la EFF si sarebbe in effetti impegnata a dimostrare che Operation Sun Devil e le retate ad essa collegate «limitavano la libertà di parola, sequestravano illecitamente equipaggiamento e dati, usavano una forza sproporzionata e in generale erano condotte in maniera arbitraria, oppressiva e non costituzionale». Tale obiettivo fu raggiunto già entro la fine del 1990, con l'assoluzione di quasi tutti i coinvolti nei raid dei due anni precedenti. Nel 1994 il caso Steve Jackson Games v. United States Secret Service avrebbe stabilito che i fornitori di servizi di comunicazione elettronica dovevano avere le stesse protezioni garantite agli operatori telefonici e non potevano essere ritenuti responsabili di un eventuale uso illegale dei servizi[166]. A seguito di altre sentenze analoghe, dal 1996 la sezione 230 del *Communications Decency Act* avrebbe decretato che «nessun fornitore o utente di un servizio informatico interattivo sarà trattato come l'editore o il responsabile di qualsiasi informazione fornita da terzi», aprendo di fatto la porta all'esistenza degli odierni social networks e dei siti di streaming, liberandoli dalla responsabilità legale sui contenuti immessi dagli utenti. In tempi recenti le «ventisei parole che hanno creato Internet»[167] sono state ripetutamente messe in discussione alla luce del ruolo che le piattaforme social hanno avuto nella diffusione di false notizie e materiale illegale[168].

Nel più lungo periodo la EFF si sarebbe dedicata al lobbying, al finanziamento della ricerca sulle libertà digitali e al sostegno economico delle cause legali che avrebbero deciso le regole della convivenza online: dalla possibilità di usare e rendere pubblici software di crittografia alle pene massime comminabili per l'infrazione dei termini di servizio di un sito web, dall'uso eccessivamente restrittivo delle leggi sul copyright online al libero accesso a documenti storici e governativi[169].

Le avventure di Kevin Mitnick, ingegnere sociale

Nessun hacker incarnò l'immagine mediatica del bandito digitale come Kevin Mitnick, nome d'arte The Condor. Per quasi vent'anni il suo nome apparve sulla stampa generalista e su quella specializzata come sinonimo dell'hacker criminale, capace di manipolare le forze oscure della tecnologia digitale a proprio vantaggio. Le sue avventure sono state oggetto di innumerevoli articoli, di libri e documentari, oltre che di non poche leggende ed esagerazioni, sia nei media sia tra i circoli hacker. Durante il suo terzo processo, nel 1988, l'accusa sostenne che Mitnick era capace di lanciare un attacco nucleare semplicemente fischiando in un telefono pubblico[170]. Ancora nel 1999 la CNN gli imputava di aver tenuto sotto controllo le comunicazioni interne dell'FBI, di essere entrato nei sistemi informatici del NORAD e di essere stato per questo l'ispirazione di *WarGames*[171]. In realtà, dato che tali accuse non furono mai formalizzate in un processo, è più probabile il contrario: il film ispirò la narrazione mediatica e, conseguentemente, le paure delle forze dell'ordine e dei giudici.

Nonostante in fase processuale si opponesse con forza a questa caratterizzazione, nei suoi momenti di libertà The Condor interpretò il ruolo di bandito digitale con perizia ed entusiasmo. Al contrario di Morris, della Legion of Doom e della maggior parte degli hackers del periodo, Mitnick era pienamente consapevole, come si evince dalla sua autobiografia, della gravità penale delle sue azioni. Ma questo non lo fermò dal compierle e, ancora più significativamente, dal parlarne, sia con i propri pari sia, in alcune occasioni, con giornalisti e specialisti di sicurezza informatica.

Eppure la principale abilità di Kevin Mitnick non era la sua indubitabile conoscenza dei sistemi informatici e telefonici. Il campo in cui eccelleva era l'ingegneria sociale. Per social engineering si intende, come si è accennato nel capitolo 2, la capacità di manipolare la società come un hacker manipola un sistema tecnologico: con creatività, abilità, astuzia, e con il fine di ottenere risultati che il sistema (sociale e umano) non prevedeva[172]. L'organizzazione di un'azienda, per esempio, non doveva permettere che la password del suo sistema informatico fosse comunicata via telefono a uno sconosciuto. Ma se dall'altra parte della cornetta vi era

una persona che conosceva minutamente il funzionamento dell'azienda, ivi compresi il gergo informale o dettagli tecnici del tutto sconosciuti al pubblico, era possibile che la sua pretesa di ottenere la password fosse soddisfatta. Se il tecnico era di fretta e se l'«ingegnere sociale» sapeva suonare abbastanza autorevole e spazientito, era ancora più probabile che il primo fosse disposto a fare uno strappo alla regola, comunicando la password via telefono. Come si è visto, le pubblicazioni phreak fin dagli anni Settanta davano consigli su come risultare credibili in diversi contesti e su tutte le conoscenze (dei rapporti gerarchici in una corporation, dei rapporti di genere nel servizio clienti delle compagnie telefoniche, del gergo utilizzato in una particolare azienda...) e le pratiche che erano necessarie per il successo di un social engineer. Ma nulla poteva sostituire una diligente ricerca sul «sistema sociale» che si intendeva colpire. Tra le tecniche di ricerca più diffuse tra gli hackers vi era il «dumpster diving», la pratica di rovistare nella spazzatura di una corporation o di una compagnia telefonica in cerca di documenti scartati che contenessero informazioni se non riservate, abbastanza private da dare credibilità alla messa in scena del social engineering.

Un buon esempio della pratica è fornito dallo stesso Mitnick nella sua autobiografia. L'obiettivo era quello di avere accesso al servizio di comunicazione interna di una compagnia telefonica. Per prima cosa l'hacker si procurava con altri mezzi informazioni interne ma non necessariamente segrete, come il nome e il ruolo degli impiegati delle aziende o i loro numeri di telefono. Poi effettuava una chiamata all'ufficio business della compagnia telefonica. Kevin si presentava come Jake Roberts, del Non-Pub Bureau (nome usato informalmente all'interno dell'azienda per indicare l'ufficio informazioni interno) e chiedeva di parlare con un supervisore. Raggiunto il supervisore gli chiedeva se aveva ricevuto la comunicazione che il Non-Pub Bureau aveva cambiato il proprio numero.

– No, non l'abbiamo ricevuta.
– Dovreste usare il numero 213 687-9962 [un numero inventato da Mitnick].
– No, usiamo il numero 213 320-0055.

In questo modo Mitnick otteneva il numero di un ufficio che avrebbe dovuto essere accessibile solo ai dipendenti. Ma per avere accesso non

bastava conoscere il numero, era necessario essere su una lista di impiegati autorizzati. Kevin dunque chiamava un impiegato che sapeva essere su quella lista. Presentandosi come Tom Hansen (un altro impiegato reale), comunicava al malcapitato che la lista degli autorizzati al Non-Pub Bureau era in fase di aggiornamento. «Ha ancora bisogno di avere accesso al numero privato?». Ovviamente l'impiegato rispondeva affermativamente. L'hacker allora gli chiedeva di dettargli il suo nome e numero interno. In questo modo Mitnick aveva in mano sia il numero riservato del Non-Pub Bureau sia il nome e il codice di un impiegato autorizzato ad usarlo. Dato che il numero era accessibile solo ai tecnici, gli operatori erano inclini a fornire qualsiasi informazione riservata senza ulteriori verifiche dell'identità del chiamante. «Più la sfida è difficile, più alta è l'adrenalina! Questo trucco ha funzionato per anni e molto probabilmente funziona ancora oggi!»[173]. Quasi tutte le imprese di Mitnick, nonostante l'aura di onnipotenza tecnica che i media gli conferirono, facevano leva più sugli elementi umani dei sistemi tecnologici che non su codici di programmazione o software maligno.

Ma l'ingegneria sociale può esercitarsi anche faccia a faccia. All'inizio degli anni Ottanta Kevin riusciva a intrufolarsi nella sede di Los Angeles della compagnia telefonica Pacific Bell. L'atto era visto come una naturale continuazione delle sue attività «virtuali»: «Dato che stavamo già facendo del phone phreaking, entrare nella compagnia telefonica era il massimo hack [...] per noi era il miglior parco giochi». Fermato da una guardia, Kevin si fingeva un impiegato in visita da San Diego e invitava la guardia a contattare il suo supervisore. La guardia la chiamava e Kevin se la faceva passare. Mentre la donna cercava di capire con chi stesse parlando («Chi sei? Ti conosco?») Kevin fingeva a favore della guardia: «Judy, scusami tanto, stavo facendo vedere a un mio amico l'ufficio di smistamento chiamate e ho lasciato il tesserino di riconoscimento in macchina [...] Ho una riunione con Jim lunedì alle undici se vuoi unirti. È confermato il pranzo di martedì, no?». Mentre la malcapitata Judy cercava di capire cosa stesse succedendo e prima che la guardia potesse prendere in mano il telefono Mitnick riattaccava.

In quell'occasione la truffa funzionò, ma poco dopo, nel 1981, un tentativo analogo (il furto di manuali di Pacific Bell, ottenuti fingendosi

un tecnico) costò a Mitnick, ancora minorenne, la prima condanna. Altre condanne seguiranno nel 1983, nel 1987 e nel 1988, per penetrazione illecita in sistemi informatici universitari e aziendali con l'obiettivo di copiare illecitamente linee di codice. Mitnick non comprometteva i files sui computer penetrati e non vendeva le informazioni in essi contenute. L'hacker sostiene, nei suoi scritti autobiografici, di aver commesso questi atti illegali solo per mettersi alla prova e soddisfare la propria curiosità, in piena continuità con l'etica hacker[174]. La lettura di questi stessi scritti suggerisce che ugualmente importanti erano la competizione con chi tentava di catturarlo e la notorietà che fin dalla seconda metà degli anni Ottanta il nome di Kevin Mitnick stava guadagnando.

La notorietà è però un'arma a doppio taglio. A partire dall'arresto del 1988 il nome di Mitnick cominciava ad apparire sulle pagine della stampa nazionale, che lo presentava come uno stregone semi-onnipotente. Questa aura di minaccia è riflessa nel trattamento giudiziario dell'hacker, allora venticinquenne: fu in quell'occasione che l'accusa arrivò a suggerire al giudice che, se gli fosse stato dato accesso al telefono, Mitnick sarebbe stato capace di lanciare un attacco nucleare fischiando nella cornetta. Difficile dire quanto l'affermazione fosse seria o quanto credito le sia stato dato dal giudice, ma è un fatto che, dopo essersi visto negare la cauzione, Mitnick passò in isolamento otto dei dodici mesi della sua condanna. L'uso del telefono gli era permesso solo sotto la supervisione di una guardia. La ragione era, secondo un articolo di «Time Magazine» del 1989, che «mettere un telefono nelle mani di Mitnick equivaleva a dare una pistola a un sicario»[175].

Appena uscito di prigione il giovane tornò immediatamente all'hacking e all'ingegneria sociale, con una caparbietà che suggerisce una vera e propria dipendenza (riconosciuta peraltro dal tribunale, che gli impose un periodo in un centro di riabilitazione), soprattutto in considerazione dello stato in cui l'attività aveva ridotto la sua vita fino ad allora e della speciale attenzione di cui era oggetto da parte dell'opinione pubblica e degli specialisti di sicurezza informatica. Per il suo talento, le sue imprese, e per il fatto di essere stato tra i primi hackers a vedere l'interno di una cella, Mitnick stava infatti diventando una celebrità nel mondo hacker. Nel 1991, inoltre, era stato oggetto di un popolare libro,

Cyberpunk di Katie Hafner e John Markoff, che descriveva le sue peripezie fino ad allora e lo metteva a fianco di altri hackers famosi, come Robert Morris, e di spie tedesche che negli anni Ottanta avevano venduto segreti informatici al KGB[176]. Il capitolo dedicato a Mitnick si intitolava *The Dark-Side Hacker*, un riferimento al film *Star Wars* (il lato oscuro della Forza) che era già stato usato dalla stampa nazionale per definirlo almeno dal 1988 e che segnala la consapevolezza, da parte dei media, di una risemantizzazione in senso negativo della pratica.

Con l'inizio degli anni Novanta le avventure di Kevin Mitnick assunsero un carattere spiccatamente romanzesco. Nel 1992, temendo giustamente un nuovo arresto per aver violato i termini della libertà vigilata, Mitnick fece perdere le proprie tracce. Attraverso una serie di elaborate truffe telefoniche (alla motorizzazione, alla Social Security Administration, al Dipartimento dei Trasporti, a Microsoft) assunse l'identità di Eric Weiss, con tanto di patente, certificato di nascita e numero di sicurezza sociale originali. Eric Weiss era il vero nome di Harry Houdini.

Eric/Kevin decise di trasferirsi a Denver e, appena arrivato, si procurò, di nuovo tramite social engineering, il numero utilizzato dagli operatori telefonici locali per controllare le linee. In questo modo sarebbe stato in grado di sapere se qualcuno lo stava controllando. Come in tanti altri casi il trucco non richiedeva altro che la capacità di recitare e una conoscenza specifica e approfondita del gergo e della struttura gerarchica della compagnia telefonica:

> Bastava procurarsi il numero dell'ufficio centrale che si occupava dello smistamento delle telefonate dell'area di cui volevo prendere controllo e dire qualcosa del tipo: «Ciao, sono Jimmy del Dipartimento di Ingegneria. Come va?». Poi avrei continuato con «Qual è il numero del VDU?» – il termine gergale per Visual Display Unit, che dava accesso remoto al centro di smistamento [...]
>
> Solitamente il tipo mi avrebbe concesso il numero telefonico per accedere al suo ufficio centrale. Ma se un tecnico voleva sfidarmi conoscevo abbastanza del sistema da improvvisare una scusa plausibile al volo. Poteva essere qualcosa del tipo: «Stiamo creando un nuovo sistema di chiamata e stiamo inserendo tutti i numeri nel nostro software di gestione telefonica»[177].

Nel 1993 Mitnick riusciva, usando in ugual misura tecniche di hacking, phreaking e social engineering, a penetrare i computer di Sun

Microsystems (sviluppatori responsabili per la piattaforma Java) e di svariati produttori di telefoni cellulari (Motorola, Nokia, Novatel, Qualcomm), impossessandosi del loro software. Si noti che, come Mitnick non si stancherà di ripetere nel corso dei propri processi e come verrà riconosciuto anche dai suoi detrattori, nessuno degli hacks da lui effettuati comportava un guadagno personale. Il codice sottratto era semplicemente messo da parte, spesso per non essere più utilizzato. L'obiettivo era invariabilmente duplice: impossessarsi di software da esibire «come trofeo» e ampliare le proprie possibilità di accesso ai sistemi informatici, venendo a conoscenza di bugs o informazioni riservate che rendessero più efficaci l'hacking o l'ingegneria sociale.

Il 4 luglio 1994 il «New York Times» pubblicava in prima pagina un articolo di John Markoff dal titolo *Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit*. Il pezzo combinava falsità («Un teenager ha usato un computer e un modem per penetrare nel computer del North American Aerospace Defense Command, prefigurando il film del 1983 *WarGames*»), illazioni presentate come fatti (il sospetto che Mitnick fosse in grado di spiare le telefonate dell'FBI o che avesse prodotto un falso comunicato stampa per screditare una banca che gli aveva negato un lavoro), stereotipi («È un nerd sovrappeso, ma quando è dietro una tastiera si sente onnipotente») e svariate esagerazioni sul pericolo rappresentato dall'hacker («Se diventi il suo bersaglio può rendere la tua vita miserabile»). Correttamente Markoff riconosceva che Mitnick non sembrava essere mosso da motivi economici, lasciando all'immaginazione del lettore il movente di crimini dati per certi, ma mai provati in tribunale. Non è chiaro cosa potesse aver spinto Markoff, probabilmente insieme a Levy il più importante giornalista specializzato in informatica della sua generazione, a pubblicare un pezzo così scarsamente documentato. Parte della spiegazione è nel sensazionalismo che caratterizzava larga parte della copertura mediatica dell'hacking del periodo: l'unico crimine provato citato nell'articolo era la violazione dei termini della libertà vigilata, un atto che, da solo, non avrebbe potuto garantire la prima pagina del «New York Times»[178].

Certo è che, se Mitnick non era «il più ricercato del cyberspazio» prima dell'articolo, lo sarebbe diventato dopo. L'attenzione mediatica verso

l'hacker si sarebbe intensificata nell'anno successivo e con essa le pressioni sulle autorità federali per la sua cattura. Braccato dalle forze dell'ordine, Mitnick fu costretto a cambiare tre identità e tre città in due anni, vivendo di espedienti e ai limiti della sussistenza.

Ma di nuovo questo non lo fece desistere dall'hacking. In collaborazione con un hacker israeliano, usando una tecnica teorizzata per primo da Robert Morris (il così detto IP spoofing, che permetteva di aggirare i controlli di sicurezza sulle connessioni tra computer simulando una connessione legittima), Mitnick entrò nei servers privati di un esperto di sicurezza informatica, Tsutomu Shimomura. L'azione era giustificata, secondo Mitnick, semplicemente dal fatto che Shimomura aveva fama, nei circoli hacker e della sicurezza, di essere tanto abile quanto tracotante: «Abbiamo deciso di colpire il suo ego per avvicinarlo alla realtà – solo perché potevamo». Il successo dell'operazione forniva a Mitnick l'accesso alle mail tra Shimomura e Markoff e a diversi software di sicurezza informatica. Soprattutto gli concedeva, per alcune ore, l'ebbrezza che cercava: «Incredibile! Che estasi! Deve essere quell'estasi che prova un ragazzino quando raggiunge l'ultimo livello di un videogioco con cui ha lottato per mesi. O come raggiungere la cima del Monte Everest».

Ma questo momento di gioia sarebbe costato caro. La violazione ai danni di Shimomura era raccontata, circa un mese dopo, da Markoff sul «New York Times»[179]. Gli amministratori di The Well scoprirono sui propri servers un pacchetto con tutti i files di Shimomura. Mitnick aveva accesso ai loro computer e li stava usando come storage personale.

All'inizio del 1995 Shimomura iniziava a collaborare con l'FBI e grazie alla loro autorità riusciva a farsi dare dai provider di Internet la possibilità di monitorare il traffico in tempo reale. Quando Mitnick entrò di nuovo in The Well e poi nel server di posta del «New York Times» le autorità furono in grado di rintracciare il collegamento come proveniente da Raleigh, South Carolina. Immediatamente Markoff (il cui ruolo ufficiale nell'investigazione rimane poco chiaro e sarà oggetto di critiche da parte della comunità hacker) e Shimomura si recarono a Raleigh, dove furono accolti da un team composto da agenti federali e addetti alla sicurezza delle compagnie telefoniche. I due ascoltarono la registrazione di una conversazione telefonica tra Emmanuel Goldstein, il caporedattore di

«2600», e una persona che Markoff riconobbe come Mitnick. Di lì a poco l'hacker fu arrestato. Aveva così inizio una vicenda giudiziaria ed extragiudiziaria che avrebbe definito l'evoluzione dell'hacking negli anni a venire.

Free Kevin

La parabola biografica di Kevin Mitnick è importante per almeno due motivi. Il primo è che essa offre uno scorcio sulle motivazioni che hanno spinto tanti giovani che non pensavano a sé stessi come criminali a dedicarsi all'hacking. Il caso di Kevin Mitnick è certamente straordinario, reso estremo dalle sue capacità di social engineering, dalla sua probabile dipendenza dall'hacking e dall'attenzione ricevuta. Ma dai suoi scritti si desume che le motivazioni dei suoi crimini non erano dissimili da quelle che animavano tanti giovani hackers del periodo: la sfida nei confronti delle macchine, delle autorità e dei propri pari; la curiosità e la volontà di provare la propria intelligenza; la ricerca della celebrità all'interno di una comunità di nicchia, dispersa nella rete ma tenuta insieme dai BBS e da pubblicazioni specializzate; la competitività tra hackers e la sfida nei confronti degli specialisti di sicurezza informatica.

Tutto questo era spesso incomprensibile per chi non facesse parte dell'underground elettronico. Il fatto che si potesse avere la possibilità di trarre enormi profitti dall'hacking, ma si decidesse di non farlo, pur esponendosi ai medesimi rischi legali di un criminale comune, era, per l'opinione pubblica e per le autorità, semplicemente irrazionale. Al momento dell'arresto, Mitnick era in possesso, secondo l'accusa, di circa 20.000 numeri di carte di credito che avrebbero potuto essere usate a piacimento. Mai l'uso di queste carte gli fu contestato: l'unico vantaggio materiale che egli ebbe dal suo hacking e dalle sue truffe furono chiamate gratuite, per un totale che non poteva aver superato le poche migliaia di dollari. La copertura giornalistica si trovava così, paradossalmente, a evidenziare la potenziale minaccia rappresentata dagli hackers, senza poter citare danni significativi effettivamente causati. Le autorità giudiziarie, per parte loro, non avevano mezzi adeguati per punire crimini potenziali, ma, spinti dall'opinione pubblica e forse anche

dall'umiliazione della lunga latitanza di Mitnick, non potevano limitarsi ai pochi anni di prigione che i crimini effettivamente commessi avrebbero comportato. Questo determinò un trattamento giudiziario altamente inusuale e decisamente duro, di cui parleremo a breve.

Il secondo motivo di interesse del caso Mitnick è il suo effetto sul significato della parola hacker. La copertura mediatica fu di un'intensità mai vista prima e probabilmente dopo; il resoconto dei giornalisti era a volte estremamente ostile e spesso, come si è visto, sensazionalistico. Sulle pagine dei giornali e nelle interviste rilasciate alla televisione l'hacker diventava l'incarnazione delle paure legate alla rivoluzione digitale. Imprese tecniche estremamente complesse e dallo scarso appeal mediatico venivano semplificate al punto da apparire come magia; la loro minaccia, proprio perché indefinita, toccava tutto e tutti. Se i 414s e Morris erano ragazzi prodigio, Mitnick, il fuggitivo, era un «dark-side hacker» capace di colpire chiunque.

Proprio questa caratterizzazione, tuttavia, contribuì a un cambiamento del significato della pratica all'interno delle stesse comunità hacker. Come vedremo il trattamento giudiziario di Mitnick spinse le comunità hacker a riconoscersi come un gruppo di interesse e, in alcuni casi, a cercare di spiegare al mondo esterno sé stesse e i propri valori.

La più importante accusa mossa a Mitnick riguardava il furto ai danni di Sun Microsystem di un sistema operativo, Solaris. I danni erano calcolati da Sun in ben 80 milioni di dollari. Mitnick non aveva mai venduto o reso pubblico il software, lo aveva semplicemente copiato su servers da lui controllati. Il calcolo, evidentemente esagerato, era basato sulla somma pagata da Sun a AT&T per acquisire i diritti di Solaris. Come scrive efficacemente Mitnick, sarebbe equivalso a punire chi avesse rubato una lattina di Coca-Cola come se si fosse impossessato della formula della bevanda. Nonostante fosse per legge obbligata a riportare eventuali perdite nel proprio bilancio annuale, Sun non aveva peraltro menzionato gli 80 milioni di dollari ai propri azionisti al momento dell'hack di Mitnick. E poco dopo il sistema operativo sarebbe stato messo in vendita per soli 100 dollari a copia. Il danno effettivo era, per l'azienda, praticamente inesistente.

Questo sollevava questioni legali ed etiche centrali al nuovo ecosistema digitale. L'interesse delle autorità era quello di dare all'hacker più famoso

del momento una punizione esemplare, per scoraggiare azioni analoghe e provare all'opinione pubblica e ai media che i nuovi pericoli del «cyberspazio» erano sotto controllo. Ma come punire in maniera severa un crimine senza vittime? Il *Computer Abuse Act*, nella sua revisione del 1986, prevedeva il crimine di «alterare, danneggiare o distruggere» files altrui, cosa che Mitnick non aveva fatto. Il copiare software, senza venderlo, sottrarlo al legittimo proprietario o negare la sua possibilità di profitto poteva essere interpretato come crimine (l'accesso era dopotutto illecito), ma il processo prometteva di essere incerto e prolungato, la pena ben più mite della punizione esemplare che l'FBI, le compagnie telefoniche e parte della stampa si aspettavano. Il ruolo di Markoff e Shimomura – due civili – nell'arresto dell'hacker era criticato da più parti[180]. Il rischio era un nuovo nulla di fatto, analogo all'assoluzione di Knight Lightning e The Prophet in occasione di Operation Sun Devil[181].

La strategia contro Mitnick fu dunque extraprocessuale. All'hacker fu negata l'udienza per fissare la cauzione: avrebbe dovuto attendere in prigione l'inizio del processo. La data di quest'ultimo non fu fissata che quattro anni dopo l'arresto, solo dopo che Mitnick aveva accettato di patteggiare.

Questo trattamento avrebbe innescato una campagna di sensibilizzazione e protesta guidata da «2600. The Hacker Quarterly». Appena dopo l'arresto la rivista ammoniva in copertina che Mitnick era solo il «primo a cadere» e che, se la criminalizzazione dell'hacking fosse continuata, altri (e in particolare i lettori di «2600») lo avrebbero seguito. A rafforzare il messaggio lo stesso numero pubblicava il codice sorgente di uno dei files trovati in possesso illecito di Mitnick, dimostrazione di quanto fosse facile procurarselo[182]. Ma è nel 1997 che la campagna cominciò a decollare. Il fatto che l'hacker fosse costretto in prigione senza un regolare processo era visto come prova dell'atteggiamento vendicativo delle autorità giudiziarie e federali e di una criminalizzazione che aveva più a vedere con le esigenze dei media e le paure del pubblico che non con l'effettiva gravità dell'hacking[183]: se anche un assassino poteva almeno chiedere di pagare la cauzione in attesa del processo, perché l'udienza era stata negata a Mitnick? La campagna di sensibilizzazione faceva uso del semplice slogan «Free Kevin», senza

ulteriore spiegazione, stampato su magliette e adesivi e scritto su siti hacker o di cui gli hackers avevano preso illecitamente possesso. La mancanza di contestualizzazione, unita all'onnipresenza dello slogan, doveva suscitare curiosità e domande. Principale bersaglio della protesta erano i media e la loro caratterizzazione dell'hacking come atto esclusivamente criminale. Il libro che Markoff e Shimomura avevano pubblicato poco dopo l'arresto di Mitnick era oggetto di particolare sdegno, soprattutto dopo che la casa di produzione Miramax aveva deciso di trarne un film e alcuni hackers erano riusciti a procurarsi il copione. Tutti i partecipanti alla convention HOPE[184] del 1996 si presentarono vestendo maschere di Kevin Mitnick[185]. Nel 1997 il sito di Yahoo News fu modificato da un gruppo hacker che minacciava, in puro stile yippie, il rilascio di un virus che avrebbe messo in ginocchio Internet se Mitnick non fosse stato liberato[186]. L'anno successivo un gruppo chiamato «Hacking for Girlies» (Hacking per ragazzine) avrebbe preso controllo del sito del «New York Times», pubblicando immagini oscene e provocazioni a Markoff per il suo ruolo nella vicenda Mitnick[187].

È probabile che la campagna abbia avuto scarso peso nella vicenda giudiziaria di Mitnick. Nel 1999 l'hacker decideva infine di accettare un patteggiamento che lo condannava a 46 mesi di carcere (in buona parte già scontati) e ad una multa irrisoria. Significativo il fatto che la condanna prevedesse anche due anni di libertà vigilata durante i quali a Mitnick era vietato usare qualsiasi tipo di computer. Dal momento che buona parte delle tecnologie della vita quotidiana contenevano processori, la decisione sollevava dubbi su cosa potesse essere legalmente definito computer ed evidenziava, una volta di più, le difficoltà della legislazione ad adattarsi al cambiamento tecnologico. Per gli hackers questo supplemento di pena, ben più vessatorio di quanto i giudici potessero immaginare, confermava l'atteggiamento ostile e l'analfabetismo tecnico delle autorità.

Il risultato della campagna era più evidente all'interno della comunità hacker ed ebbe in essa più importanti conseguenze[188]. Per la prima volta dal tempo degli Yippies una cultura tecnica tornava all'attivismo politico organizzato. La campagna «Free Kevin» avrebbe mostrato agli hackers che

la comunità poteva farsi carico di cause politiche e sociali (almeno sui temi – crimine informatico, libertà di parola e di accesso all'informazione, crittografia – che vedevano d'accordo la maggior parte dei praticanti) e che alcune forme di comunicazione politica, particolarmente congeniali alle comunità hacker, potevano avere un significativo successo nel nuovo ecosistema digitale. Questa lezione sarà raccolta dai gruppi hacktivisti di cui parleremo nel capitolo 7.

152 C. Sims, *Computer Failure Disrupts A.T.&T. Long Distance*, in «The New York Times», 16 gennaio 1990.

153 «Phrack», n. 31, file 5.

154 United States Attorney Office, Comunicato stampa, 9 maggio 1990, riportato in «Phrack», n. 31, file 5.

155 «Phrack», n. 31, file 10.

156 D.E. Denning, *The United States vs. Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking*, in «Communications of the ACM», 1991, 34, pp. 22-43.

157 *For Your Protection. For Your Own Good*, in «2600. The Hacker Quarterly», VII, 1990, 1, pp. 3-7 e 34-35.

158 Ivi, p. 34.

159 J.P. Barlow, *Crime and Puzzlement*, in «Electronic Frontier Foundation», 1990, https://web.archive.org/web/20210320162248/https://www.eff.org/pages/crime-and-puzzlement.

160 P.X. Nathan, *Secret Service On Trial*, in «2600. The Hacker Quarterly», X, 1993, 1, pp. 18-23. Per una discussione sulla percezione esagerata delle potenzialità criminali degli hacker alla fine del millennio si veda Taylor, *Hackers*, cit., pp. 1-11.

161 F. Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*, University of Chicago Press, Chicago 2008.

162 Barlow, *Crime and Puzzlement*, cit.

163 *Ibid.*

164 J.P. Barlow, *A Not Terribly Brief History of the Electronic Frontier Foundation*, in «Electronic Frontier Foundation», 8 novembre 1990, https://web.archive.org/web/20210320155147/https://www.eff.org/pages/not-terribly-brief-history-electronic-frontier-foundation.

165 *What is the EFF?*, in «2600. The Hacker Quarterly», VII, 1990, 2, p. 10.

166 *Steve Jackson Games, Inc. v. U.S. Secret Service*, No. 36 F.3d 457 (Court of

Appeals for the Fifth Circuit, 28 ottobre 1994).

167 J. Kosseff, *The Twenty-Six Words that Created the Internet*, Cornell University Press, Ithaca 2019.

168 T. Romm, E. Dwoskin, *Trump Signs Order that Could Punish Social Media Companies For How They Police Content, Drawing Criticism and Doubts of Legality*, in «The Washington Post», 28 maggio 2020; R. Learman, *Social Media Liability Law Is Likely To Be Reviewed under Biden*, in «The Washington Post», 18 gennaio 2021.

169 *Victories*, in «Electronic Frontier Foundation», https://web.archive.org/web/20220401230041/https://www.eff.org/victories.

170 K. Mitnick, W.L. Simon, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Little, Brown and Company, New York 2011.

171 J. Christensen, *The Trials of Kevin Mitnick*, in «cnn.com», 18 marzo 1999, https://web.archive.org/web/20210213214112/http://edition.cnn.com/SPECIALS/1999/mitnick.background/.

172 C. Hadnagy, *Social Engineering: The Science of Human Hacking*, Wiley, Indianapolis 2018.

173 Mitnick, Simon, *Ghost in the Wires*, cit., pp. 21-25.

174 K. Mitnick, *One Chapter: Kevin Mitnick's Story*, in «The Register», https://web.archive.org/web/20210621145001/https://www.theregister.com/2003/01/13/chapter_one_kevin_mitnicks_story/.

175 *Technology: Drop the Phone*, in «Time Magazine», 9 gennaio 1989, http://content.time.com/time/subscriber/article/0,33009,956685,00.html.

176 C. Stoll, *Cuckoo's Egg*, Pocket Books, New York 1989.

177 Mitnick, Simon, *Ghost in the Wires*, cit., p. 280.

178 J. Littman, *The Fugitive Game: Online with Kevin Mitnick*, Little, Brown and Company, Boston 1997, pp. 106-110.

179 J. Markoff, *Taking a Computer Crime to Heart*, in «The New York Times», 28 gennaio 1995.

180 Littman, *The Fugitive Game*, cit.

181 R. Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, in «Berkeley Technology Law Journal», XVIII, 2003, 3, pp. 909-944.

182 *The World v. Kevin Mitnick*, in «2600. The Hacker Quarterly», XII, 1995, 1, pp 4-5.

183 *Enough is Enough*, in «2600. The Hacker Quarterly», XIV, 1997, 1, pp. 4-5.

184 HOPE (Hackers on Planet Earth) è una delle principali conventions hacker, organizzata da «2600» dal 1994.

185 E. Goldstein, *Freedom Downtime*, in «2600. Films», 2001, https://www.youtube.com/watch?v=WN4fCK23Srk.

186 C. Woodford, *The Internet: A Historical Encyclopedia*, vol. 2, ABC-CLIO,

Santa Barbara 2005, p. 184.
187 A. Harmon, *Hacker Group Commandeers The New York Times Web Site*, in «The New York Times», 14 settembre 1998.
188 Coleman, Golub, *Hacker Practice*, cit.

5.
Free Software, 1983-1991

Una doppia rivoluzione, 1975-1981

Alla metà degli anni Settanta l'industria informatica entrava in un periodo di impetuoso cambiamento. Il *time-sharing*, la possibilità per diversi utenti di accedere tramite economici terminali alla potenza di calcolo di uno stesso computer, aveva dato agli specialisti un primo assaggio di cosa significasse avere un computer per il proprio uso personale. La necessità di formare un numero sempre crescente di studenti aveva portato allo sviluppo di linguaggi di programmazione più semplici e accessibili, in particolare BASIC. Il microprocessore (inventato da Ted Hoff e Federico Faggin per Intel nel 1971) aveva ridotto drasticamente i costi di produzione dell'hardware e le sue dimensioni.

I tempi erano maturi perché il computer uscisse dai laboratori industriali e universitari e diventasse l'oggetto domestico che conosciamo oggi. Nel 1975 «Popular Electronics», una rivista di divulgazione tecno-scientifica rivolta ad hobbisti e radioamatori, prometteva «il primo minicomputer al mondo che può competere con i modelli commerciali»[189]. Per soli 400 dollari i lettori potevano ordinare il kit di costruzione di quello che sarebbe stato ricordato come il primo personal computer della storia: l'Altair 8800. Le sue funzioni erano estremamente limitate, nel confronto sia con gli odierni PC sia con i computer, molto più costosi e ingombranti, che erano usati da istituzioni e aziende. L'assemblaggio richiedeva una saldatrice, molta perizia e una certa dose di fortuna, in mancanza di istruzioni dettagliate o assistenza tecnica dall'azienda produttrice. L'Altair non aveva schermo o tastiera: l'unico feedback visivo era fornito dai 36 leds del pannello frontale e l'unico modo per inserire istruzioni erano degli interruttori che, accesi o

spenti, rappresentavano gli uno e gli zero del codice binario. Ogni volta che la macchina era spenta perdeva tutti i dati. Anche l'utente che avesse portato a termine con successo i difficili processi di assemblaggio e programmazione avrebbe in ogni caso ottenuto, secondo lo storico Paul Ceruzzi, «poco più di una serie di luci lampeggianti sul pannello frontale»[190].

Eppure, nelle parole dello stesso Ceruzzi, l'uscita dell'Altair avrebbe dato inizio a un'«esplosione di energia e creatività nel mondo del computer che non ha quasi uguali nella storia»[191]. I motivi sono principalmente due. In primo luogo vi era la comunità di appassionati di tecnologia che gravitava intorno a pubblicazioni come «Popular Electronics». Giovani e giovanissimi, spesso estranei alla ricerca universitaria e appassionati di qualsiasi aspetto delle tecnologie elettroniche (dalla radio ai telefoni, ai calcolatori), gli hobbisti non solo garantirono un mercato per l'Altair, ma contribuirono in maniera decisiva a colmarne le lacune e ad ampliarne le funzionalità. Non pochi di questi appassionati pensavano a sé stessi come a hackers e si univano in associazioni come l'Homebrew Computer Club (Club del computer fatto in casa), il circolo californiano fondato nel marzo 1975 che vedeva tra i propri membri future figure chiave della Silicon Valley quali Steve Jobs e Steve Wozniak.

La difficoltà di costruzione e programmazione, lungi dall'essere un deterrente, diventava per questi hackers una sfida collettiva, al pari di quella affrontata dai radioamatori dell'ARRL prima della Grande Guerra (vedi cap. 1) o dai phreaks che tentavano di penetrare AUTOVON o il fortress phone (vedi cap. 2). La mancanza di assistenza tecnica era compensata dal piacere del processo di prova ed errore e, soprattutto, dalla possibilità di rivolgersi a una comunità di persone che avevano affrontato (e in alcuni casi superato) le stesse difficoltà e che si ritrovavano in fiere, associazioni e pubblicazioni dedicate.

Il secondo fattore che ha contribuito al successo di Altair è di natura tecnica. Il primo personal computer era espandibile grazie a connettori per schede interne (i *bus*, che sarebbero diventati uno standard dei PC)[192] e le sue specifiche erano di pubblico dominio. Questo significava che chiunque poteva commercializzare schede interne e periferiche che

ampliassero le poche funzioni cui la macchina poteva inizialmente assolvere e ne aumentassero la memoria e la capacità di calcolo. Dato che già esisteva una base di appassionati e che questi erano già avvezzi all'assemblaggio in prima persona della tecnologia, le espansioni dell'Altair ebbero un successo immediato. In capo a tre anni la macchina poteva essere collegata a una telescrivente con tastiera e a lettori di cassette magnetiche, di floppy disks e di carte perforate. La popolarità dell'Altair avrebbe portato alla commercializzazione di numerose imitazioni e, soprattutto, avrebbe dimostrato ad attori affermati e a imprenditori rampanti che esisteva un mercato per computer a basso prezzo e di limitate prestazioni. Nel 1976 Jobs e Wozniak fondavano la Apple computer e l'anno successivo mettevano in commercio Apple II. Nel 1981 usciva IBM PC. Entrambe le macchine furono presentate come oggetti quotidiani, alla portata di tutti. Entrambe mantenevano, almeno temporaneamente, l'espandibilità che aveva fatto il successo dell'Altair, aprendo le porte a un fiorente mercato di schede interne e periferiche prodotte da terze parti.

La rivoluzione della fine degli anni Settanta non riguardò solo l'hardware. Prima dell'Altair e dei personal computers non esisteva una vera e propria industria del software. Le aziende fornivano ai propri clienti, spesso corporations o uffici governativi, sia i computer sia i programmi che su di essi giravano. Questi ultimi erano, nella maggior parte dei casi, pensati per funzionare soltanto sulla macchina con la quale erano spediti. L'innovazione del software avveniva dunque in concomitanza con lo sviluppo di nuovo hardware o su richiesta diretta del cliente.

Questo quadro fu complicato, dalla metà degli anni Settanta, dall'avvento di UNIX, un sistema operativo che poteva girare su macchine diverse. Il software e il linguaggio con il quale era stato programmato (C) erano stati entrambi sviluppati da AT&T. I termini di un accordo del 1956 tra AT&T e il governo statunitense prevedevano però che l'azienda fondata da Graham Bell potesse mantenere il proprio monopolio di fatto sulle comunicazioni telefoniche nazionali solo a patto che non si impegnasse in altri settori, ivi compreso quello dell'informatica. UNIX era dunque distribuito gratuitamente o a prezzo di costo e il suo codice sorgente era a disposizione dei ricercatori per

essere studiato e modificato, un accidente storico che avrebbe portato alla sua eccezionale diffusione e alla sua longeva popolarità (il sistema operativo è ancora oggi alla base di MacOS e Linux). L'apertura del codice sorgente fece sì che la capacità di innovazione fosse trasferita in larga parte agli utenti finali, ricercatori e hackers universitari che sapevano apprezzare la flessibilità del sistema operativo e potevano cambiare e ampliare il software a seconda delle proprie esigenze. Nel 1977 l'Università di Berkeley arrivò a pubblicare una propria versione indipendente, Berkeley Software Distribution (BSD), che a sua volta sarebbe diventata il punto di partenza di altre varianti di UNIX[193].

UNIX e il linguaggio di programmazione C erano però troppo complessi per funzionare su Altair o sui personal computers della prima generazione. L'opportunità presentata da questa mancanza fu colta da due giovani di Seattle, Paul Allen e Bill Gates, che scrissero una versione modificata di BASIC (un linguaggio di programmazione relativamente semplice, inizialmente pensato per la didattica) che poteva girare sull'Altair. Nonostante BASIC fosse stato creato al Dartmouth College e fosse stato loro concesso gratuitamente, i due ne fecero il primo prodotto di una nuova azienda, «Micro-Soft», lo vendettero agli utenti Altair e difesero aggressivamente i propri diritti di autore. Gates e Allen furono i primi a riconoscere che, con la rivoluzione commerciale dell'hardware, un nuovo mercato si apriva per il software. Così facendo entrarono in rotta di collisione con la tradizione di libero scambio del codice e delle informazioni tecniche, propria sia degli hackers universitari sia degli hackers extrauniversitari e degli appassionati di elettronica.

Questo scontro fu inaugurato da una celebre lettera aperta del 1976, scritta da Gates e pubblicata sulla newsletter dell'Homebrew Computer Club, nella quale il fondatore di Microsoft (l'azienda avrebbe assunto l'attuale nome due anni dopo) denunciava il libero scambio di informazioni tecniche – una delle caratteristiche centrali delle culture hacker e di ogni cultura tecnica – come semplice «furto».

> Come la maggior parte degli hobbisti di certo sa, la maggior parte di voi ruba il software. Bisogna pagare per l'hardware, ma il software è qualcosa da condividere liberamente. [...] Chi può permettersi di lavorare per nulla? Quale appassionato può permettersi di spendere tre anni-uomo nella programmazione, nel trovare tutti i bugs,

nel documentare il prodotto e distribuirlo gratuitamente? [...] Quello che state facendo è, per dirla francamente, un furto. [...]

Niente mi farebbe più piacere che poter assumere dieci programmatori e riempire di software di qualità il mercato degli appassionati[194].

Quest'ultimo desiderio sarebbe stato presto esaudito e superato (anche se la qualità del software sarebbe stata spesso contestata dagli hackers): nel 1981 Microsoft avrebbe firmato un accordo con IBM che avrebbe assicurato il successo di MS-DOS, primo sistema operativo sviluppato dall'azienda di Seattle e diretto precursore di Windows.

Ma sono le domande retoriche nella citazione precedente che hanno suscitato le maggiori ire nelle comunità hacker e di appassionati e, in retrospettiva, la maggiore ironia. Con la sua lettera Gates dava simbolicamente i natali all'industria del software. Ma inevitabilmente apriva anche la strada alla «pirateria» informatica e, cosa probabilmente meno scontata, poneva le basi per i movimenti Free Software ed Open Source, di cui ci occuperemo nei prossimi paragrafi.

GNU is not UNIX

La commercializzazione del software inaugurata da Microsoft non toccava direttamente i centri universitari. Come detto, questi si affidavano in larga parte a UNIX, un sistema operativo che era per molti versi il software ideale dell'hacker universitario: gratuito e dalla sorgente aperta, era nato come un insieme di strumenti per la gestione e lo scambio dei files e si era evoluto in un sistema operativo completo grazie all'intervento di innumerevoli utenti, che si scambiavano, in maniera del tutto gratuita, innovazioni e informazioni. La sua elegante gestione dei files in rete e la possibilità di adattarlo a macchine, periferiche e protocolli diversi lo resero uno dei pilastri di ARPANET, il progenitore del moderno Internet. Le prime newsletters online, come USENET, erano accessibili solo tramite UNIX. Sfortunatamente la disponibilità del codice sorgente e la grande flessibilità rendevano il sistema operativo particolarmente vulnerabile ai virus, come Robert Morris avrebbe dimostrato al mondo nel 1988 (vedi cap. 3).

Ma gli interessi della neonata industria del software si affacciarono presto anche nei circoli universitari. Il taglio ai fondi militari dedicati alla

ricerca informatica dopo la fine della guerra in Vietnam spingeva gli istituti di ricerca e i singoli ricercatori a trovare nuove fonti di finanziamento. Il libero scambio di informazioni tra pari, proprio non solo delle comunità hacker ma dell'intera comunità universitaria, era sempre più spesso ostacolato dai contratti di riservatezza firmati dai programmatori con aziende private; alcune periferiche e alcuni programmi cominciavano ad essere spediti senza il codice sorgente – e dunque senza la possibilità di essere modificati o scambiati. Altri software erano distribuiti con delle «time bombs» che ne impedivano il funzionamento gratuito dopo un certo periodo di tempo. Nel 1983, infine, AT&T acquisì la possibilità di esercitare il proprio copyright su UNIX, un preludio dello smantellamento del suo monopolio sulla telefonia che sarebbe stato portato a termine nel 1984. I giorni del sistema operativo hacker sembravano finiti.

Fu l'insieme di questi fattori, uniti a uno spirito idealistico, a una notoria cocciutaggine e a una produttività fuori dal comune, che spinse un brillante hacker dell'AI Lab del Massachusetts Institute of Technology, Richard Stallman, a tentare di sviluppare un sistema operativo libero da copyright e con esso una comunità di appassionati che si sarebbe occupata di ampliarlo, diffonderlo e mantenerlo gratuitamente.

Nel 1983 Stallman scriveva un messaggio dal titolo *Free UNIX!*[195] su una newsletter USENET dedicata al sistema operativo:

> Sto per scrivere un sistema software compatibile con UNIX che si chiamerà GNU (per GNU Non è UNIX [*GNU's Not UNIX*]) e lo darò gratuitamente a chiunque sia in grado di usarlo. Ogni contributo in tempo, denaro, programmi ed equipaggiamento sarà molto importante. [...]
>
> Quella che considero la regola d'oro è che se mi piace un programma devo condividerlo con altra gente a cui piace. Non posso in buona coscienza firmare un accordo di riservatezza o un contratto di licenza sul software.
>
> Per poter continuare a usare i computer senza violare i miei principi ho deciso di mettere insieme un gruppo di software libero [*free*] abbastanza nutrito da poter fare a meno di tutto il software che non sia libero[196].

L'annuncio era in piena continuità con la cultura hacker universitaria, dal nome del nuovo sistema operativo (un ironico e paradossale acronimo ricorsivo) alla volontà di migliorare il software attraverso uno sforzo

collettivo, al baldanzoso individualismo (Stallman chiede aiuto, ma si dice pronto a procedere anche da solo in un compito – la scrittura di un intero sistema operativo – che in passato aveva occupato interi team per anni e anni). Già in questo messaggio iniziale era insita un'evoluzione del discorso hacker sull'accesso all'informazione: l'utilizzo del software era presentato non come un modo per soddisfare la propria curiosità e non solo come un mezzo per raggiungere una maggiore efficienza, ma come diritto fondamentale proprio di una comunità, garantito semplicemente dalla capacità di farne uso.

Il messaggio del 1983 venne ampliato nei suoi scopi e meglio specificato nei suoi significati politici due anni dopo, in un articolo pubblicato da Stallman (che nel frattempo si era dimesso dal MIT per dedicarsi a tempo pieno al progetto GNU) su una rivista di settore[197]. Il «manifesto GNU» suonava a tratti come una risposta punto per punto alla lettera agli hobbisti di nove anni prima. Laddove Gates denunciava i danni che la pirateria portava all'innovazione, Stallman sosteneva che il libero scambio permetteva un più efficiente coordinamento degli sforzi, evitando la programmazione di software dalle identiche funzioni su sistemi diversi. Laddove Gates vedeva nella condivisione un furto ai danni dei programmatori, Stallman la considerava un servizio alla società: come l'aria, il software doveva essere a disposizione di tutti. La creatività e il servizio al prossimo potevano e dovevano essere un compenso sufficiente.

Ciò nonostante, scriveva Stallman, i programmatori potevano continuare a vivere del proprio lavoro: quello che l'etica del software libero proibiva non era la vendita in sé, ma le restrizioni all'esplorazione e alla modifica del codice sorgente una volta che il software fosse stato eventualmente venduto. Il concetto sarà più volte ribadito, soprattutto in seguito alle polemiche seguite all'emergere del movimento Open Source (vedi *infra*):

> «Free software» significa software che rispetta le libertà dell'utente e della comunità. Genericamente, significa che *gli utenti hanno la libertà di far girare, copiare, distribuire, studiare, cambiare e migliorare il software* [corsivo nell'originale]. Perciò il «free software» è una questione di libertà, non di prezzo. Per capire il concetto occorre pensare a «free» come nella parola «freedom» [libertà], non come in «free beer» [birra gratis]. A volte lo chiamiamo «libre software» prendendo a prestito la parola francese o spagnola per «free»,

per chiarire che non vogliamo dire che il software deve essere gratis. Potresti dover pagare per avere delle copie di un free software, oppure potresti averle ottenute gratuitamente. A prescindere da come le hai ottenute, avrai sempre la possibilità di copiare e cambiare il software e persino di venderlo[198].

I programmatori sarebbero stati pagati dalle università e il software libero avrebbe creato nuove occasioni di impiego, sotto forma di didattica, consulenze e assistenza. In maniera più utopistica, il manifesto proponeva in conclusione una tassa sulla vendita dell'hardware che sarebbe dovuta andare a finanziare lo sviluppo del software.

Per coordinare gli sforzi di sviluppo e, soprattutto, di diffusione della filosofia del software libero Stallman fondava nello stesso anno la Free Software Foundation (FSF), con l'obiettivo di «proteggere la filosofia free software», promuovere il software libero e l'idea stessa di cosa significasse «libertà» in ambiente digitale.

È difficile sopravvalutare quanto questa interpretazione collettivista del libertarianesimo hacker debba alla particolare personalità ed esperienza di Richard Stallman. Entrato nell'AI Lab nel 1971, ad appena 18 anni, Stallman aveva idealizzato la comunità di hacker che, al MIT, si scambiava liberamente i frutti del proprio lavoro e collettivamente migliorava il sistema operativo usato nel laboratorio:

Ogniqualvolta un'altra università o una compagnia voleva trasferire e usare un programma eravamo contenti di farglielo fare. Se vedevi qualcuno usare un software non conosciuto e interessante era sempre possibile chiedere di vedere il codice sorgente, leggerlo, cambiarlo o cannibalizzarne delle parti per fare un nuovo programma.

Nel 1981 il MIT decise di aggiornare le proprie macchine, passando a un sistema operativo proprietario: per usarlo gli hackers del MIT dovevano firmare un accordo di riservatezza. Per Stallman questo non significava soltanto un ostacolo al suo lavoro o un problema morale: la comunità della quale si sentiva parte era direttamente minacciata.

[L'obbligo di sottoscrivere un accordo di riservatezza] significava che il primo passo per poter usare un computer era la promessa di non aiutare il tuo prossimo. Una comunità di cooperazione era proibita. La regola imposta dai proprietari del software era: «Se condividi con il tuo prossimo sei un pirata. Se vuoi dei cambiamenti [ai programmi] devi supplicarci perché li facciamo»[199].

A prima vista la figura di RMS (così Stallman era conosciuto nelle comunità hacker) sembrava conformarsi allo stereotipo del nerd: sovrappeso, dai vestiti *casual* e stropicciati, dai capelli lunghi e la barba mal tenuta. Ma il suo comportamento non aveva nulla a che vedere con l'idea dell'hacker introverso e socialmente inetto: abile oratore e teatrante, Stallman evocava nel suo pubblico, anche grazie alla rigidità delle sue convinzioni e ad una certa ostentata saccenza, l'idea di un predicatore religioso[200]. Le sue azioni dimostrative erano diventate leggendarie nei circoli hacker universitari. RMS rifiutava di mettere passwords di sicurezza nei sistemi da lui gestiti al MIT e aveva messo in piedi una vera e propria campagna interna per l'abbandono di ogni tipo di ostacolo all'accesso ai sistemi informatici. In maniera ancora più grave, almeno dal punto di vista del Dipartimento della Difesa, le credenziali istituzionali di Stallman per l'accesso ad ARPANET erano periodicamente pubblicate nelle newsletters hacker, in un momento in cui la rete era appannaggio esclusivo di ricercatori autorizzati e personale militare[201].

La fama non era legata soltanto al suo attivismo: ugualmente importante era la qualità del suo lavoro. Stallman era il creatore di EMACS, un editor di testo tra i più avanzati del suo tempo. Particolarità del software era la facilità con la quale poteva essere personalizzato ed esteso dai suoi utenti: in cambio della distribuzione gratuita Stallman chiedeva che le modifiche gli fossero comunicate, in modo che potessero essere eventualmente integrate in una versione successiva dell'editor, andando a beneficio dell'intera comunità. Così l'hacker divenne il coordinatore di una «EMACS Commune», un gruppo di programmatori che, in maniera gratuita e lavorando attraverso la rete, curavano l'evoluzione del software.

La straordinaria capacità di lavoro di Stallman è stata immortalata in un episodio raccontato dal bestseller di Steven Levy, *Hackers*. Nel 1981 Symbolics, un'azienda privata, aveva cominciato a commercializzare le proprie innovazioni a un sistema operativo che era stato sviluppato gratuitamente dall'AI Lab. Per tutta risposta Stallman aveva preso a replicare tutte le nuove funzioni vendute da Symbolics, programmandole da zero e diffondendole gratuitamente, sobbarcandosi il lavoro che normalmente sarebbe stato affidato a un intero team. Sebbene l'appellativo di «ultimo vero hacker», attribuitogli in virtù di queste

imprese da Levy[202], sia certamente un'esagerazione e l'episodio sia difficile da verificare, la statura di RMS tra gli hackers e i programmatori era innegabile. Se c'era qualcuno che, ai loro occhi, poteva guidare un gruppo di hackers verso la creazione di un sistema operativo «libero» quella persona era Richard Matthew Stallman. Eppure questo sistema operativo non vide mai la luce, perlomeno non nella forma o con i significati politici previsti da RMS.

Linux is not GNU

I software sviluppati dalla FSF erano compatibili con qualsiasi sistema UNIX. Ciò aiutava la gestione del progetto (chiunque poteva sviluppare un software GNU, perché poteva testarlo sulla propria macchina UNIX) ed era fondamentale per assicurare la sua rilevanza negli anni: i singoli software creati dalla FSF erano immediatamente utilizzabili, senza la necessità di aspettare che l'intero sistema operativo fosse completato. Ma questo creava anche un dilemma: come assicurarsi che il codice distribuito gratuitamente non fosse incluso in programmi non liberi e distribuito come software proprietario? La legislazione sul copyright, negli Stati Uniti estesa al software dal 1974, non offriva alcuna flessibilità: il software o era proprietario o era nel pubblico dominio – e in quest'ultimo caso chiunque avrebbe potuto usarlo a piacimento, anche per fini commerciali e restringendo l'accesso alle linee di codice che erano «nate libere» dal lavoro di hackers e volontari.

La soluzione escogitata da Stallman altro non è che un hack, operato non sulla tecnologia, ma sulla legge[203]. Come si ricorderà, la definizione di hack che abbiamo finora usato ne situa l'essenza nella capacità di ottenere da una tecnologia prestazioni e funzioni non previste dal suo designer originale. Laddove le normali licenze servono a limitare gli usi che si possono fare di un software, la GNU General Public License (GPL), scritta da Stallman e dal giurista Eben Moglen nel febbraio 1989, serve a «limitare i limiti» imponibili all'uso di un programma. La licenza (oggi nella sua terza versione)[204] garantisce la possibilità di copiare, modificare e distribuire il codice a patto che la stessa licenza sia applicata anche all'interezza del nuovo programma nel quale il codice è inserito.

In questo modo l'inclusione di codice protetto da GPL all'interno di un

software rende quell'intero software libero di essere letto, copiato, modificato. Se qualcuno usa quel software in un altro contesto (ad esempio in un nuovo sistema operativo) anche quel nuovo prodotto dovrà essere necessariamente «libero» nella sua interezza. Le licenze GPL, che Stallman ha chiamato ironicamente «copyleft», hanno un carattere virale: si moltiplicano insieme al software che accompagnano senza bisogno di una dichiarazione esplicita dell'autore e, soprattutto, trasformano il software proprietario in software libero[205].

Nel caso la GPL non sia rispettata e il codice protetto sia incluso all'interno di programmi «chiusi», il codice in questione torna sotto la protezione del diritto d'autore e chi lo abbia usato impropriamente può essere denunciato per infrazione dei diritti di proprietà intellettuale. La Free Software Foundation usa insomma la legge del copyright esistente piegandola ai propri fini, per proteggere non l'esclusività dei diritti ma la loro condivisione[206].

Questo ebbe conseguenze profonde, sia all'interno delle comunità hacker sia al loro esterno. In primo luogo le licenze copyleft e il loro successo hanno messo, inaspettatamente, la conoscenza e il dibattito sulle leggi del diritto d'autore al centro delle comunità hacker. L'esperienza dello GNU Project, protetto dall'ingegnoso scudo della GPL, aveva provato che, a scapito delle previsioni di Gates, software funzionante e comunità ben organizzate potevano svilupparsi attorno al lavoro volontario, sostenuti dall'economia della reputazione che è parte fondamentale di tutte le culture hacker. Le licenze copyleft furono oggetto di attacchi violenti da parte di alti rappresentanti della compagnia, che vedevano nel loro carattere virale una minaccia non solo al loro modello commerciale, ma all'intero sistema economico basato sulla proprietà intellettuale[207].

In retrospettiva, è possibile affermare che i programmi non furono la più grande innovazione prodotta dalla Free Software Foundation o il suo più importante contributo al mondo dell'informatica o alla società moderna. A poco più di dieci anni dall'uscita della prima licenza copyleft un gruppo di accademici sarà ispirato dalla GPL nella scrittura di una serie di licenze che facessero uso del suo meccanismo «virale» e della sua inversione creativa delle regole del copyright per diffondere una

conoscenza «libera» che non si limitasse al mondo del software[208]. Le licenze Creative Commons[209], oggi usate su ogni tipo di prodotto intellettuale, dai romanzi ai film, dalle t-shirts alle voci di Wikipedia, sono uno dei tanti modi in cui la cultura hacker ha influenzato e influenza la società contemporanea.

Il lato software delle attività della Fondazione si rivelò meno di successo di quello legislativo. Ci vollero circa cinque anni perché il progetto GNU riuscisse a sviluppare una versione di EMACS, un compiler, un assembler[210], un'interfaccia grafica e altri elementi fondamentali di un sistema operativo. All'inizio degli anni Novanta tutto quello che mancava era un kernel, il software che gestisce le funzioni di base del sistema, il movimento dei dati e il processore. Lo sviluppo di questo cruciale codice si era rivelato più difficile del previsto: la FSF aveva intrapreso diverse prove che si erano rivelate altrettanti vicoli ciechi e la mancanza di quest'ultimo pezzo del puzzle, o di un piano credibile di sviluppo, cominciava a creare agitazione nella comunità dei programmatori volontari.

La soluzione sarebbe emersa dall'altra parte del mondo. All'inizio degli anni Novanta, in Finlandia, un giovane hacker stava cercando il modo di connettere il proprio computer di casa al sistema UNIX del Dipartimento di Informatica dell'Università di Helsinki, di cui era studente. Ne aveva tutti i diritti, ma il suo computer casalingo era un personal computer basato, come quasi tutti i compatibili IBM, su un processore Intel. UNIX, anche nella versione rivista da GNU, prevedeva processori e macchine ben più potenti, perlopiù possedute da professionisti e istituzioni.

Linus Torvalds decise dunque di cominciare a sviluppare una versione di UNIX che potesse girare sul proprio modesto computer. Nell'agosto 1991 Torvalds scriveva un messaggio su una newsletter dedicata a Minix, una versione di UNIX semplificata e pensata per la didattica, dalla quale l'hacker era partito per sviluppare il proprio sistema:

> Ciao a tutti, là fuori, utenti di minix –
>
> Sto creando un sistema operativo gratuito (è solo un hobby, non sarà grande e professionale come GNU) per 386 (o 486) cloni AT[211] [...] Vorrei feedback su cosa alla

gente piace/non piace in minix, perché il mio OS [sistema operativo] gli assomiglia in qualche modo[212].

Dalle risposte che Torvalds diede agli interessati[213] è possibile capire che la parentesi nella citazione precedente non era falsa modestia: il giovane hacker stava davvero soltanto cercando di creare una versione limitata di UNIX che potesse girare sul suo computer personale e connettersi all'esterno, come sfida e probabilmente come modo per mettersi in contatto e in vista nella comunità di appassionati. Ovviamente anche questa versione ridotta non sarebbe stata possibile senza l'accesso gratuito a software di qualità liberamente usabile prodotto negli anni da Stallman e dalla sua associazione, in particolare il compiler. Torvalds e i programmatori che presto lo avrebbero accompagnato dovevano «soltanto» scrivere il kernel che ancora mancava al progetto GNU[214] e far sì che questo dialogasse con macchine meno sofisticate e più diffuse rispetto a quelle su cui lavoravano i volontari della Free Software Foundation.

Quest'ultimo elemento fu una delle chiavi del successo del sistema operativo che, già dalla fine del 1991, avrebbe assunto il nome di Linux. Il messaggio di Torvalds trovava orecchie attente in un pubblico di programmatori che non sempre avevano accesso ai computer universitari e avevano tutto l'interesse ad usare una versione di UNIX sul proprio personal computer. Il bacino di persone che potevano aiutare un progetto del genere era dunque molto più ampio rispetto a quello inizialmente disponibile per Stallman. Altra scelta di successo fu la modalità di distribuzione adottata: in luogo di diffondere singoli software funzionanti e lasciare per ultimo il codice che avrebbe legato il tutto in un sistema operativo, Torvalds decise di rilasciare, a soli pochi mesi dal primo messaggio, un sistema operativo a malapena funzionante e «praticamente inutile», ma che poteva essere testato e migliorato direttamente da altri utenti[215].

L'impresa, così, non rimase un hobby a lungo. In pochi mesi la comunità di Linux contava centinaia di persone, che inviavano non solo commenti e soluzioni a bugs, ma anche nuove funzionalità. Stupito e affascinato da questa popolarità, Torvalds recuperò, inconsapevolmente, l'onorata tradizione ham delle QSL cards (vedi cap. 1), chiedendo a chi

usava Linux di inviargli una cartolina: ben presto gli arrivarono ringraziamenti, saluti e offerte di collaborazione da tutto il mondo.

La popolarità portò però anche i primi dilemmi. Torvalds non aveva intenzione di vendere il software. Ma, proprio come era successo vent'anni prima con Altair Basic, gli utenti avevano presto cominciato a distribuirlo e venderlo autonomamente. Era possibile che qualcuno trasformasse quanto era stato scritto fino ad allora in un software proprietario e che la comunità informale guidata dall'hacker finlandese perdesse il controllo dell'evoluzione del software. Torvalds prese dunque la cruciale decisione di proteggere il proprio kernel con la licenza GPL creata da Stallman, con effetti duraturi sia su Linux sia sulla licenza stessa. Il sistema operativo avrebbe visto la propria distribuzione gratuita garantita nel tempo e avrebbe così conosciuto, negli anni successivi, un successo e una diffusione senza pari. Nel 1999, a meno di dieci anni dal debutto, Torvalds poteva a buona ragione vantare «milioni di utenti, migliaia di sviluppatori e un mercato in crescita»[216]. Oggi quasi ognuno di noi usa Linux giornalmente, spesso senza saperlo. Il suo kernel è alla base di Android, il sistema operativo per cellulari più diffuso al mondo, e circa la metà dei siti web che visitiamo sono ospitati su servers Apache, un software Open Source che nasce su Linux. Nel 2013 il sistema operativo di Torvalds è stato adottato ufficialmente dalla NASA[217] e nel 2021 è atterrato su Marte, installato sul mini elicottero *Ingenuity*[218].

La GPL, grazie anche al suo carattere virale, si sarebbe nutrita di questo successo, arrivando ad essere applicata a molti software sviluppati per Linux. È estremamente probabile che, senza il successo anche mediatico del movimento Open Source (vedi capitolo successivo) e del suo modello produttivo, l'ethos delle licenze free non si sarebbe esteso ad altri campi del sapere.

Le differenze tra Stallman e Torvalds furono però da subito evidenti, nonostante l'ammirazione e quasi deferenza, almeno inizialmente, del secondo verso il primo. Assente era, nelle azioni dell'hacker finlandese, qualsiasi rivendicazione politica: la creazione di Linux era spiegata con il divertimento e l'esplorazione dei sistemi informatici (classici motivatori delle culture hacker) e con la volontà individuale di avere funzioni che i software commercializzati non fornivano. La GPL, definita da Torvalds

«un brillante dispositivo», non era adottata per difendere un'idea di comunità o la libertà di condivisione della conoscenza:

> Al contrario di tanti fanatici hardcore della GPL, che pensano che ogni innovazione software debba essere donata all'universo sotto la general public license, io credo che debba essere il diritto dell'inventore individuale decidere cosa fare della propria invenzione[219].

Le differenze non si limitavano peraltro alle sole interpretazioni etico-politiche della licenza. Il successo di Linux toglieva il terreno sotto i piedi al progetto GNU: il sistema operativo «free», che era l'ultimo obiettivo della Free Software Foundation, già esisteva, ma era free come in «free beer», non free come in «freedom». La GPL proteggeva infatti il kernel, ma non impediva che si potessero sviluppare software proprietari e «chiusi» con esso compatibili. Dalla metà degli anni Novanta in poi la Free Software Foundation si sarebbe concentrata sul lobbying e sull'applicazione della licenza GPL, mettendo in secondo piano lo sviluppo di software originali. Particolarmente irritante, dal comprensibile punto di vista di Stallman, era il fatto che l'intero sistema operativo venisse ad essere conosciuto come Linux, a scapito del fatto che la maggior parte del software appartenesse originariamente al progetto GNU. Le insistenze della Free Software Foundation perché il sistema fosse chiamato GNU/Linux sono perlopiù cadute nel vuoto: nella tecnologia come nel lessico, la facilità d'uso ha avuto la meglio sulla correttezza formale.

Per la cultura hacker nel suo complesso l'introduzione di Linux ebbe due conseguenze principali. In primo luogo, Linux forniva agli hackers extrauniversitari un «campo giochi» da esplorare a proprio piacimento, senza timore di infrangere la legge. Non tutti scelsero questa strada, ma la libertà insita nel nuovo sistema operativo è, insieme all'orgoglio di contribuire a un progetto globale e universalmente conosciuto, uno dei motivi della partecipazione hacker allo sviluppo di Linux e di software con esso compatibili.

La seconda conseguenza, probabilmente nel lungo periodo più importante, è che, nel fornire un campo di esplorazione legittima, Linux inaugurava un nuovo significato pubblico della parola «hacker», non più necessariamente legato all'anonimato e al sospetto di criminalità. Le

conseguenze di questo cambiamento saranno esplorate nei prossimi due capitoli.

189 «Popular Electronics», VII, 1975, 1, copertina.

190 P. Ceruzzi, *A History of Modern Computing*, The MIT Press, Cambridge (Mass.) 2003, p. 230.

191 *Ibid.*

192 Un bus è uno slot nella scheda madre nel quale è possibile inserire schede che aumentano le capacità del computer, come una scheda grafica o una scheda audio.

193 M.K. McKusick, *Twenty Years of Berkeley Unix. From AT&T-Owned to Freely Redistributable*, in *Open Sources: Voices from the Open Source Revolution*, a cura di C. DiBona, S. Ockman e M. Stone, O'Reilly Media, Sebastopol (CA) 1999, pp. 31-46.

194 B. Gates, *An Open Letter to Hobbyists*, 3 febbraio 1976, https://web.archive.org/web/20220311025916/https://www.digibarn.com/collections/newsletters/homebrew/V2_01/homebrew_V2_01_p2.jpg.

195 Il titolo può essere interpretato come «Liberiamo UNIX/UNIX libero» o «UNIX gratuito». Il duplice significato di «free» sarà un costante argomento di discussione del movimento Free Software e la causa di non poche ambiguità sui suoi obiettivi.

196 R. Stallman, *Free UNIX!*, in «Net.Unix-Wizards», 27 settembre 1983, https://web.archive.org/web/20220331223722/https://www.gnu.org/gnu/initial-announcement.en.html.

197 R. Stallman, *Realizable Fantasies: The GNU Manifesto*, in «Dr. Dobb's Journal», X, 1985, 3, pp. 30-34.

198 *What Is Free Software?*, in «GNU Operating System», https://web.archive.org/web/20220404115415/http://www.gnu.org/philosophy/free-sw.en.html.

199 R. Stallman, *The GNU Project*, in *Free Software, Free Society: Selected Essays of Richard M. Stallman*, a cura di J. Gay, Free Software Foundation, Boston 2002, pp. 17-32.

200 S. Williams, *Free As In Freedom: Richard Stallman's Crusade for Free Software*, O'Reilly Media, Sebastopol (CA) 2002.

201 Levy, *Hackers*, cit., pp. 439-440.

202 Ivi, p. 437.

203 L. Lessig, *Code and Other Laws of Cyberspace v. 2.0*, Basic Books, New York 2006.

204 *GNU General Public License*, in «GNU Operating System»,

https://web.archive.org/web/20220404064050/http://www.gnu.org/licenses/gpl-3.0.html.

205 Ceruzzi, *A History of Modern Computing*, cit., p. 340.

206 L. Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World*, Random House, New York 2001, pp. 52-61 (trad. it. *Il futuro delle idee*, Feltrinelli, Milano 2006).

207 C. Mundie, *The Commercial Software Model. Prepared Text of Remarks by Craig Mundie, Microsoft Senior Vice President*, in «microsoft.com», 3 maggio 2001, https://web.archive.org/web/20050621082004/http://www.microsoft.com/presspass/exec/craig/05-03sharedsource.mspx.

208 Lessig, *Code and Other Laws*, cit., p. 199.

209 *Creative Commons Italia*, https://web.archive.org/web/20220403061359/https://creativecommons.it/chapterIT/.

210 Compiler e assembler sono i software che traducono il linguaggio di programmazione (comprensibile all'utente) in un linguaggio binario «comprensibile» alla macchina.

211 Per *AT clones* Torvalds intende computer compatibili con gli IBM AT, la più diffusa linea di personal computers dalla metà degli anni Ottanta.

212 L. Torvalds, *LINUX's History*, in «Carnegie Mellon University, Computer Science», https://web.archive.org/web/20210502020655/https://www.cs.cmu.edu/~awb/linux.history.html.

213 *Ibid.*

214 *The Tanenbaum-Torvalds Debate*, in *Open Sources*, cit., pp. 221-252.

215 L. Torvalds, D. Diamond, *Just for Fun: The Story of an Accidental Revolutionary*, Harper Business, New York 2001, p. 88 (trad. it. *Rivoluzionario per caso. Come ho creato Linux (solo per divertirmi)*, Garzanti, Milano 2005).

216 L. Torvalds, *The Linux Edge*, in *Open Sources*, cit., pp. 101-112.

217 *Linux Foundation Training Prepares the International Space Station for Linux Migration*, in «Linux Foundation», https://web.archive.org/web/20220318080913/https://training.linuxfoundation.org/solutions/corporate-solutions/success-stories/linux-foundation-training-prepares-the-international-space-station-for-linux-migration/.

218 E. Ackerman, *How NASA Designed a Helicopter That Could Fly Autonomously on Mars*, in «IEEE Spectrum», 17 febbraio 2021, https://web.archive.org/web/20220318114625/https://spectrum.ieee.org/nasa-designed-perseverance-helicopter-rover-fly-autonomously-mars.

219 Torvalds, Diamond, *Just for Fun*, cit., p. 98.

6.
Open Source, 1993-2000

La rete e il bazar

Nel 1980 Tim Berners-Lee, un consulente informatico del Centro europeo per la ricerca nucleare (CERN), cominciò ad usare un programma da lui scritto, Enquire, per tenere traccia delle migliaia di software, hardware e studiosi che ruotavano attorno all'istituzione. Ogni oggetto nel database aveva un codice unico e poteva essere collegato a tutti gli altri tramite quello che Ted Nelson aveva definito, già negli anni Sessanta, un ipertesto[220]. In questo modo non era necessario gerarchizzare le informazioni a priori oppure ordinarle in categorie rigide: i collegamenti erano creati nell'atto stesso di inserire l'informazione, e il database poteva essere percorso secondo vie diverse, da un collegamento all'altro, a seconda degli specifici interessi dell'utente.

Ma le ambizioni di Berners-Lee andavano ben al di là della gestione di informazioni su un singolo network. «Immagina se tutte le informazioni presenti sui computer dappertutto fossero connesse [...] Immagina se potessi programmare il mio computer per fargli creare uno spazio dove qualsiasi cosa può essere connessa a qualsiasi altra cosa»[221]. Questa la visione che, nel 1989, animava la proposta di Berners-Lee per un sistema basato sull'ipertesto che collegasse tutte le informazioni sui computer del CERN e, potenzialmente, tutte le informazioni presenti in Internet. Negli anni successivi Berners-Lee e i suoi colleghi procedettero a creare un linguaggio di formattazione delle pagine che contenevano hyperlink (l'HTML), gli standard di comunicazione tra i diversi nodi della rete (HTTP), un sistema di registrazione delle singole pagine (URI) e, soprattutto, una rete di istituzioni perlopiù universitarie disposte a utilizzare tali strumenti e a condividere le proprie informazioni. In capo

a quindici anni questa idea avrebbe rivoluzionato le modalità con le quali l'umanità interagisce con i computer, dando vita al World Wide Web e trasformando Internet – prima di allora uno strumento per esperti di informatica – in una tecnologia di uso quotidiano.

Nel 1993 il web era diventato abbastanza diffuso da sollevare preoccupazioni in merito a chi lo doveva controllare: il CERN avrebbe cominciato a richiedere un pagamento per l'uso dell'HTML e per l'accesso al web, al pari di quanto era successo con altri sistemi di navigazione di Internet? Il timore che il servizio potesse diventare a pagamento o soggetto a limitazioni rischiava di inibire la partecipazione di nuovi utenti istituzionali e l'espansione della rete. Berners-Lee chiese dunque al CERN di assicurare la gratuità e apertura del codice HTML e dei protocolli web. La richiesta era senza dubbio ispirata dal lavoro di Stallman e degli hackers del free software (e difatti la prima proposta di Berners-Lee era di apporre al web la licenza GPL)[222], ma ben presto Berners-Lee si sarebbe spinto fino a caldeggiare il rilascio nel pubblico dominio. Il 30 aprile 1993, in una delle decisioni più importanti nella storia della tecnologia dell'età contemporanea, la dirigenza del CERN accoglieva la richiesta, concedendo a chiunque, fosse esso attore privato, istituzionale o commerciale, la possibilità di usare i protocolli web e il codice HTML, di aprire siti web, di cederli o venderli, senza alcun compenso al CERN o a Berners-Lee. Il web avrebbe così iniziato il percorso che da semplice modalità di navigazione delle informazioni in rete lo avrebbe portato ad essere percepito come sinonimo di Internet stessa.

In quegli stessi anni altri fenomeni contribuirono all'apertura di Internet alla popolazione generale. Il *National Information Infrastructure Act* del 1993 imponeva alla National Science Foundation, l'agenzia governativa statunitense che aveva il compito di gestire lo sviluppo di Internet, di aprire la rete agli interessi commerciali: aziende private potevano cominciare a vendere l'accesso a Internet ad altre aziende o a privati cittadini. Nel 1994 Netscape Navigator, uno dei primi browser web, annunciava che il suo software sarebbe stato rilasciato gratuitamente per utenti privati. Dal 1995 Microsoft includeva nel sistema operativo Windows il browser web Internet Explorer. Nel giro di appena due anni,

tra il 1993 e il 1995, il pubblico (o perlomeno quella porzione di pubblico, in costante crescita, che aveva accesso a una linea telefonica e a un personal computer) otteneva la possibilità di entrare in Internet, uno spazio informativo di facile navigazione (il web), un linguaggio estremamente semplice per creare pagine proprie (l'HTML) e software per visualizzare le informazioni (i browser) gratuiti o già inclusi nei sistemi operativi più diffusi.

Fu proprio in quel momento di crescita esponenziale dell'interconnessione digitale e di sfrenato entusiasmo per le possibilità dell'informatica e del nuovo mercato online che le prime versioni funzionanti di Linux cominciarono a circolare. La «cultura partecipativa» – la celebre espressione con la quale lo studioso di media Henry Jenkins ha definito le comunità che vivono grazie al contributo creativo dei propri membri a un'attività collettiva[223] – di Linux acquisiva caratteristiche che quella Free Software non aveva mai potuto avere: una portata globale e migliaia di membri che potevano applicarsi alla soluzione dei tanti problemi connessi con la creazione di un nuovo sistema operativo, dalla ricerca dei bugs alla creazione di software specializzato. Il modello di lavoro delle comunità hacker arrivava così a superare, in alcuni campi, quello degli ormai affermati colossi del software: laddove questi dovevano affidarsi ai propri stessi programmatori o a utenti pagati per il «beta testing», le innumerevoli comunità nate in rete attorno alla creazione di software potevano contare su migliaia di utenti/programmatori entusiasti di poter mettere alla prova le ultime funzionalità di un programma e, in caso di malfunzionamenti, di dimostrare la propria perizia proponendo soluzioni o miglioramenti.

La differenza tra i due modelli organizzativi e sociali è riassunta da Eric Raymond, hacker e maggiore ideologo del futuro movimento Open Source, nella metafora della «cattedrale» e del «bazar». Laddove il primo modello prevedeva un controllo centralizzato, una rigida divisione del lavoro e un approccio quasi reverenziale al software, il bazar vedeva apporti volontari e variegati, un brulicare caotico di iniziative individuali «dal quale un sistema coerente e stabile emerge apparentemente grazie a una serie di miracoli»[224]. La teorizzazione di Raymond presentava una versione particolarmente individualista dell'etica hacker. Laddove

Stallman evidenziava il valore sociale della condivisione e la capacità che un codice liberamente scambiato aveva di creare una comunità, Raymond partiva dalla premessa che ogni buon software nasceva dalla necessità di un programmatore di soddisfare un'esigenza personale ed estremamente pratica: la creazione di funzioni o capacità che il software prima non aveva. Il bazar che era Linux era così regolato da una sorta di mano invisibile, mossa dagli interessi dei suoi singoli contributori:

> Il mondo di Linux si comporta sotto molti aspetti come un libero mercato o un ecosistema, un insieme di agenti egoistici che tentano di massimizzare l'utilità, e nel processo crea un ordine spontaneo e che si autocorregge, più elaborato ed efficiente di quello che si sarebbe mai potuto ottenere con una pianificazione centralizzata [...] Possiamo vedere il metodo di Linus come un modo per creare un efficace mercato del compiacimento dell'ego: connettere strettamente l'egoismo dei singoli hackers a progetti così difficili da poter essere portati a termine solo tramite la cooperazione[225].

Una seconda caratteristica dei progetti inaugurati da Torvalds era la loro capacità di rendere gli utenti una parte attiva del processo di sviluppo del software. In luogo di attendere di avere una versione pienamente funzionante, come aveva fatto, con risultati fallimentari, la Free Software Foundation, il modello di Torvalds prevedeva di diffondere il software il più frequentemente possibile. Agli utenti – in questa prima fase spesso hackers e programmatori essi stessi – rimaneva il compito di scovare i bugs, individuare le funzioni più utili e segnalare problemi e possibili soluzioni alla comunità. La «legge di Linus», definita da Raymond, recita: «Se ci sono abbastanza occhi ogni bug è banale». I malfunzionamenti del software, che potevano occupare i «costruttori di cattedrali» per mesi, potevano essere risolti in tempi brevissimi grazie al «potere della folla» e all'esposizione del problema a migliaia di approcci e punti di vista differenti.

Non vi è dubbio che il «crowdsourcing», oggi applicato ad ogni tipo di iniziativa culturale, dalla creazione di archivi storici alla trascrizione di manoscritti antichi, alla scrittura di Wikipedia, sia una fondamentale innovazione nel processo di creazione della conoscenza nel XXI secolo. L'attribuzione dell'innovazione al solo Linus Torvalds è tuttavia un'esagerazione, legata più al successo di Linux e all'entusiasmo di Raymond che non alla reale storia del software o della rete. Come abbiamo visto, le intenzioni di Torvalds erano inizialmente quelle di

trovare aiuto per un progetto che egli stesso riteneva personale ed estremamente limitato. La vera differenza da progetti precedenti, primo fra tutti quello guidato da Stallman, sta nell'aver cominciato il proprio progetto collaborativo in un momento storico nel quale l'interconnessione informatica si stava diffondendo in maniera esponenziale al di fuori dei circoli accademici.

Indubbio merito di Torvalds, giustamente sottolineato da Raymond, è stato semmai quello di non cercare di esercitare un controllo eccessivamente stretto sulla comunità che si stava formando attorno a Linux. Questo permise alle comunità Open Source di definirsi come più egalitarie non solo rispetto alle grandi aziende del software, ma anche rispetto ai progetti accademici e, soprattutto, alla comunità GNU. Gli sviluppatori non dovevano passare un processo di verifica delle loro capacità per vedersi assegnato un determinato compito: essi si «autoselezionavano» a seconda delle parti del software che pensavano di poter migliorare, delle proprie capacità e dei propri interessi. Data la natura volontaria del lavoro e il grande numero di individui coinvolti era possibile «parallelizzare il debugging»: gruppi diversi lavoravano contemporaneamente e indipendentemente allo stesso problema e la soluzione più efficiente sarebbe poi stata inclusa nella nuova versione del software.

Un individuo o un gruppo erano necessari per dare vita al progetto e per dimostrare le sue potenzialità, ma passate le fasi iniziali il promotore diventava un semplice coordinatore e risolutore delle controversie, mentre il giudizio sulle singole innovazioni passava alla comunità, che le giudicava secondo le regole di un utopistico «libero mercato»: efficacia, utilità, interesse erano, almeno in teoria, gli unici metri di giudizio per l'accettazione o il rifiuto delle soluzioni proposte.

La vendetta degli hackers?

Il 1998 è l'anno durante il quale il modello di sviluppo inaugurato da Torvalds e teorizzato da Raymond acquisisce il nome «Open Source» e riceve una nuova e intensa attenzione mediatica a livello globale. In quell'anno, infatti, Netscape, all'epoca una delle principali aziende di software per la rete, annunciava che il codice del suo prodotto principale,

Netscape Navigator, sarebbe diventato pubblico e che la futura evoluzione del programma avrebbe seguito le modalità di sviluppo delineate in *The Cathedral and the Bazaar*[226]. Raymond vedeva in questa mossa una «vendetta degli hackers» dopo anni di marginalizzazione, stereotipizzazione e criminalizzazione nei media e nell'opinione pubblica: una compagnia inclusa in *Fortune 500* (la lista delle più lucrative aziende statunitensi redatta dalla rivista «Fortune») sceglieva un modello di sviluppo nato da una comunità di ragazzini e visionari[227]. È tuttavia probabile che la mossa, indubbiamente innovativa e coraggiosa, fosse dovuta non solo o non tanto alla fiducia nel modello, quanto alla pressione alla quale Netscape era sottoposta dalla crescente concorrenza nel mercato dei browsers, in particolare da parte di Microsoft.

Ciò nonostante la scelta di Netscape agì da catalizzatore per la nascita del movimento Open Source. Tra il febbraio e l'aprile 1998 lo stesso Raymond, l'influente editore di pubblicazioni informatiche Tim O'Reilly e altri protagonisti del nascente ecosistema dei programmi open source si sarebbero ritrovati per formalizzare la definizione di «sorgente aperta» e gli scopi del movimento che la sosteneva.

Non sorprende che il primo polo di autodefinizione fosse, in negativo, il *modus operandi* delle grandi aziende di hardware e software, caratterizzate da una rigida gerarchia, da una stretta pianificazione e, nell'opinione degli hackers, da una totale mancanza di creatività e rispetto per i propri utenti. L'ostilità era, nonostante l'atteggiamento sprezzante della dirigenza Microsoft[228], pienamente corrisposta. Dei documenti interni di Microsoft, ottenuti e resi pubblici da Raymond, dimostravano che l'azienda di Gates era al corrente del potenziale pericolo rappresentato dal software open source. Le due relazioni, ribattezzate da Raymond «Halloween documents»[229] perché pubblicate alla fine dell'ottobre 1998, rimarcavano la qualità e la complessità dei software sviluppati da comunità di volontari. La diffusione di Linux era aiutata dalla libera distribuzione in rete e dall'uso didattico che ne facevano scuole e università. L'adozione da parte delle aziende era incoraggiata dal fatto che, assumendo un programmatore, esse potevano modificare indipendentemente il software e assicurare la sua longevità anche nel caso in cui i primi sviluppatori avessero perso interesse al suo mantenimento.

La minaccia era particolarmente pressante nel campo dei servers, dove Apache – un web server open source – e Linux la facevano da padroni: i sistemi operativi montati su un server erano spesso gestiti da professionisti, che apprezzavano la flessibilità di Linux e non erano spaventati dalla sua complessità.

Ciò che più preoccupava gli analisti di Microsoft non era tuttavia la sfida tecnologica, ma quella posta dal modello economico e sociale dei progetti open source. I documenti ammettevano che i vantaggi dello «sviluppo e debugging parallelo», in cui diversi gruppi e individui cercavano indipendentemente la soluzione a un unico problema, non erano replicabili in un modello di lavoro salariato. Il mercato della gratificazione dell'ego e della reputazione che, ormai da decenni, teneva insieme le comunità hacker e ne garantiva la riproduzione non poteva essere imitato in un'azienda tradizionale:

> L'abilità del processo open source di riunire e sfruttare l'intelligenza collettiva di migliaia di individui in Internet è semplicemente incredibile. Ancora più importante: l'evangelizzazione del processo open source cresce in rapporto alla crescita di Internet molto più velocemente di quanto sembri fare la nostra evangelizzazione[230].

Per affrontare una concorrenza che non mirava al profitto, bensì alla gratificazione individuale, Microsoft doveva attaccare non il prodotto, ma l'ecosistema nel quale questo processo avveniva. I documenti raccomandavano di sviluppare e diffondere dei protocolli di comunicazione in rete proprietari che permettessero a Microsoft di esercitare una sorta di monopolio. In questo modo i prodotti open source si sarebbero visti negato l'accesso al mercato e la loro maggiore capacità di «evangelizzazione» sarebbe divenuta irrilevante. La minaccia, sentita come quasi irrisoria, al mercato dei consumatori era affrontabile accentuando l'integrazione dei prodotti Microsoft (ancora oggi la maggior parte dei software dell'azienda non funziona in ambiente Linux) e mantenendo Windows semplice da usare per utenti inesperti. Dopotutto, come prevede uno dei documenti, «l'orientamento hacker di Linux non soddisferà mai le esigenze di facilità d'uso dell'utente medio di un computer»[231].

La distanza dalle industrie software «tradizionali» era dunque scontata, riconosciuta da Microsoft e orgogliosamente rivendicata dagli hackers.

Ben più spinosa e urgente era, al momento della fondazione della Open Source Initiative (OSI), nel febbraio 1998, la questione di cosa separasse il movimento Open Source da quello del Free Software fondato da Stallman più di dieci anni prima.

Il problema non era primariamente tecnico o legale: come ha ammesso lo stesso Stallman[232], la maggior parte delle licenze open source rispettava la GPL ed ogni GPL era definibile come open source. La differenza era comunicativa ed etica. Se la «vendetta degli hackers» e la loro riabilitazione agli occhi della società dovevano essere complete, il modello Open Source e i suoi prodotti dovevano, secondo Raymond e l'OSI, essere adottati da grandi attori industriali. E per farlo occorreva una campagna di marketing e un «rebranding» che distanziasse le nuove licenze dall'aria di «comunismo» del Free Software e dal sospetto che queste volessero sovvertire le leggi della proprietà intellettuale. L'idea, immediatamente sostenuta dallo stesso Torvalds, era che

> Il nostro successo dopo Netscape sarebbe dipeso dal rimpiazzare gli stereotipi negativi della FSF con i nostri stereotipi positivi – storie pragmatiche, di maggiore affidabilità, costi minori e migliori funzionalità, dolci alle orecchie di manager e investitori[233].

Per farlo occorreva abbandonare il proselitismo dal basso della FSF, teso a far leva sull'etica e l'orgoglio di programmatori e hackers, e sostituirlo con «un'evangelizzazione top-down», pensata esplicitamente per suscitare l'interesse dei dirigenti d'azienda. Il successo di Linux doveva convincere i media a dare visibilità al movimento e le aziende della lista *Fortune 500* ad adottare, se non il processo del bazar, almeno i prodotti software che da esso scaturivano.

Stallman per parte sua rifiutava che un criterio esclusivamente pragmatico come quello dell'efficienza potesse essere al centro del movimento. Per l'hacker del MIT non era sufficiente che il software fosse potente, funzionante e aperto alla modifica da parte degli utenti. Esso doveva rispettare le libertà dei suoi utenti anche nelle sue funzioni:

> E se un software fosse progettato per mettere delle catene sui suoi utenti? Allora la sua potenza significherebbe che le catene sono più strette e la sua efficienza che esse sono più difficili da rimuovere. Capacità maligne, come lo spiare gli utenti, limitare gli utenti, back doors e aggiornamenti obbligatori sono comuni nel software proprietario e

alcuni sostenitori dell'open source vorrebbero metterle anche nei programmi open source[234].

Non solo: un'azienda avrebbe potuto pubblicare un software come open source (cioè il cui codice è completamente visibile) dopo averlo costruito «come una cattedrale», senza adottare il processo di lavoro del bazar[235].

Stallman riconosceva che il termine «free» poteva spaventare qualcuno. La scelta di compiacere il *big business*, di concentrarsi sulle questioni pratiche e organizzative e di ignorare le implicazioni etiche della creazione del software avrebbe portato all'ampliamento della comunità dei programmatori volontari, ma anche a una diluizione dei valori hacker di condivisione e libertà personale: «quando la gente sarà abituata a dire e pensare 'open source' questo sarà un ostacolo nella loro comprensione e riflessione sulla filosofia del free software».

Sul piano mediatico e comunicativo la strategia di Raymond funzionò perfettamente. A pochi mesi dalla fondazione dell'OSI altre aziende (Oracle, Informix[236], IBM, Dell) avrebbero seguito l'esempio di Netscape nell'annunciare che parte dei loro servizi sarebbe stata compatibile con Linux o con altri progetti Open Source. Nell'agosto 1998 «Forbes» pubblicava un articolo, significativamente intitolato *Per amore dell'hacking*, che descriveva la storia del software «liberato». L'approccio «comunitario» di Stallman era definito idealistico e fallimentare, mentre il nuovo modello era indicato come la svolta che aveva permesso agli hackers di affrancarsi dalla percezione negativa che li aveva perseguitati fin dagli anni Ottanta. Il «marketing» di Raymond era abbracciato senza riserve:

> Il software liberato è diventato una Olimpiade intellettuale dove alcune delle migliori menti ingegneristiche del mondo competono – non per accaparrarsi investimenti, ma per impressionare i propri pari. [...]
>
> Questi artisti chiamano sé stessi «hackers» ma sono molto lontani dai tronfi quattordicenni (anche conosciuti come crackers) che conquistano le prime pagine dei giornali cercando di entrare nei computer del Pentagono[237].

Nell'ottobre dello stesso anno «The Economist» sanciva l'avvenuta riabilitazione degli hackers raccontando il successo commerciale di Red Hat, compagnia di distribuzione di Linux fondata nel 1993 da Bob

Young, e definendo il sistema operativo Open Source «non solo gratuito, ma probabilmente migliore [di Windows], offrendo stabilità e scalabilità che [Windows] non può raggiungere [...]. Nel lungo periodo Linux e altri programmi open source possono causare a Mr. Gates molti grattacapi»[238].

Open Source e cultura hacker

Se la nascita del movimento Open Source ebbe l'effetto, nel medio e lungo periodo, di riabilitare la parola «hacker» agli occhi dell'industria[239] e di una parte dei media, più incerto è, nel breve periodo, l'effetto che essa ebbe sulla sottocultura hacker nel suo complesso. Nonostante Linux fosse adottato dalla totalità degli hackers, l'underground elettronico era, in quegli anni, ben lontano dal sentirsi riabilitato, o dal considerare l'adozione di Linux da parte di privati o aziende come una vittoria della comunità. L'espressione «open source» appare, tra il 1993 e il 2000, sulle pagine di «2600» e di «Phrack», per un totale, rispettivamente, di nove e dodici volte, mentre il nome di Torvalds non appare su «2600» ed è citato soltanto due volte su «Phrack». L'espressione «free software», per quanto più discussa, anche in virtù della sua più lunga storia, non supera le poche decine. Linux appare ben più frequentemente, ma quasi sempre in contesti tecnici (la spiegazione di un hack, per esempio) e non per i suoi significati politici o sociali. Per contrasto, il nome di Kevin Mitnick ricorre nello stesso periodo 510 volte su «2600» e 174 su «Phrack», con un picco proprio nel biennio 1998-1999, che vedeva la nascita del movimento Open Source, ma anche l'apice della campagna per la liberazione di Mitnick.

Non vi è dubbio che i lettori delle due principali riviste dell'underground hacker conoscessero, apprezzassero e usassero i prodotti Free Software e Open Source, a volte con entusiasmo quasi religioso[240]; è certo che alcuni di loro vi abbiano contribuito e che i software non proprietari fossero da essi visti come prodotti di un'unica cultura hacker. Ma il loro valore politico, così come le differenze tra i modelli di sviluppo, non erano discussi o percepiti come centrali alla comunità. Il dibattito Raymond-Stallman era più importante per le riviste accademiche e tecniche che non per gli scritti autoprodotti dagli

hackers esterni all'università. L'impressione è che permanesse, alla fine del millennio, quella divisione tra hackers accademici (ora diventati accademico-imprenditoriali), preoccupati dell'etica, della qualità e della profittabilità del software, e hackers extra-accademici e «underground», tendenzialmente anti-sistema, anti-corporation, e più vicini allo stile e alle priorità dei phone phreaks e dell'hacking del decennio precedente.

Questo non significa che non esistesse, negli anni Novanta, un'unica cultura hacker: i due filoni condividevano alcuni luoghi di incontro (le conventions, ma anche i *fora* online dei progetti open source), alcuni miti fondativi, immaginari (soprattutto quello fantascientifico), strumenti (Linux era universalmente preferito a Windows) e caratteristiche culturali quali la classe sociale, l'individualismo, il libertarianesimo, la capacità tecnico-creativa come metro del valore individuale, le modalità di comunicazione verso l'esterno.

In quest'ultimo campo la continuità tra i due gruppi e il legame del movimento Open Source con la storia delle culture tecniche statunitensi è particolarmente evidente. Nel teorizzare il marketing del movimento, Eric Raymond si presentava come inventore di una strategia che in realtà nuova non era. Per attirare l'attenzione dei media occorreva raggiungere, scriveva, un «livello ottimale di provocazione», una «dissonanza attrattiva» che suscitasse la curiosità del giornalista per l'«evangelista» e lo spingesse a concedergli spazio sulla sua testata. Per farlo occorreva «discutere giovialmente del mio interesse nelle armi da fuoco, nell'anarchia e nella stregoneria, dando però l'impressione di essere il più ben tenuto, bambinesco e iper-americano possibile. Il trucco è suonare strano e criptico con un'aria di onestà e semplicità». Non è dato sapere se Raymond conoscesse la biografia e gli scritti di Abbie Hoffman o se avesse semplicemente raccolto, dalla tradizione phreak poi divenuta hacker, le basi della comunicazione mediatica yippie. Hoffman, fosse stato in vita alla fine del millennio, avrebbe certamente rifiutato i fini esclusivamente pragmatici del movimento Open Source, e avrebbe senz'altro disprezzato alcune delle sue posizioni politiche. Ma probabilmente non avrebbe avuto problemi a riconoscere in Raymond (che si presentava a conferenze stampa e manifestazioni vestito da Obi-Wan Kenobi, all'urlo di «May the Source be with you»[241], accompagnato

da un pinguino in plastica – il simbolo di Linux – e dalla bandiera americana) un praticante del suo monkey theatre. E avrebbe forse riconosciuto il suo successo: il motto «May the Source be with you» sarebbe diventato per un qualche tempo uno slogan hacker (ancora oggi stampato su tazze e magliette) e sarebbe stato riportato da stampa e tv. Le performances di Raymond, la «rispettabilità» del movimento e, soprattutto, l'efficienza e l'onnipresenza di Linux avrebbero assicurato agli hackers una copertura molto più benevola rispetto a quella che era stata loro riservata nel decennio precedente, aprendo le porte per un'ulteriore espansione della cultura, questa volta anche al di là dei confini delle pratiche tecnologiche.

220 T. Nelson, *Computer Lib/Dream Machines* (1974), Microsoft Press, Redmond 1988, p. 44.

221 T. Berners-Lee, M. Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*, HarperBusiness, San Francisco 1999, p. 4.

222 Ivi, p. 73.

223 H. Jenkins, *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century*, The MIT Press, Cambridge (Mass.) 2009.

224 E.S. Raymond, *The Cathedral & the Bazaar. Musings on Linux and Open Source by an Accidental Revolutionary*, O'Reilly Media, Sebastopol (CA) 1998, p. 2.

225 Ivi, p. 24.

226 *Netscape Announces Plans to Make Next-Generation Communicator Source Code Available Free on the Net*, in «Netscape.com», 22 gennaio 1998, https://web.archive.org/web/19980127155653/http://home.netscape.com/newsref/pr/newsrelease558.htm.

227 E.S. Raymond, *The Revenge of the Hackers*, 2000, https://web.archive.org/web/20211021123529/http://www.catb.org/~esr/faqs/hacker-revenge.html.

228 In un'intervista, ad esempio, Gates affermava con aria di superiorità: «Non ho mai sentito un cliente menzionare Linux». J. Brinkeley, *Microsoft Witness Attacked for Contradictory Opinions*, in «The New York Times», 15 gennaio 1999.

229 V. Valloppillil, *Open Source Software: A (New?) Development Methodology*, in «catb.org», 11 agosto 1998, https://web.archive.org/web/20211125224853/http://www.catb.org/~esr/halloween/halloween1.html#quote1; Id., *Linux OS Competitive Analysis: The Next Java VM?*, in «catb.org», 11 agosto 1998

https://web.archive.org/web/20211206025209/http://www.catb.org/~esr/halloween/halloween2.html. Microsoft ha in seguito confermato l'autenticità dei documenti: E. Muth, *Microsoft Responds to the Open Source Memo Regarding the Open Source Model and Linux*, in «microsoft.com», 5 novembre 1998, https://web.archive.org/web/19991013112307/http://microsoft.com/ntserver/nts/news/mwarv/linuxresp.asp.

230 Valloppillil, *Open Source Software*, cit.

231 *Ibid.* La previsione si è finora rivelata corretta, perlomeno nel campo degli utenti di personal computers: nonostante Linux abbia il quasi monopolio delle grandi infrastrutture di impresa e di ricerca, più del 95% degli utenti desktop mondiali usa sistemi operativi proprietari. Più complessa e sfumata la situazione del mercato dei sistemi operativi mobili, al tempo inesistente, che vede oggi Android – un sistema operativo formalmente «open» che però ospita perlopiù apps proprietarie – in posizione di leadership. *Desktop Operating System Market Share Worldwide*, in «StatCounter Global Stats», 2021, https://gs.statcounter.com/os-market-share/desktop/worldwide/.

232 R. Stallman, *Why Open Source Misses the Point of Free Software*, in «GNU Operating System», https://web.archive.org/web/20210603074620/https://www.gnu.org/philosophy/open-source-misses-the-point.html.en.

233 Raymond, *The Revenge*, cit.

234 Stallman, *Why Open Source Misses the Point*, cit.

235 È quanto succede dal 2005 con Android, il sistema operativo per apparecchi mobili, pubblicato in maniera «aperta», ma sviluppato in quasi totale autonomia da Google.

236 *Leading Items*, in «Linux Weekly News», 23 luglio 1998, https://web.archive.org/web/20211120022743/http://lwn.net/1998/0723/.

237 J. McHugh, *For the Love of Hacking*, in «Forbes», 10 agosto 1998, https://web.archive.org/web/20220420091632/https://www.forbes.com/forbes/1998/0810/6203094a.html.

238 *Red Hat Trick*, in «The Economist», 3 ottobre 1998, https://web.archive.org/web/20220411143426/https://www.economist.com/business/1998/10/01/red-hat-trick.

239 Si noti, a titolo di esempio, che il quartier generale di Meta, la compagnia che gestisce Facebook, sorge al numero 1 di Hacker Way, a Menlo Park in California.

240 Coleman, *Coding Freedom*, cit., pp. 36-37.

241 Entrambi riferimenti alla serie di film *Star Wars*, che nel 1999 vedeva una nuova uscita dopo più di 15 anni. Obi-Wan Kenobi ne è uno dei protagonisti principali, «May the Force be with you» («Che la forza sia con te», storpiata in «Che la Sorgente sia con te») ne è uno dei refrain. R. Chalmers, *Msoft Welcomes the Linux Community, to the Car Park*, in «Tech Monitor» (blog), 15 febbraio 1999,

https://web.archive.org/web/20220420091716/https://techmonitor.ai/technology/msoft_welcomes_the_linux_community_to_the_car_park.

7.
Hacktivismo, 1995-2011

Global domination through media saturation

Nell'agosto 1998 un gruppo hacker chiamato «Cult of the Dead Cow» (cDc, «culto della vacca morta») rilasciava pubblicamente un software chiamato «Back Orifice» («orifizio posteriore»), una deformazione volgare del nome del software Microsoft «Back Office».

Il programma è un ottimo esempio di una delle principali forme che l'hacking ha assunto dalla fine del millennio. Il suo bersaglio era Microsoft, che dalla metà degli anni Novanta era arrivata a ricoprire per gli hackers lo stesso ruolo che per i phreaks aveva avuto AT&T: un modello che aiutava a definire in negativo le regole etiche e comportamentali della comunità. Laddove Windows, il principale prodotto di Microsoft, trattava i propri utenti come bambini, presentando loro un'esperienza informatica «preconfezionata», Linux, il sistema operativo hacker, permetteva il completo controllo della macchina e dei suoi processi. Laddove Microsoft aveva come fine il profitto, anche a scapito, secondo gli hackers, degli interessi dell'utente finale, Linux aveva come unico obiettivo l'efficienza tecnica e la possibilità dell'utente di piegare la macchina ai propri fini. Un campo nel quale Windows era particolarmente debole era quello della sicurezza: nel suo impeto di creare un prodotto accessibile e commercializzabile Microsoft ne nascondeva le vulnerabilità, ignote alla maggior parte dei suoi clienti ma evidenti per gli utenti esperti.

La funzione di Back Orifice era quella di rendere palesi, anche per i non specialisti, le falle di sicurezza di Windows. Esso permetteva di controllare un computer Windows da remoto senza che il proprietario se ne accorgesse, installandosi automaticamente, riavviandosi ogni volta che

si accendeva il computer e registrando quello che veniva immesso nella tastiera (ad esempio le passwords)[242]. La tipologia di programma non era nuova e aveva in alcuni casi usi legittimi (ad esempio l'assistenza da remoto). Ciò che rendeva particolare Back Orifice erano le modalità della sua distribuzione. Invece di mantenere segreta l'esistenza dell'exploit, sfruttandolo fino a che la sicurezza Microsoft non se ne fosse accorta e avesse aggiornato il sistema operativo, la possibilità di installare surrettiziamente Back Orifice su ogni piattaforma Windows fu pubblicamente annunciata durante una conferenza hacker (Def Con 6) a cui erano invitati anche esperti di sicurezza. Un comunicato stampa, firmato dal «ministro della propaganda» del gruppo, The Deth Vegetable, aveva preparato l'evento con toni ironicamente minacciosi («Usi un sistema operativo Microsoft in un network? Le nostre condoglianze»)[243]. Dopo pochi giorni la notizia sarebbe stata raccolta dalle maggiori pubblicazioni nazionali, da «Wired»[244] al «New York Times»[245]. Il rilascio di Back Orifice riportava all'attenzione pubblica uno dei temi che hanno accompagnato la storia dell'hacking fin dai giorni dei telefoni e quella del computer hacking fin dal Morris worm: rendendo pubblica una vulnerabilità tecnologica si dava la possibilità ai malintenzionati di avvantaggiarsene. Ma al contempo si spingevano i proprietari della tecnologia, che senza la pressione dell'opinione pubblica non avrebbero forse avuto l'incentivo economico per agire, a risolvere il problema.

La questione era però in questo caso esasperata. Da una parte vi era la facilità di accesso di Back Orifice: il trojan era distribuito gratuitamente dal sito cDc e il suo uso era reso estremamente semplice dall'interfaccia grafica e da precise istruzioni: con esso «anche un bambino di otto anni può distruggere tutto», secondo l'annuncio di The Deth Vegetable a Def Con 6[246]. Ogni curioso poteva provare l'ebbrezza di essere un hacker: in pochi giorni, secondo lo stesso gruppo, il software aveva raggiunto 14.000 download. Dall'altra parte vi era la perizia comunicativa di un gruppo hacker il cui motto era «Dominazione globale attraverso la saturazione dei media».

Cult of the Dead Cow era stato fondato da alcuni ragazzini texani nella seconda metà degli anni Ottanta, attorno a un BBS phreak[247], e cominciò ad essere conosciuto nella subcultura hacker dal 1990 in quanto

organizzatore, a Houston, di una delle prime conventions di computer hacking, HoHoCon. Il gruppo, che fino ad allora aveva limitate capacità tecniche, inaugurò una consapevole campagna mediatica dalla metà degli anni Novanta. Secondo Joseph Menn, cDc aveva una mailing list di giornalisti a cui mandare i propri comunicati stampa periodici, nella quale erano inclusi, per scherzo, gli indirizzi illecitamente ottenuti di celebrità come Harrison Ford, Sean Connery e Mr. T. Gli obiettivi politici erano ancora vaghi, ma lo stile era indubbiamente quello del monkey theatre. Dopo che Reagan aveva annunciato di essere affetto da Alzheimer il gruppo rivendicava di averglielo iniettato con un dardo di cerbottana. Se le loro richieste non fossero state soddisfatte (tra queste il bando delle sigarette sottili e la ripresa di un programma televisivo brasiliano) avrebbero infettato con l'Alzheimer tutti gli ex presidenti. Come nel caso degli Yippies, l'attenzione era ricercata non tramite la credibilità della minaccia, ma attraverso l'oltraggio che lo scherzo avrebbe generato, in un momento in cui l'opinione pubblica era emotivamente colpita dalla lettera pubblica nella quale l'ex presidente aveva rivelato di essere affetto dalla malattia.

«Siamo un'unità di guerriglia neo-marxista, anarco-socialista, nata con il solo obiettivo di finire in TV», recitava il sito cDc nel 1996[248]. Ovviamente il gruppo non era nulla di tutto ciò. L'unica etichetta politica applicabile era quella del generico libertarianesimo delle culture hacker, insofferenti ad ogni tipo di limitazione delle libertà personali. Ma il gruppo coniò la propria etichetta, chiamando le proprie attività «hacktivism» – una crasi tra le parole hack e attivismo –, che Oxblood Ruffin (Laird Brown), «ministro degli esteri» cDc, definiva come «usare la tecnologia per migliorare i diritti umani nei media elettronici», con l'importante corollario: «non serve molta gente per cambiare le cose. Basta un buon programmatore»[249].

Gli obiettivi politici di questa autoproclamata «avanguardia» erano legati alle tradizionali priorità hacker: la sicurezza delle informazioni personali e la libertà di espressione. Ma il gruppo, consapevole di dover competere nell'arena mediatica prima ancora che in quella tecnologica, mostrava maggiore abilità rispetto ad altri hackers con velleità politiche, citando la *Dichiarazione universale dei diritti umani*[250] e la *International Covenant on*

Civil and Political Rights dell'ONU a sostegno delle proprie posizioni e intessendo relazioni con la Electronic Frontier Foundation e altri gruppi di interesse. Il primo tema affrontato dal gruppo fu quello della censura di Internet. Attraverso il rapporto con un gruppo hacker cinese chiamato Hong Kong Blondes e usando la popolarità guadagnata nel conflitto con Microsoft scatenato da Back Orifice il gruppo riuscì ad attirare l'attenzione dei media sul tema della libertà di espressione in Cina. Come sostenuto da Menn e da molti altri critici al tempo e in seguito, è estremamente probabile che il gruppo di dissidenti cinesi fosse un'invenzione di Oxblood Ruffin. Ma questo non fa altro che provare le capacità comunicative del gruppo e l'efficacia del monkey theatre: la vicenda di un personaggio solitamente visto come negativo (l'hacker) che si dedica a combattere un'istituzione ancora più negativa (il Partito comunista cinese), come un moderno Davide contro Golia su scala globale, era esattamente quello che gli organi di informazione stavano cercando (e in molti casi ancora cercano) nella copertura del fenomeno hacker. La notizia sarebbe stata riportata da tutti i maggiori giornali senza ulteriore verifica e le parole attribuite da Oxblood all'immaginario Blondie Wong sarebbero state citate *verbatim* in *No Logo* di Naomi Klein, uno dei libri più popolari della sinistra globale alla fine del millennio.

Questo «hack sui media» ebbe l'effetto desiderato. La parola «hacktivismo» non fu raccolta soltanto dagli organi di informazione, ma dagli hackers stessi, che cominciarono, in svariati casi, a prendere di mira governi autoritari, corporations e individui visti come dannosi per la libertà di informazione o per altre cause collegate. La natura degli attacchi era spesso difficilmente riconducibile alla definizione di hack che ha caratterizzato gli individui e i gruppi finora descritti in questo libro. Dalla fine del millennio, infatti, esistevano software che avevano reso relativamente semplice condurre un attacco informatico, in particolar modo gli attacchi DDoS (Distributed Denial of Service), che rendono temporaneamente inutilizzabili i siti web sovraccaricandoli di visite. Un altro strumento tipico delle dimostrazioni digitali, che richiedeva maggiori competenze (ma a volte soltanto la distrazione o sciatteria di un «webmaster»), era il «defacing», la pratica di ottenere i privilegi di amministratore di un sito altrui e di modificare la homepage, spesso con

immagini ironiche o oscene[251]. L'utilizzo di questi metodi non richiedeva dominio sulla tecnologia, o creatività nel trovare una soluzione tecnica, ed era per questo guardato con disprezzo da chi si considerava un «vero hacker». Tuttavia, anche grazie alla mancanza di distinzioni nella copertura mediatica, gli attacchi DDoS e il defacing divennero due degli strumenti principali del nuovo «hacktivismo».

Anche per distinguersi da chi usava questi strumenti per semplice vandalismo, cDc fondava un sotto-gruppo, Hacktivismo, e nel 2001 pubblicava un manifesto che, rifacendosi alle dichiarazioni ONU, recitava:

> [...] La comunità hacker internazionale ha un imperativo morale ad agire e noi Dichiariamo:
> – Che il pieno rispetto dei diritti umani e delle libertà fondamentali include la libertà di un accesso equo e ragionevole all'informazione [...]
> – Che [...] ci opponiamo all'uso del potere dello Stato di controllare l'accesso al lavoro di critici, intellettuali, artisti o figure religiose.
> – Che la censura statale di Internet è una forma grave di violenza organizzata e sistematica contro i cittadini [...]
> – Che studieremo modalità e mezzi per aggirare la censura di Stato su Internet e che useremo tecnologie che sfideranno le violazioni dei diritti di informazione[252].

Il gruppo avrebbe pubblicato, nei cinque anni successivi, software per inserire contenuti censurati o vietati in files apparentemente innocui (CameraShy), come ad esempio GIF o fotografie digitali, in modo che potessero sfuggire al controllo dei censori; Six/Four, un software il cui nome fa riferimento alla data del massacro di Piazza Tienanmen e che doveva permettere la navigazione anonima; e una licenza, sul modello della GPL di Stallman, che in luogo di proteggere la libertà del software certificava che il programma da essa protetto era rispettoso della libertà di espressione e dei diritti umani (HESSLA - Hacktivismo Enhanced-Source Software License Agreement)[253]. Quest'ultimo progetto, in particolare, evidenzia la differenza tra gli hacktivisti legati a cDc e gruppi hacker ugualmente idealisti ma limitati alla politica del software, come i fondatori della Free Software Foundation. I secondi avevano fatto giustamente notare che la nuova licenza avrebbe limitato la «libertà» del codice senza impedire che gli Stati autoritari facessero uso del programma o di programmi alternativi[254]. Per i primi, però, che

rispettavano Stallman, ma lo consideravano un «hippie» di un'altra generazione[255], l'obiettivo era tanto pratico quanto comunicativo: nel distribuire strumenti per la navigazione anonima, Hacktivismo forniva esempi di come la cultura hacker poteva intervenire legittimamente nel discorso pubblico, mettendo l'accento sulla governance di Internet e assicurando che i temi della crittografia, della privacy e della «neutralità» della rete sarebbero rimasti al centro dell'attivismo digitale negli anni a venire.

Hacktivismo non fu l'unico gruppo derivato dal Cult of the Dead Cow, né probabilmente il più conosciuto. Questo onore va a L0pht, un'organizzazione con sede a Boston che includeva alcuni membri di punta di cDc. Oltre ad essere uno dei primi «hackerspace» (luoghi dove gli hackers possono ritrovarsi fisicamente per lavorare in gruppo, oggi molto popolari), fondato nel 1992, L0pht fu uno dei primi gruppi hacker a vendere i propri servizi (nella forma di software, ma soprattutto di consulenze sulla sicurezza informatica) e a intrattenere rapporti ufficiali con aziende e autorità. Più abili tecnicamente delle loro controparti in Hacktivismo, i membri di L0pht furono capaci di attirare l'attenzione mediatica (un articolo del «Washington Post» li definiva «le rock star dell'élite hacker nazionale»)[256] tramite il loro rapporto diretto e spesso conflittuale con le aziende di software, in particolare Microsoft: ogniqualvolta questa pubblicava un aggiornamento di Windows, L0pht trovava delle vulnerabilità e le elencava in avvisi pubblici, costringendo l'azienda a modificare il proprio software o perlomeno a rispondere. Non ci volle molto perché le aziende e il governo preferissero avere L0pht come consulente o interlocutore piuttosto che come avversario. La reputazione del gruppo era tale che, nel 1998, i suoi membri furono chiamati a testimoniare davanti al Senato degli Stati Uniti. Come abbiamo visto nel cap. 3, non era la prima volta che un hacker era invitato dal Congresso. Era però la prima volta che un gruppo hacker si presentava al governo come organizzazione legittima e aveva la possibilità di illustrare alcune delle priorità dell'etica hacker senza la mediazione degli organi di informazione. «Negli ultimi quattro anni noi sette siamo stati chiamati un conglomerato hacker, un think tank hacker, il luogo di ritrovo dei migliori hackers statunitensi, un network di esperti di

sicurezza e un gruppo di protezione dei consumatori. In realtà tutto quello che siamo è semplicemente curiosi»[257]. In un paragrafo della testimonianza scritta, intitolato *Gli hackers non sono i cattivi*, il gruppo affermava che gli hackers incarnavano una «can do attitude»[258], vista come tipicamente statunitense, e che grandi inventori americani, come Edison e Bell, erano hackers *ante litteram*, poiché «prendevano quello che era loro disponibile e lo facevano funzionare». I media erano accusati di essere responsabili dell'ignoranza della popolazione su cosa fosse un vero hacker: ogni volta che un sistema informatico era compromesso i giornali parlavano di un «ragazzino brillante». Ma, nella maggior parte dei casi, il ragazzino in questione usava un software preconfezionato, che non aveva necessità di comprendere, «così come chiunque prema il grilletto di una pistola carica non deve necessariamente capire le traiettorie, la velocità e la combustione». Il sensazionalismo che accompagnava attacchi tecnicamente banali faceva sì che sempre più ragazzini volessero guadagnare fama colpendo bersagli in vista, diluendo sia la capacità tecnica della comunità hacker sia la reputazione dei «veri hackers».

La testimonianza orale, dopo aver passato in rassegna i progetti cui lavoravano i membri del gruppo, si concentrava sui temi della vulnerabilità dei sistemi informatici e di comunicazione governativi e sul ruolo delle aziende private nel diffondere software non sicuro. Tra le raccomandazioni di L0pht vi era quella di affidarsi a sistemi dal codice aperto (come Linux), piuttosto che a «scatole nere» come Windows («È come comprare una macchina senza poter mai aprire il cofano»), di costituire un'agenzia indipendente per la valutazione della sicurezza del software commerciale e di rendere più sicure, attraverso la crittografia, la navigazione e l'autenticazione in Internet. Mudge (Peiter Zatko), leader di L0pht e membro cDc, trovava anche spazio per un accenno di monkey theatre quando affermava, in risposta alla domanda di un senatore, che uno qualsiasi dei sette hackers presenti sarebbe stato in grado, in meno di trenta minuti, di disabilitare Internet per l'intero paese.

Significativo del rispetto accordato al gruppo, e più in generale del mutamento della concezione dell'hacker anche agli occhi dei legislatori, è che i membri di L0pht si presentassero davanti ai senatori non con il proprio nome di battesimo, ma con il proprio appellativo hacker

(Mudge, Brian Oblivion, Space Rogue, Weld Pond, Kingpin... tutti paradossalmente preceduti dal titolo Mr. nella trascrizione ufficiale). Uno dei senatori comparava addirittura gli hackers a «moderni Paul Revere»[259].

Come il caso di Kevin Mitnick riassume la visione dell'hacker negli anni Novanta, così il Cult of the Dead Cow e i suoi due spin-off rappresentano i radicali mutamenti avvenuti nella percezione e nella pratica dell'hacking al volgere del secolo. Da un lato, anche grazie all'avvento di strumenti largamente usati e di un modello di sviluppo ampiamente lodato quale l'Open Source, vi è una risemantizzazione in chiave positiva, enucleata dall'esperienza di Hacktivismo, che usava strategie comunicative proprie delle comunità tecniche e strumenti del computer hacking per sostenere cause politiche quasi universalmente ritenute positive. Nei primi anni Duemila le cause hacktiviste si moltiplicheranno e, con l'avvento di Anonymous e Wikileaks, di cui parleremo a breve, l'attivismo online troverà una copertura mediatica ancora più ampia e onnipresente.

Dall'altro lato vi è una rivalutazione da parte dei governi delle capacità e delle potenzialità degli hackers, visti non più come semplici minacce ma come possibili risorse. Il nemico principale non era più il ragazzino che si divertiva ad esplorare il sito del Pentagono, ma, in particolare dopo gli attacchi dell'11 settembre 2001[260], l'hacker al soldo di una potenza straniera. L'avvicinamento che era stato inaugurato, almeno pubblicamente, da L0pht sarebbe diventato un rapporto costante negli anni seguenti, tanto che oggi la collaborazione o il diretto controllo di gruppi hacker da parte di diversi Stati è una delle forme più frequenti e mediaticamente visibili della pratica (vedi Conclusione).

We are Legion

Il gruppo hacker più famoso e influente del nuovo millennio non emergerà direttamente dai movimenti e dalle comunità descritte finora, ma da un forum online, 4chan, e da un'intervista all'attore Tom Cruise.

4chan è una bacheca digitale divisa in canali tematici, la cui particolarità è che i messaggi su di essa pubblicati scompaiono dopo un certo tempo se non ricevono continuamente risposta. Non esiste inoltre su 4chan la

possibilità di accompagnare ai messaggi il nome o il nickname del loro autore. Ogni utente è denominato «Anonymous». Il completo anonimato e la centralità della popolarità del post hanno fatto sì che alcune sue sezioni assumessero caratteri estremamente scioccanti, con contenuti sessuali espliciti, violenza e trolling usati per attirare l'attenzione dei tantissimi utenti. La mancanza di nomi e di un'identità permanente non ha impedito che su 4chan si sviluppasse una comunità, con un proprio gergo (spesso provocatoriamente volgare), i propri riti e le proprie pratiche. Una delle più caratteristiche tra queste è il «doxing»: la rivelazione di dettagli privati di una persona (indirizzo, foto, profilo social...) per esporla agli scherzi e alle molestie da parte di utenti anonimi. La motivazione addotta da questi ultimi per un'azione che non di rado comportava gravi danni per la vittima era, molto semplicemente, il divertimento o, nel gergo del forum, i «lulz»[261]. In altri casi gli utenti si organizzavano in «operazioni» volte a inondare di spam un altro forum, a rendere ingiocabile un videogioco online o ad abbattere siti web. L'annuncio dell'attacco avveniva su 4chan e poi l'organizzazione si spostava su canali chat, essi stessi anonimi. La natura dell'attacco era del tutto arbitraria, purché l'operazione fosse ritenuta divertente e in un qualche modo dimostrativa delle capacità del gruppo, e la scelta del bersaglio dipendeva più dall'efficacia del post che iniziava l'azione che non dalle caratteristiche o dalle colpe di chi si andava a colpire.

Nel gennaio 2008 un'intervista su Scientology a Tom Cruise fu pubblicata online per sbaglio da una stazione televisiva che aveva deciso di non trasmetterla. L'attore lodava Scientology come il nuovo passo nell'evoluzione della civiltà. Ma la retorica esagerata, lo stato di semi-trance in cui Cruise sembrava essere e la sua inquietante risata resero il video un meme, particolarmente apprezzato e spietatamente deriso su 4chan. Scientology cercò energicamente di rimuovere il video dalla rete, minacciando denunce a tutte le pubblicazioni online che lo avevano riprodotto. Il 15 gennaio il seguente messaggio appariva su 4chan (/b/ era la sezione del forum dedicata a qualsiasi tipo di discussione e dove ogni tipo di contenuto era permesso):

> Penso sia tempo per /b/ di fare qualcosa di grosso.
> La gente deve capire che non devono rompere il cazzo a /b/ [fuck with /b/], e parlare

per dieci minuti, e aspettarsi che la gente dia i suoi soldi a un'organizzazione che non ha assolutamente nessun cazzo di senso.

Sto parlando di «hackerare» o «chiudere» il sito ufficiale di Scientology.

È tempo di usare le nostre risorse per fare qualcosa che crediamo giusto.

È di nuovo tempo di fare qualcosa di grosso.

Parlate tra di voi, trovate un posto migliore per pianificare e poi portate a termine quello che può e deve essere fatto.

È tempo, /b/[262].

Da questo messaggio e da questa banale occasione sarebbe nato un movimento, chiamato Anonymous come ogni singolo suo partecipante, che avrebbe avuto risonanza e conseguenze mondiali, intervenendo nelle rivoluzioni tunisine ed egiziane e attirando l'attenzione di giornalisti, agenzie di sicurezza, governi e attivisti in tutto il mondo.

Spiegare Anonymous è straordinariamente difficile. Non solo perché i messaggi su 4chan scompaiono senza lasciare traccia, i partecipanti non hanno un nome e la maggior parte delle interazioni avviene in chats private. È la struttura stessa del gruppo che sfugge a una definizione univoca. A ben vedere Anonymous non era una vera e propria comunità: era una costellazione di gruppi in continuo movimento, la cui alchimia sarebbe cambiata sostanzialmente negli anni. Chiunque poteva assumere il nome Anonymous e farsi portatore di una causa, purché questa fosse capace di attirare l'attenzione di /b/ e delle chats.

Le azioni hacker, in particolar modo in Anonymous, tendono ad essere dinamiche e fluide, con svariati individui o anche gruppi che lavorano in concerto. Quello che è vero per un'operazione può non esserlo per quella seguente. A volte un hacker particolarmente ossessionato genera, temporaneamente, un flusso di lavoro organizzato e collettivo. Altre volte è solo caos e fraintendimento[263].

Anche la definizione di hacker è di difficile attribuzione, almeno nel primo periodo e almeno nell'accezione che abbiamo finora usato: buona parte degli attacchi di cui parleremo era condotta tramite DDoS, una pratica che, come abbiamo detto, era guardata con disprezzo da molti hackers: da una parte non richiedeva alcuna capacità tecnica o creatività, ma solo di far partire un software; dall'altra negava, anche quando dichiarava di volerla difendere, la libera espressione, in quanto il suo risultato era la sospensione delle normali operazioni di un sito web. Certo, alcuni hackers, anche talentuosi, avrebbero partecipato alle

operazioni di Anonymous, e le questioni oggetto di protesta erano spesse legate all'ideologia hacker. Ma la creatività e l'esplorazione non erano il punto, come scrive il collettivo stesso in una spiegazione rivolta ad altri hackers sulle pagine di «2600»:

> Ecco come di solito si svolge un epico raid di Anonymous. Degli hackers black hat [...] cedono un exploit che non è più finanziariamente proficuo o donano le loro botnets. Vanno su [vari *fora* e canali chat] e spargono la voce che un raid epico sta per cominciare. Gente a caso, appena più avanzata tecnicamente, scrive i codici per sfruttare l'exploit o tools di DDoS con mezzi punta e clicca facili da usare per chiunque, poi postano dappertutto un annuncio pubblicitario, richiamando volontari che li aiutino nella e-jihad globale. Un raid è nato, un sito è abbattuto, e poi comincia il trolling dei media. Chiunque è incoraggiato a contattare i media e rivendicare il raid per qualsiasi ridicola ragione, politica o di trolling. Una volta ho visto un servizio di Fox News che attribuiva un raid a un gruppo organizzato di malati di AIDS contro i profilattici[264].

Fortunatamente per la nostra conoscenza del fenomeno, l'antropologa Gabriella Coleman stava effettuando la propria ricerca sul campo sugli hackers proprio nel momento in cui Anonymous stava nascendo e ha seguito la parabola del «gruppo» in tutte le sue evoluzioni, partecipando alle chats, seguendo le diverse operazioni e intervistando alcuni dei protagonisti. Dal suo eccellente libro, dal quale sono tratte due delle citazioni precedenti, apprendiamo che Anonymous era atipico, come gruppo hacker, anche in un altro aspetto: la sua composizione non era quella che aveva caratterizzato le culture tecniche fin dall'inizio del Novecento, ma includeva diverse etnie e classi sociali. Al contrario di cDc, i suoi membri erano sparsi per il globo e non risiedevano soltanto in Occidente, in molti casi non si erano mai incontrati di persona e quasi sempre non conoscevano le rispettive identità anagrafiche. Anonymous era, più di altri gruppi descritti finora, figlio della più larga disponibilità di artefatti informatici, della comunicazione digitale e della semplificazione del rapporto con la tecnologia che il consumismo informatico aveva reso possibile.

Eppure almeno una caratteristica, come si intuisce dalla citazione precedente, rimaneva costante: il fondamentale rapporto del gruppo con i media «mainstream» e il monkey theatre (anche se nessuno, a quanto sappiamo, citava direttamente Hoffman o mostrava di conoscerne gli scritti) come strumento per attirarne l'attenzione su specifiche cause.

Anonymous è una bandiera che può essere usata da chiunque voglia farsi una risata provocando i media, $cientology, o postando su un forum per epilettici delle immagini lampeggianti. L'obiettivo è creare anarchia e rinforzare l'idea che Internet non deve e non può essere controllata da governi o corporations attraverso un trolling di massa, semiorganizzato e senza precedenti[265].

Come scrive Tatiana Bazzichelli, «Non è [per Anonymous] importante vincere una battaglia o mettere fuori gioco un server, ma far sì che la gente parli di argomenti cruciali, evidenziare bug nel sistema, fornire prove della corruzione, diffondere un meme, creare un'idea virale, proporre nuovi percorsi di pensiero»[266]. Si prenda ad esempio il video YouTube in cui l'operazione contro Scientology (ironicamente battezzata «Chanology») faceva il proprio debutto pubblico. Grigie nubi in veloce movimento su un cielo cittadino fanno da sfondo a una voce computerizzata, che avverte i leaders di Scientology:

Negli anni vi abbiamo osservato. Le vostre campagne di disinformazione, la vostra soppressione del dissenso [...] Anonymous ha dunque deciso che la vostra organizzazione deve essere distrutta. Per il bene dei vostri seguaci, per il bene dell'umanità e per il nostro divertimento vi espelleremo da Internet e smantelleremo la Chiesa di Scientology. [...] Non potete nascondervi, perché siamo dappertutto. [...] La conoscenza è libera. Siamo Anonymous. Siamo Legione[267]. Non dimentichiamo. Non perdoniamo. Stiamo arrivando[268].

Il gruppo di utenti di 4chan non aveva ovviamente il potere di espellere Scientology dalla rete, e tantomeno di smantellare la sua organizzazione. E non erano certo anni di osservazione che li avevano spinti all'azione, piuttosto pochi giorni, dalla pubblicazione del video di Cruise. Ma la reazione scomposta della Chiesa (un comunicato del febbraio 2008 definiva Anonymous un'«organizzazione cyber-terroristica») e la curiosità dei media resero il gruppo una realtà, anche a scapito della sua natura fluida e arbitraria. Le ragioni per le quali lo scontro tra gli hackers e Scientology era così affascinante per l'opinione pubblica erano le stesse che avevano fatto il successo di cDc: un gruppo hacker (o raccontato come tale) si scagliava contro un'entità percepita, già allora, come negativa, contrapponendo i propri limitati mezzi a un'organizzazione globale e multimilionaria. Al contrario di cDc, i cui membri erano scelti con cura e dovevano essere introdotti da chi era già all'interno del

gruppo, chiunque poteva diventare Anonymous, scaricando un software per DDoS e unendosi ai *fora* e alle chats. Perciò l'effetto dell'attenzione mediatica fu quello di moltiplicare le persone che partecipavano agli attacchi contro Scientology. Se Anonymous non era «Legione» all'inizio, lo sarebbe diventato grazie alla cassa di risonanza dei giornali, delle televisioni e dei nascenti social media: dopo la pubblicazione del video, da poche centinaia i partecipanti nelle chats sarebbero diventati migliaia[269]. Il gruppo avrebbe cominciato a organizzare canali chat dedicati al dialogo con i reporters e nel tempo sarebbero emerse come figure centrali al movimento membri il cui principale talento non era l'hacking, ma il rapporto con i giornalisti e la «propaganda» (Barrett Brown – vero nome – e Topiary in particolare).

Le azioni contro Scientology comprendevano inizialmente il temporaneo oscuramento del suo sito web tramite attacco DDoS – coordinato tramite chat anonima –, scherzi telefonici, invio di fax completamente neri per esaurire i toner delle macchine dell'organizzazione, ordine di centinaia di pizze alle sedi di Scientology. Ma presto la protesta arrivò nelle strade, con manifestazioni di fronte alle sedi di Scientology in varie città statunitensi e poi in tutto l'Occidente. I manifestanti (probabilmente parte di essi non aveva mai sentito parlare di 4chan, ma coglieva l'occasione per protestare contro un'organizzazione dalla pessima reputazione) indossavano la maschera di Guy Fawkes, per come era stata rappresentata nel film *V for Vendetta*, che sarebbe diventata il simbolo più riconoscibile di Anonymous.

La protesta si sarebbe gradualmente spenta nel corso del 2008 e per due anni 4chan sarebbe tornata alla propria routine di pornografia e trolling. Nel settembre 2010, tuttavia, una notizia apparentemente innocua – il fatto che una compagnia di software indiana stava colpendo con attacchi DDoS il sito di torrent The Pirate Bay per impedire lo scambio illegale di materiale protetto da copyright – risvegliò l'attenzione di /b/. Recuperando il nome Anonymous e i suoi simboli, gli utenti di 4chan, indignati dal fatto che compagnie private stessero usando il «loro» strumento per impedire la libera circolazione delle informazioni, cominciarono a bersagliare con attacchi DDoS la compagnia indiana e

altre organizzazioni legate alla difesa della proprietà intellettuale, in quella che fu battezzata «Operation Payback» (Operazione Vendetta).

Ma è con la sua associazione con Wikileaks che Anonymous diventa un attore della politica internazionale e probabilmente il gruppo «hacker» più conosciuto di sempre. Wikileaks è un sito dedicato alla pubblicazione di documenti sensibili e segreti, fondato dall'hacker australiano Julian Assange. Nel 2010 il sito pubblicava centinaia di migliaia di messaggi riservati tra le ambasciate statunitensi e documenti relativi alle guerre in Iraq e Afghanistan. Tra questi vi era un video, ribattezzato «Assassinio collaterale», che mostrava il punto di vista e i commenti di soldati americani mentre massacravano da un elicottero, con atteggiamento *nonchalant* e quasi divertito, civili iracheni, compresi giornalisti e bambini. Il rilascio dei documenti fu coordinato, per massimizzare l'effetto ed evitare la censura, con alcune delle maggiori testate giornalistiche internazionali.

In risposta all'indignazione del governo americano, che aveva definito Assange una minaccia alla sicurezza nazionale[270], Amazon smise di ospitare sui propri servers il sito di Wikileaks e MasterCard, Visa, Paypal rifiutarono di accettare donazioni in favore dell'organizzazione. L'attacco contro Amazon e i servizi di pagamento online ostili a Wikileaks segnava la trasformazione di «Operation Payback» in «Operation Avenge Assange» (Operazione Vendicare Assange). Nel giro di pochi giorni il traffico simulato dall'attacco DDoS aveva reso inaccessibile il sito di Paypal e quello di MasterCard e aveva fatto apparire Anonymous su tutti i giornali del mondo (i servers di Amazon si rivelarono meglio protetti). Due gli strumenti che avevano permesso a un forum online e a un relativamente sparuto gruppo di attivisti e trolls di colpire gli interessi e la reputazione di alcune delle più grandi aziende finanziarie al mondo. Il primo erano le botnets: reti di computer infettate da un trojan che, senza la consapevolezza dei loro proprietari, erano controllate da una singola persona (un «botmaster»), che in questo caso ordinava loro di partecipare a un DDoS. In questo modo un singolo individuo poteva simulare il traffico di migliaia o decine di migliaia di utenti su un sito web nello stesso momento. Il secondo era ironicamente chiamato LOIC (Low Orbit Ion Cannon), un software che permetteva di offrire

volontariamente il proprio computer a una botnet in occasione di un attacco. Nessuno dei due strumenti richiedeva particolare talento o un grande numero di partecipanti. Ciò non impedì ai media di affermare che un gruppo di migliaia di hackers aveva abbattuto MasterCard[271], innescando di nuovo l'effetto moltiplicatore che avrebbe portato ad Anonymous nuovi «membri» e nuove munizioni per i propri attacchi. Tra i nuovi arrivati vi erano tuttavia anche hackers più tradizionali e talentuosi, come provato dalla maggiore sofisticazione delle due operazioni successive, Operation Tunisia e Operation Egypt.

L'attenzione di Anonymous sui due Stati nordafricani fu richiamata, come sempre, in maniera casuale e arbitraria[272]. Nel caso tunisino, un partecipante alle chats cominciò a insistere che Anonymous avrebbe dovuto aiutare chi, alla fine del 2010, si stava ribellando contro il regime di Ben Ali, ricevendo infine attenzione. Nel caso egiziano l'azione fu motivata dalla chiusura di Twitter e poi dell'intera rete da parte di Mubarak nel gennaio 2011. Le due operazioni seguivano il consueto iter di defacing e DDoS, ma in questo caso vi furono contatti diretti con gli attivisti tunisini ed egiziani e un aiuto effettivo nel garantire la privacy delle loro comunicazioni e il loro accesso a Internet. Di nuovo il rapporto con i media si rivelava fondamentale: uno degli obiettivi principali era quello di denunciare il disinteresse delle testate occidentali per le rivolte medio-orientali. Quando finalmente le «primavere arabe» finirono in prima pagina Anonymous era ormai diventato un attore internazionale[273].

LulzSec

Si potrebbe pensare che il successo, almeno temporaneo, delle primavere arabe avrebbe portato a una responsabilizzazione del gruppo o persino alla sua graduale istituzionalizzazione in gruppo politico e di pressione. In realtà accadde il contrario. Grazie all'osservazione partecipata di Gabriella Coleman sappiamo che alcuni membri di punta del gruppo cominciavano a guardare con impazienza alle cautele necessarie per un rapporto produttivo con i media e alla gestione di delicate situazioni di protesta sul terreno. Era tempo di tornare ai «lulz».

L'occasione fu data, all'inizio del 2011, dalle vanterie di un'azienda di

sicurezza informatica, HBGary, che sosteneva di essere in grado di attribuire un nome e un cognome ad alcuni membri di Anonymous. Nel giro di poco tempo Sabu, uno degli hackers più capaci del gruppo, otteneva accesso illegale ai servers e agli accounts social di HBGary e pubblicava tutte le mail interne dell'azienda. Prima ancora del contenuto delle comunicazioni (che rivelavano che la compagnia proponeva ai propri clienti delle campagne mediatiche e di hacking contro organizzazioni come Wikileaks), ciò che contava era il danno reputazionale (un'agenzia di sicurezza che non è capace di proteggere i propri stessi servers) e soprattutto l'impressione di onnipotenza che l'hack attribuiva al gruppo. Azioni del genere erano in piena continuità con la tradizione hacker degli anni Ottanta e Novanta: si trattava di un hack complesso (non il semplice uso di scripts creati da altri), che dominava in maniera completa e umiliante l'avversario. Ma non aveva nulla a che vedere con l'Hacktivismo e poteva riflettersi in maniera negativa su Anonymous. Così uno sparuto gruppo di membri tra i più attivi e tecnologicamente capaci decise di fondare LulzSec (Lulz Security), con l'obiettivo esplicito di «distruggere e mettere a nudo corporations, governi, spesso la popolazione nel suo complesso, e possibilmente tutto quello che c'è in mezzo, solo perché possiamo»[274]. La scelta era motivata anche dalla sensazione che il coinvolgimento in questioni internazionali ed etiche avesse allontanato gli hackers da quello che davvero contava: il divertimento. Il sito del gruppo recitava: «Ciao, buongiorno, come va? Splendido! Siamo LulzSec, un piccolo team di individui lulzy [neologismo: appassionati di lulz?] che pensano che la mancanza di stile della cyber community sia di peso a quello che realmente conta: il divertimento»[275].

Divertimento e filosofia del «solo perché possiamo» sono probabilmente le migliori spiegazioni degli obiettivi scelti da LulzSec: gli hackers colpivano dove trovavano vulnerabilità e nei luoghi che avrebbero dato maggiore visibilità al gruppo. La prima vittima, nel maggio 2011, fu Fox News, con il furto di diversi accounts dei suoi dipendenti e la lista dei candidati al popolare reality show *X-factor*. La motivazione (evidentemente pretestuosa per chi conosca il tono e i contenuti dell'«informazione» di Fox News) era il fatto che un

programma Fox aveva offeso il rapper Common. La seconda vittima fu il canale televisivo PBS, il cui sito web fu modificato per riportare la notizia che il rapper Tupac (ucciso nel 1996) era ancora vivo in Nuova Zelanda. La terza furono le compagnie di videogiochi, come Riot, Bethesda Softworks e Sony. Attraverso un «semplice» SQL injection LulzSec ottenne accesso ai dati riservati di Sony Pictures, rendendoli immediatamente pubblici. Poi il gruppo si rivolse a obiettivi istituzionali: il sito del Senato statunitense e persino quello della CIA (abbattuto per diverse ore tramite DDoS).

Dopo solo cinquanta giorni di attività il gruppo si sciolse, dando però il via a una nuova operazione, «AntiSec», rivolta contro i white hat hackers delle agenzie di sicurezza informatica. Gli attacchi contro compagnie di videogiochi, organi di informazione e istituzioni sarebbero in ogni caso continuati nel corso del 2011, anche dopo l'arresto di alcuni membri di LulzSec (tra questi Jake Davis – Topiary – cittadino britannico allora diciottenne, maestro del monkey theatre e principale responsabile della comunicazione di Anonymous e LulzSec). Si sarebbe in seguito saputo che gli arresti erano stati resi possibili dalla collaborazione con l'FBI di uno dei leader di Anonymous e LulzSec, Sabu (Hector Monsegur).

Per una spiegazione più dettagliata della complessa e avvincente storia di LulzSec e AntiSec si rimanda ai già citati libri della giornalista Parmy Olson (che aveva accesso privilegiato al gruppo) e di Gabriella Coleman. Ciò che interessa qui è notare, come ha già fatto la stessa Coleman[276], la reazione della cultura hacker nel suo complesso e ciò che questa ci dice sull'evoluzione della pratica in anni recenti. Laddove Anonymous aveva suscitato in non pochi casi dubbi (in particolare sui DDoS) e un senso di superiorità rispetto ad azioni che non erano ritenute «vero hacking», LulzSec e AntiSec riscossero un ampio successo – anche tra i white hats, che erano il loro bersaglio principale. Al contrario del collettivo senza volto che era Anonymous, i componenti di LulzSec avevano e rivendicavano un'identità, sebbene mascherata dai soprannomi, e divennero delle vere e proprie celebrità. In un pezzo significativamente intitolato *Risvegli* un anonimo contributore di «2600» celebrava «una sorta di rinascimento che ha riaperto una porta dalla quale molti di noi, nel corso degli anni, si sono allontanati. Quella porta può portare a cose

come una completa trasparenza, pura beffa [mischief] e, più importante, giustizia»[277].

Ironicamente, il motivo del successo di LulzSec tra gli hackers era però il fatto che il gruppo aveva abbandonato le cause politiche per un obiettivo che tutti gli hackers potevano apprezzare, a prescindere dal loro rapporto con la legge: usare hacks brillanti per mettere in imbarazzo avversari ricchi e influenti. Nel processo il gruppo aveva abbandonato molte delle cautele morali che avevano caratterizzato l'hacktivismo di cDc e Anonymous, abbracciando un hacking volutamente distruttivo che non aveva problemi a colpire anche vittime che gli stessi perpetratori consideravano innocenti. Nel rivelare i dati personali (mal) custoditi da Sony, Fox e altri, LulzSec rivelava la vulnerabilità dei loro sistemi informatici e la loro incapacità o mancanza di volontà di proteggere la privacy dei loro clienti. Ma al contempo danneggiava i clienti stessi, rendendo pubbliche le loro informazioni personali. Sabu, Topiary, Kayla, tflow, i membri più in vista di LulzSec, sembravano rappresentare, agli occhi delle comunità hacker, un ritorno alle glorie degli anni Novanta, quando celebrità come Kevin Mitnick tenevano in scacco le autorità federali e ammaliavano i media. In realtà rappresentavano un ritorno a come i media avevano ritratto gli hackers negli anni Novanta: il criminale misterioso e semi-anarchico, il vandalo tanto capriccioso quanto onnipotente nella sua simbiosi con la tecnologia, raccontato dai giornali a partire dalla fine degli anni Ottanta, si era infine materializzato.

242 *Back Orifice Windows Remote Administration Tool*, in «Cult of the Dead Cow», https://web.archive.org/web/19981205143320/http://www.cultdeadcow.com/tools/bo.html.

243 The Deth Vegetable, *Running a Microsoft Operating System on a Network? Our Condolences*, in «Cult of the Dead Cow», https://web.archive.org/web/19981205234956/http://www.cultdeadcow.com:80/news/back_orifice.txt.

244 M. Stutz, *Back Orifice Goes Forth*, in «Wired», 7 agosto 1998, https://web.archive.org/web/20201215010625/https://www.wired.com/1998/08/back-orifice-goes-forth/.

245 M. Ritchel, *Hacker Group Says Program Can Exploit Microsoft Security Hole*, in «The New York Times», 4 agosto 1998,

https://web.archive.org/web/20210922115503/https://archive.nytimes.com/www.nytimes.com/library/tech/98/08/cyber/articles/04hacker.html.

246 Registrazione della conferenza scaricata attraverso torrent.

247 J. Menn, *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World*, PublicAffairs, New York 2019; T. Jordan, P. Taylor. *Hacktivism and Cyberwars: Rebels with a Cause?*, Routledge, London 2004, pp. 97-115.

248 Citato in Menn, *Cult of the Dead Cow*, cit., p. 67.

249 Oxblood Ruffin, *Hacktivism, From Here To There*, https://web.archive.org/web/20120402161141/http://lawmeme.law.yale.edu/static/pastevents/digitalcops/papers/ruffin_hacktivism.pdf.

250 Art. 19: «Ogni individuo ha diritto alla libertà di opinione e di espressione, incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere».

251 Un archivio amatoriale di pagine «defaced» tra il 2001 e il 2013 mostra vari esempi della pratica, offrendo alcune statistiche. Se queste sono da credersi, la grande maggioranza dei 15.000 siti presi in considerazione appartengono a siti governativi o di corporations statunitensi. Le pagine riprodotte nell'archivio vedono una maggiore frequenza di siti governativi cinesi nei primi anni Duemila, forse per effetto della campagna cDc. *Attrition Defacement Mirror*, https://web.archive.org/web/20211101074752/https://attrition.org/mirror/attrition/.

252 *The Hacktivismo Declaration*, in «Cult of the Dead Cow», 4 luglio 2001, https://web.archive.org/web/20010802051308/http://www.cultdeadcow.com/cDc_files/declaration.html.

253 *The Hacktivismo Enhanced-Source Software License Agreement*, in «Hacktivismo», https://web.archive.org/web/20040805164456/http://hacktivismo.com/about/hessla.php.

254 *The HESSLA's Problems*, in «GNU Operating System», https://web.archive.org/web/20121224022628/https://www.gnu.org/licenses/hessla.en.html.

255 Oxblood Ruffin, *Hacktivism*, cit.

256 P. Ferdin, *Into the Breach*, in «The Washington Post», 4 aprile 1998, https://web.archive.org/web/20151024042715/https://www.washingtonpost.com/archive/politics/1998/04/04/into-the-breach/8ae3cf86-fbd7-4037-a1b6-842df39d9db7/.

257 *Weak Computer Security in Government: Is the Public at Risk? Hearing before the Committee on Governmental Affairs United States Senate*, U.S. Government Printing Office, Washington 1998, p. 22.

258 Ivi, p. 75. Per «can do attitude» si intende un atteggiamento di possibilismo ottimista, che spinge all'azione anche a scapito delle difficoltà.

259 Ivi, p. 36. L'episodio cui si fa riferimento è quello del patriota americano che nel 1775, durante la Rivoluzione, aveva dato l'allarme agli insorti avvisandoli dell'attacco delle truppe britanniche alla cittadina di Concord, sede del quartier generale degli insorti in Massachusetts.

260 Il *Patriot Act* dell'ottobre 2001 ampliava significativamente i poteri del governo federale nel campo della sorveglianza e della sicurezza dei networks. In particolare permetteva il controllo dei sistemi di comunicazione informatica da parte delle autorità anche senza un mandato, ma solo con il consenso della potenziale vittima.

261 Deformazione di LOL («laughing out loud», ridere a voce alta), espressione che indica scherzo o divertimento negli scritti online. Lulz assume nel tempo un significato più aggressivo, in quanto divertimento fine a sé stesso, dai tratti surreali, spesso a spese di qualcun altro.

262 Citato in Coleman, *Hacker, Hoaxer*, cit., p. 55.

263 Ivi, p. 156.

264 Anonymous, *Who is Anonymous or How To Troll the Media for Fun and Profit*, in «2600. The Hacker Digest», vol. 28, 2011, p. 23.

265 *Ibid.*

266 T. Bazzichelli, *Networked Disruption: Rethinking Oppositions in Art, Hacktivism and the Business of Social Networking*, DARC-Digital Aesthetics Research Center, Aarhus 2013, p. 146.

267 Il riferimento è a un passo dei Vangeli, nel quale un uomo posseduto da un demone afferma, nella versione di Marco (5,9), «Il mio nome è Legione, perché siamo molti».

268 *Message to Scientology*, 2008, https://www.youtube.com/watch?v=JCbKv9yiLiQ.

269 P. Olson, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*, Little, Brown and Company, New York 2012, p. 47.

270 *US Says Wikileaks Could 'Threaten National Security'*, in «BBC News», 26 luglio 2010, https://web.archive.org/web/20160130101950/http://www.bbc.com/news/world-us-canada-10758578.

271 Si veda ad esempio N. Cohen, *Web Attackers Find a Cause in WikiLeaks*, in «The New York Times», 9 dicembre 2010, https://web.archive.org/web/20220413122718/https://www.nytimes.com/2010/12/10/world/10wiki.html.

272 Coleman, *Hacker, Hoaxer*, cit., pp. 147 e 192.

273 Il gruppo fu, ad esempio, l'unico citato dal rapporto NATO su informazione e sicurezza internazionale della primavera del 2011,

https://web.archive.org/web/20110603224942/http://www.nato-pa.int/default.asp?SHORTCUT=2443.

274 *50 Days of Lulz*, in «pastebin.com», 25 giugno 2011, https://web.archive.org/web/20110701120214/https://pastebin.com/1znEGmHa.

275 https://web.archive.org/web/20110703170926/http://lulzsecurity.com/.

276 Coleman, *Hacker, Hoaxer*, cit., pp. 256-264.

277 *Awakenings*, in «2600. The Hacker Digest», vol. 28, 2011, pp. 130-131.

Conclusione.
L'esplosione dell'hacking

Nel 2015 un attacco attraverso phishing e malware riusciva a guadagnare accesso ai computer di diverse compagnie elettriche ucraine. Per la prima volta uno spauracchio che era stato agitato dai media almeno fin dagli anni Novanta infine si materializzava: buona parte della rete elettrica del paese fu messa fuori uso per svariate ore[278]. Ma il responsabile di questo hack non era un gruppo di ragazzini prodigio o di cyber-criminali. Secondo la maggior parte degli esperti l'attacco era il culmine di una campagna di *cyberwarfare* condotta dalla Russia fin dall'invasione della Crimea del 2014. Il gruppo hacker che aveva lanciato l'attacco si chiamava Sandworm ed era parte integrante delle forze di intelligence russe. Negli anni successivi lo stesso gruppo sarebbe stato ritenuto responsabile di un tentativo di intromissione nelle elezioni francesi del 2017, di un nuovo attacco contro l'Ucraina attraverso un virus chiamato NotPetya[279] e del tentato sabotaggio del sistema informatico delle Olimpiadi invernali coreane nel 2018, per protesta contro l'esclusione degli atleti russi[280].

I libri di storia ricorderanno il 25 febbraio 2022 come la data di inizio dell'invasione russa dell'Ucraina. In realtà, come fa notare un rapporto Microsoft dell'aprile 2022, la guerra è iniziata il giorno prima, quando Sandworm ha rilasciato FoxBlade – un trojan usato per condurre attacchi DDoS e cancellare dati dai computer infettati – contro centinaia di computer governativi e aziendali ucraini, con lo scopo di raccogliere informazioni e indebolire le infrastrutture del paese. Nei giorni successivi ogni passo dell'esercito russo sul terreno sarebbe stato accompagnato da un parallelo avanzamento nel cyberspazio. Quando, il 1° marzo, missili russi colpivano l'antenna di Kyiv TV, operatori russi

sabotavano i networks digitali delle compagnie di media ucraine. La conquista russa della centrale nucleare di Zaporižžja era preparata da un'intrusione nei suoi sistemi informatici. L'attacco ai centri abitati era invariabilmente preceduto dall'attacco alle infrastrutture digitali dei loro organi governativi. Lo stesso rapporto Microsoft individua, a partire dagli attacchi osservati, l'esistenza di almeno sette gruppi legati ai servizi militari e di spionaggio russi, ognuno con compiti specifici, dalla distruzione di dati al phishing, dall'esplorazione di vulnerabilità informatiche al furto di informazioni e dati[281].

La Russia non è ovviamente l'unico Stato ad aver incluso tecniche hacker all'interno del proprio arsenale bellico e di intelligence. L'era del così detto «hacking di Stato» si è aperta anzi nel 2010, quando un worm chiamato Stuxnet mise in ginocchio il programma nucleare iraniano, rendendo inservibile la centrale di Natanz. La complessità del worm, la precisione dei suoi bersagli (il virus ignorava tutti i computer che non avevano l'esatta configurazione software dei computer della centrale iraniana) e le conoscenze tecniche necessarie al suo funzionamento (Stuxnet aumentava la velocità di rotazione delle centrifughe della centrale a intervalli regolari, deteriorandole senza comportare rischi di fissione e senza destare l'attenzione degli operatori)[282] fecero immediatamente pensare a uno sforzo finanziato da formazioni statali. Molti, e tra questi il *whistleblower* Edward Snowden[283], hanno puntato il dito verso gli Stati Uniti e Israele. Il Center for Strategic and International Studies, che dal 2006 tiene traccia dei maggiori attacchi hacker su scala globale, conta, tra il luglio 2021 e il giugno 2022, 118 attacchi, nella grandissima parte attribuiti a formazioni statali e condotti contro obiettivi strategici quali agenzie governative, personaggi politici, aziende mediatiche e centrali energetiche. Indubbiamente non si tratta che della punta di un iceberg che gli attori coinvolti (Cina, Stati Uniti e Russia in particolare) sono riluttanti a vedere emergere nella sua completezza di fronte all'attenzione pubblica[284].

Il 7 maggio 2021 uno dei principali oleodotti statunitensi, il Colonial Pipeline, smise improvvisamente di funzionare. In poche ore le pompe di benzina del Sud-Ovest degli Stati Uniti erano a secco, anche a causa del panico degli automobilisti, che facevano a gara per riempire i serbatoi

prima della chiusura totale. Il traffico aereo della zona, dipendente dalle forniture dell'oleodotto, andò in tilt. Il 9 maggio l'amministrazione Biden dichiarò lo stato di emergenza. L'oleodotto sarebbe rientrato in funzione il 12 maggio.

Pochi giorni dopo, il 30 maggio, i macelli del più grande produttore di carne statunitense, JBS Foods, andarono fuori uso, creando disagi nella distribuzione dei prodotti non solo negli Stati Uniti, ma anche in Canada e in Australia, e agitando lo spettro di un rialzo dei prezzi della carne a livello globale. In pochi giorni i macelli ripresero le operazioni.

Si tratta di due esempi di un fenomeno oggi dilagante: l'estorsione digitale. Entrambe le ditte erano state vittime di un ransomware, un virus disegnato per rendere inaccessibili i dati su un computer o su un network fino a che la vittima non abbia pagato un riscatto. Nel caso di Colonial Pipeline il ransomware non aveva toccato i software che regolavano il flusso di benzina, ma quelli che regolavano i pagamenti. Incapace di richiedere il compenso per il carburante inviato e timorosa di un dilagare dell'attacco ad altre infrastrutture informatiche, era stata la stessa Colonial a decidere la chiusura dell'impianto. Il responsabile era un gruppo chiamato DarkSide. JBS era stata invece attaccata da un gruppo che si firmava REvil. Entrambi hanno con tutta probabilità sede in Russia.

La relativa velocità con la quale entrambe le situazioni sono state risolte è dovuta al fatto che le ditte hanno pagato, nel giro di poche ore, quanto richiesto (75 bitcoin – equivalenti a 5 milioni di dollari al tempo – nel caso di Colonial, 11 milioni nel caso di JBS), ma anche al fatto che i gruppi non sono alle dirette dipendenze di uno Stato. La Russia ed altri Stati possono tollerarne la presenza, e presumibilmente si rallegrano quando la vittima è un avversario geopolitico, ma i perpetratori puntano solo al profitto. Restituire prontamente i dati al pagamento del riscatto dimostra alla prossima vittima che pagare conviene, massimizzando le probabilità di successo dell'estorsione. DarkSide è arrivata persino a scusarsi pubblicamente dei disagi causati alla popolazione.

Anche in questo caso non si tratta che della punta di un iceberg, emersa all'attenzione pubblica solo per la scala delle conseguenze degli attacchi. Le vittime di ransomware sono oggi aziende di ogni dimensione e anche individui, che si trovano davanti alla scelta se pagare il riscatto o impiegare fondi potenzialmente maggiori per riparare al danno – senza

alcuna certezza sul fatto che i dati saranno effettivamente recuperati, ma con la certezza di dover ammettere pubblicamente una falla nei propri sistemi di sicurezza. I termini della scelta, uniti all'emergere delle criptovalute, che permettono il pagamento non tracciabile del riscatto, hanno determinato tanto la straordinaria diffusione della pratica quanto la mancanza di statistiche precise su di essa. I ransomwares sono tuttavia citati nel *Global Cybersecurity Outlook 2022* del World Economic Forum come la principale minaccia informatica, insieme al social engineering, alle imprese e alla crescita industriale, con una stima di diffusione di 270 attacchi per azienda nel 2021[285]. L'agenzia di sicurezza informatica SonicWall ha registrato nello stesso anno e tra i clienti da essa monitorati 623 milioni di attacchi ransomware in tutto il mondo, un numero quasi raddoppiato rispetto all'anno precedente e triplicato rispetto al 2019[286].

Sebbene un lontano accenno alla tradizione hacker statunitense raccontata in questo libro in alcuni casi permanga (Sandworm è per esempio un riferimento al libro di fantascienza *Dune*, DarkSide a *Star Wars* e forse a Kevin Mitnick, social engineering è ovviamente un'espressione di origine hacker), il così detto «hacking di Stato» e la cyber-estorsione hanno poco a che vedere con la definizione di hack che ci ha finora guidato. Laddove questa mette al centro la capacità del rapporto tra individuo e tecnologia di creare una comunità, l'hacking di Stato deve essere interpretato attraverso la lente della storia e della cultura militare e dei servizi di intelligence. L'uso di ransomwares è probabilmente più comprensibile all'interno della storia della criminalità organizzata che non come parte della storia delle culture tecniche[287]. Questa differenza è ben percepita dagli addetti ai lavori: il citato rapporto di Microsoft sulla guerra digitale in Ucraina fa uso esteso di termini che appaiono in questo libro e che sono nati dalla cultura hacker (malware, worm, cyberspazio…). Ma le parole hacker o hacking non appaiono mai.

Discorso diametralmente opposto si deve fare per i mezzi di informazione generalisti. Relativamente pochi episodi di ransomware finiscono sulle pagine dei giornali, ma quando lo fanno, come nel caso degli attacchi a JBS Foods e Colonial Pipeline, i responsabili sono invariabilmente descritti come hackers. Almeno dal 2010 i media hanno usato la parola hacking per indicare azioni ostili tra Stati che avvenivano

nel dominio digitale. Si tratta di un nuovo volto pubblico dell'hacker, pur preparato dal ruolo globale assunto da gruppi indipendenti come Anonymous: non più ragazzo prodigio, accademico, imprenditore, troll o attivista, ma sabotatore e spia professionista. Per sapere quanto questa rappresentazione mediatica sia accurata occorre studiare la composizione di gruppi come Sandworm, REvil e DarkSide, e la storia e le motivazioni degli individui che ne fanno parte: un compito arduo e importante, ma che va al di là delle ambizioni di questo libro.

La preminenza dell'hacking di Stato sui quotidiani non significa che altre forme di hacking siano scomparse, o che la parola hack sia tornata ad assumere un significato esclusivamente negativo. Al contrario, si è assistito, nell'ultimo decennio, a una vera e propria 'esplosione' dell'hacking. Aziende e istituzioni organizzano periodicamente «hackathons», competizioni nelle quali diversi individui si applicano alla risoluzione di uno stesso problema tecnico. Il Maker Movement ha raccolto, a partire dal primo decennio del millennio, elementi centrali dell'etica e delle pratiche hacker, con un rinnovato accento sulla modifica delle tecnologie non informatiche e con la creazione di «makerspaces» direttamente ispirati ai luoghi di incontro hacker[288]. La parola hack è stata usata in relazione alla biologia (*biohackers*: amatori che si dilettano in esperimenti di biologia e nella modifica «fai da te» del codice genetico)[289], a trucchi di economia domestica (*life hacking*: l'uso di espedienti per rendere più efficienti compiti e attività quotidiani, dalla cucina alla vita sentimentale)[290] e persino ai mobili Ikea (*Ikea hacking*: la pratica di modificare i prodotti dell'azienda svedese per personalizzarli o trasformarli)[291]. Più in generale, l'influenza delle culture hacker è evidente (ma da molti ignorata) in svariati fenomeni centrali alla modernità digitale. Wikipedia, probabilmente il più importante strumento di diffusione della conoscenza oggi esistente, fa uso del modello di lavoro «crowd-based» che è stato per la prima volta sperimentato dalle comunità Free Software e Open Source. Le licenze Creative Commons sono direttamente ispirate dalla GPL di Stallman e dalle licenze Open Source. I concetti di Open Access e Open Science[292], entrambi adottati come linee guida delle politiche di finanziamento alla ricerca dell'Unione Europea, si rifanno a una filosofia di libero accesso

all'informazione in rete che ha visto gli hackers come primi e più insistenti proponenti. La subcultura hacker, che – come si è accennato nell'Introduzione – è stata per decenni difficile da assorbire nella cultura mainstream in virtù dei suoi elementi tecnici, è stata infine assimilata. Quando parlo di «esplosione» dell'hacking non voglio perciò alludere soltanto alla sua diffusione, ma anche alla sua frammentazione in fenomeni a volte molto diversi tra loro. Sebbene tutte le pratiche sopra elencate siano legate più o meno strettamente alle culture tecniche statunitensi del Novecento, nessuna può a pieno titolo rientrare nella definizione di cultura hacker per come è stata qui raccontata. Per questo ho deciso di concludere il volume con Anonymous, dopo aver a lungo meditato se fosse il caso di escluderlo del tutto: si tratta di un gruppo definito come hacker, che mostra evidenti caratteristiche legate alla tradizione hacker (in particolare le forme della comunicazione mediatica), ma che, in virtù delle modalità estremamente aperte di adesione, segna una svolta rispetto all'economia della reputazione e alla centralità del virtuosismo tecnico che avevano caratterizzato i suoi predecessori novecenteschi.

La definizione che abbiamo finora usato probabilmente non è più sufficiente, dunque, per esplorare le diverse forme che l'hacking ha assunto nel nuovo millennio. Ciò non vuol dire che essa sia inutile per comprenderle. Al contrario, ci ha permesso di evidenziare fenomeni storico-culturali che ritengo fondamentali per spiegare tanto il successo dell'idea contemporanea di hacker quanto parti importanti dell'odierna «cultura digitale».

Primo tra tali fenomeni è il rapporto simbiotico tra culture tecniche e media «tradizionali». Come si è visto, tutti i gruppi qui raccontati donavano longevità e significato ai propri incontri immateriali attraverso la materialità di tradizionali riviste cartacee. Scritte da appassionati per appassionati, le riviste – che sono state la fonte principale di questo saggio – non si limitavano a informare: esse creavano la comunità, tracciavano i suoi limiti, sancivano i comportamenti ed elevavano alcuni praticanti al rango di modelli e celebrità. Ancora più profondo e pregno di conseguenze era il rapporto con i media «mainstream». Le diverse caratterizzazioni mediatiche che ho raccontato non hanno avuto conseguenze solo sull'opinione pubblica o sulla natura degli interventi

legislativi, ma anche sulle stesse comunità hacker, che in svariati casi si adeguavano alla rappresentazione che di esse era fatta. Come la fantascienza influenza l'immaginario tecnologico, ispirando in alcuni casi l'innovazione nel mondo reale, così le paure e gli interessi commerciali dei media influenzano il percorso delle comunità hacker e il significato che la pratica di volta in volta assume per i loro membri.

Il secondo fenomeno riguarda le forme della comunicazione politica. Lo stile del monkey theatre è diventato talmente diffuso sui social networks da sembrare una parte inevitabile e quasi naturale del comportamento online, ma, come si è visto, esso ha una storia di più lunga data, che inizia con la riflessione su come un gruppo minoritario e di nicchia possa guadagnare l'attenzione del sistema mediatico. Lo scherzo come forma di comunicazione politica, la conferma e amplificazione delle aspettative, delle paure e dei pregiudizi dei media e dell'opinione pubblica, l'esagerazione della minaccia rappresentata dalle proprie capacità e attività, fanno parte di un «hacking sui media» che, teorizzato e messo in pratica dalle culture tecniche lungo il corso del secondo Novecento, ha avuto e sta avendo, nel difficile mercato dell'attenzione online, un successo strepitoso. I due fenomeni, insieme, descrivono una sorta di 'co-creazione' delle culture hacker da parte dei media e dei praticanti stessi, un processo fatto di reciproci tentativi di manipolazione che, se non ebbero mai successo nell'imporre alla controparte la propria interpretazione della pratica, hanno in qualche misura modificato le rappresentazioni di entrambi.

In ultimo vi è il legame «genealogico» che il computer hacking intrattiene con altre culture tecniche nate prima di esso. L'hacking è parte di una tecnocultura che è perfettamente riconoscibile in alcune caratteristiche fondamentali (il rapporto privilegiato e creativo tra giovane e tecnologia; il ruolo del singolo individuo e dell'amatore nell'innovazione tecnologica; gli stereotipi legati al genere, all'apparenza fisica e alle capacità sociali del giovane genio) fin dal XIX secolo. Se l'hacking ha mantenuto, nel corso dei decenni, il proprio fascino misterioso e la propria centralità nel discorso pubblico, è stato anche in virtù del suo essere insediato in profondità nella cultura statunitense, ora reinterpretata in chiave globale.

Anche in ragione delle molteplici forme e implicazioni che ha assunto

l'hacking contemporaneo, gli storici dovranno, in un prossimo futuro, inoltrarsi nel territorio ancora largamente sconosciuto delle culture tecniche che hanno creato il nostro presente digitale. Le culture hacker in Italia, in Europa e nel resto del mondo, il rapporto tra hacking e culture tecniche non legate ai mezzi di comunicazione, la creazione di identità e comunità in mancanza di compresenza fisica, l'idea di innovazione in ambito digitale, sono solo alcuni dei temi che, studiati a volte da altre discipline, ancora attendono una prospettiva storiografica e diacronica. La storia raccontata in questo libro non è che un inizio.

278 R. Lee, M. Assante, T. Conway, *Analysis of the Cyber Attack on the Ukranian Power Grid*, 2016, https://web.archive.org/web/20220412145716/https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.

279 Al contrario di un normale ransomware, che crittografa i dati su un computer e li rende inutilizzabili fino a che il proprietario non paghi un riscatto, NotPetya era disegnato per crittografare i dati in maniera irreversibile.

280 A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, New York 2019.

281 Microsoft Digital Security Unit, *Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine*, 27 aprile 2022, https://web.archive.org/web/20220718075027/https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

282 A. Van Dine, *After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities*, in *Project on Nuclear Issues: A Collection of Papers from the 2016 Nuclear Scholars Initiative*, a cura del Center for Strategic and International Studies, 2017, pp. 101-114.

283 *Whistleblower* (letteralmente «chi soffia in un fischietto», come a dare l'allarme) indica un individuo che, interno a un'organizzazione, ne denuncia il comportamento illegale o immorale. Snowden, ex impiegato della National Security Agency, ha denunciato nel 2014 la sorveglianza illegittima, da parte del governo statunitense, di cittadini e governi.

284 *Significant Cyber Incidents*, a cura del Center for Strategic and International Studies, https://web.archive.org/web/20220718094005/https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

285 World Economic Forum, *Global Cybersecurity Outlook 2022*, gennaio 2022, p. 13,

https://web.archive.org/web/20220718110524/https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

286 *2022 SonicWall Cyber Threat Report*, 2021, pp. 29-31.

287 M. Ryan, *Ransomware Revolution: The Rise of a Prodigious Cyber-Threat*, Springer, Cham 2021, cap. 9.

288 M. Hatch, *The Maker Movement Manifesto: Rules for Innovation in the New World of Crafters, Hackers, and Tinkerers*, McGraw-Hill Education, New York 2013.

289 A. Delfanti, *Biohackers: The Politics of Open Science*, Pluto Press, London 2013, cap. 6.

290 J.M. Reagle, *Hacking Life: Systematized Living and its Discontents*, The MIT Press, Cambridge (Mass.) 2019.

291 *Ikeahackers.net*, https://web.archive.org/web/20220413164811/https://ikeahackers.net/.

292 Con la prima espressione si intende il libero accesso, da parte della comunità scientifica e della popolazione, agli scritti e ai dati prodotti dall'accademia; con la seconda si intende la partecipazione, permessa dal libero accesso al sapere, dei cittadini e dei portatori di interesse al processo di innovazione scientifica e tecnologica.

Glossario

4chan Forum online fondato nel 2008, nel quale tutti i contributori sono anonimi.

ARRL American Radio Relay League (vedi cap. 1).

Beta testing Stadio dello sviluppo del software nel quale il suo corretto funzionamento è verificato da un numero limitato di utenti.

Black hat hacker Hacker che pratica l'attività per profitto o con cattive intenzioni.

Botnet Rete di computer controllati da remoto da un unico utente, spesso usati per attacchi DDoS.

Bulletin Board System (BBS) Forum online accessibile via modem che permetteva, sin dai primi anni Ottanta, lo scambio di messaggi e files attraverso la linea telefonica. Precursore dei moderni *fora* web.

Bug Errore in un software che ne impedisce il corretto funzionamento.

Codice Morse Alfabeto che codifica lettere e numeri in segnali, elettrici o sonori, più o meno lunghi, detti punti e linee. Inventato da Samuel Morse attorno al 1837.

Cracker Hacker che si intromette illegalmente in sistemi informatici.

Crowdsourcing Pratica di delegare a un largo numero di persone l'adempimento di un compito (scrittura di un codice, creazione di un archivio, trascrizione di manoscritti...), generalmente tramite la rete.

DDoS (Distributed Denial of Service) Attacco DoS che proviene da diverse fonti, come i computer connessi in una botnet.

Defacing Pratica di alterare illecitamente un sito web dopo aver guadagnato i privilegi di amministratore su di esso.

Denial of Service (DoS) Interruzione di un servizio a causa di un attacco informatico, generalmente attraverso il sovraccarico delle risorse necessarie al suo adempimento.

Doxing L'atto di rivelare le informazioni riservate di una persona, spesso per esporla a molestie online.

Dumpster diving È la pratica di scandagliare la spazzatura alla ricerca di informazioni riservate o di materiali che possano essere riutilizzati nella costruzione di apparecchi elettronici.

DXing Tentativo di comunicare, via radio amatoriale, con stazioni il più lontano possibile.

Exploit Software pensato per avvantaggiarsi di una vulnerabilità di un altro software.

GNU (General Public License) Licenza, congeniata dalla Free Software Foundation, che

garantisce il diritto di leggere e modificare il codice da essa protetto.

Hackerspace Luogo fisico nel quale gli hackers possono lavorare collettivamente e scambiarsi idee, scoperte e innovazioni.

Hacking di Stato Hacking sponsorizzato da uno Stato o direttamente integrato nei suoi servizi militari o di intelligence.

IP spoofing Pratica di falsificare il codice che identifica un computer in maniera univoca in un network (IP address) per aggirare controlli di sicurezza su di esso basati.

Mainframe Nome colloquiale dei primi enormi computer commercializzati dagli anni Cinquanta agli anni Ottanta. Il termine è oggi usato per indicare supercomputer, ugualmente ingombranti ma estremamente più potenti, usati in ambito aziendale e universitario.

Malware Codice che ha intento maligno (furto o distruzione di dati, accesso non autorizzato, spionaggio...).

Meme In ambito digitale, un artefatto (immagine, GIF, video...), o un'idea, che si diffonde ed è riprodotto o modificato in diverse comunità online. Spesso è ironico e basato su elementi della cultura popolare (film, eventi di attualità, celebrità...).

Network distribuito Network nel quale ogni nodo ha la stessa importanza e nel quale un messaggio può intraprendere diverse strade per raggiungere la medesima destinazione.

Onde corte Parte della banda radio fra i 3 e i 30 MHz. Inizialmente ritenute inutili per la comunicazione, acquistarono importanza con la scoperta che esse sono riflesse dalla ionosfera e possono così raggiungere distanze considerevoli.

OSI Open Source Initiative (vedi cap. 6).

Patch Codice aggiunto a un programma preesistente per correggere bugs o modificarne le funzionalità.

Phishing Tentativo di carpire informazioni riservate attraverso messaggi che vogliono apparire come provenienti da istituzioni o da persone fidate per il destinatario. La parola deriva da «fishing» (pescare). La sostituzione di f in ph è un chiaro riferimento al phreaking.

Ransomware Software che crittografa i dati su un computer altrui, impedendo l'uso da parte del legittimo proprietario fino a che questi non abbia pagato un riscatto al perpetratore.

Script kiddie (Skiddie) Individuo che usa codice sviluppato da altri per ottenere i risultati di un hack.

Social engineering L'insieme delle tecniche necessarie a sfruttare in maniera illecita l'elemento umano di un sistema tecnologico.

SQL injection Inserimento illecito di codice all'interno di un database (spesso online) per ottenere accesso o controllo su di esso.

Trojan horse Software programmato per non essere rilevato dal computer su cui opera, spesso con l'obiettivo di garantire l'accesso o il controllo sul computer stesso.

Troll Chi fa *trolling*. Originariamente un orco nel folklore scandinavo e nell'immaginario della letteratura fantasy.

Trolling È la pratica di partecipare a discussioni online con l'obiettivo di indispettire, tormentare o scandalizzare i propri interlocutori.

UNIX Sistema operativo sviluppato da Bell Labs a partire dal 1969. Primo sistema operativo capace di funzionare su più macchine.

Webmaster È il principale gestore e responsabile dell'inserimento di contenuti all'interno di un sito web.

White hat hacker Hacker che pratica la propria attività per svelare vulnerabilità informatiche e non per avvantaggiarsene.

Worm Programma che può fare copie di sé stesso e installarsi su altri computer, spesso all'insaputa del suo proprietario.