

DAVIDE BENNATO

CULTURE TECNOLOGICHE EMERGENTI.
ANALISI DI UNA COMUNITÀ DI *WARDRIVERS**

Con il termine *wardriver* si definisce un particolare tipo di utente di tecnologie informatiche dedito all'attività del *wardriving*, ovvero la pratica di intercettare e penetrare nelle reti di computer senza fili (reti wireless) tramite un monitoraggio del territorio effettuato attraverso un computer portatile appositamente predisposto¹. La sessione di *wardriving* consiste nell'andare in giro in automobile nello spazio urbano portando con sé l'apparecchiatura per il *wardriving* e identificando le reti che vengono così rilevate (Bennato 2004; Ryan 2004; Sandvig 2004).

Definita in questo modo è evidente che la comunità in questione è una variante della più ampia comunità degli hacker con cui condivide organizzazione sociale, strategie d'uso della tecnologia e norme etico/deontologiche.

Lo scopo del saggio è quello di delineare il profilo di una comunità di *wardriver* italiani attraverso un'analisi della cultura hacker e riportare i risultati di una ricerca etnografica svolta tra dicembre 2004 e aprile 2005.

* La corretta citazione del presente saggio è la seguente: Bennato, D., 2008, *Culture tecnologiche emergenti. Analisi di una comunità di wardrivers*, in M. Santoro, a cura, *Cultura in Italia. Nuovi media, vecchi media*, Il Mulino, Bologna, pp.75-98.

¹ Il termine nasce dalla crasi di *war* (guerra) e *driving* (guida dell'automobile). Il riferimento alla guerra non ha niente a che fare con l'aspetto bellico, ma è una citazione dell'immaginario cinematografico. Infatti il film che ha mostrato al grande pubblico gran parte delle tecniche hacking a cui il *wardriving* si ispira è *War Games* (John Badham, USA, 1983).

1. *La comunità hacker*

1.1 *La definizione di hacker*

È piuttosto difficile dare una definizione stringente di cosa debba intendersi con “hacker”, in quanto non solo questa etichetta nel corso della sua storia ha definito comunità diverse (Levy 1984; Sterling 1992; Hannemyr 1999), ma anche all’interno della comunità che si riconosce in questa definizione ci sono stati diversi slittamenti di significato (Chandler 1996; Nissenbaum 2004).

Ai fini della nostra analisi preferiamo dare una definizione operativa di questo termine che faccia riferimento alla teoria del modellamento sociale della tecnologia (*Social Shaping of Technology*, cfr. Williams e Edge 1996; Mackenzie e Wajcman 1999) in quanto considera l’utente della tecnologia come un utente attivo. Per fare ciò utilizzeremo il concetto di appropriazione (Mackay e Gillespie 1992) poiché non solo è quello che rende meglio l’atteggiamento hacker nei confronti della tecnologia ma anche perché permette di superare l’*impasse* di analizzare il computer come tecnologia o come *medium*. Infatti l’appropriazione deve moltissimo agli studi sull’uso sociale delle tecnologie della comunicazione (Silverstone, Hirsch e Morley 1991).

Definiamo l’hacker come un utente che mette in atto specifiche strategie di appropriazione della tecnologia informatica seguendo norme definite dalla comunità di appartenenza (etica hacker).

Il riferimento alla componente etica non sembri fuori luogo in quanto è uno dei pochi elementi di stabilità della comunità hacker.

Queste strategie prendono il nome di *hack*. Il termine ha un’origine chiara – le prime comunità di appassionati di tecnologia del Mit (*Massachusetts Institute of Technology*) di Boston degli anni ’60 – ma un’interpretazione controversa. In estrema sintesi potremmo considerare gli *hack* una modalità d’uso della tecnologia (prevalentemente informatica) che necessita di una robusta competenza tecnica al limite col virtuosismo, è fortemente creativa ed usa un approccio per tentativi ed errori (Levy 1984; Turkle 1984; Hannemyr 1999; Nissenbaum 2004).

Prima di entrare in dettaglio sulle caratteristiche sociali della comunità hacker, è bene analizzare i processi che hanno trasformato il termine in un sinonimo della parola “pirata informatico”, altrimenti si rischia un’ambiguità che renderebbe, se non vano, quantomeno opaco

il nostro tentativo di comprendere le caratteristiche salienti della comunità hacker e wardriver.

L'immagine dell'hacker non ha mai goduto di una buona fama (Thomas 2005). Paradossalmente mentre la letteratura di fantascienza che ha fatto propria la figura dell'hacker (per esempio: Gibson 1996) lo ha sempre dipinto come un anti-eroe dalle connotazioni positive (cfr. Caronia e Gallo 1997), i media hanno sempre tratteggiato l'hacker come un pericoloso criminale informatico (Taylor 1999; Thomas 2002; Turgeman-Goldschmidt 2005). La sovrapposibilità del concetto hacker/criminale può essere considerata come risultato di una vera e propria *escalation* negativa: programmatore compulsivo (Weizenbaum 1976), nemico della società dell'informazione (Halbert 1997), terrorista elettronico (Reed 2002), drogato di tecnologia (Thomas 2004), virus della società dell'informazione (Nissenbaum 2004).

Storicamente il termine «hacker» ha avuto una connotazione fortemente positiva volta a definire ora il “mago” dei computer in grado di far fare alla macchina praticamente qualsiasi cosa (Thomas 2005), ora l'appassionato in grado di trovare soluzioni creative a problemi complessi (Hannemyr 1999). Inoltre l'ideologia alla base della cultura hacker è diventata una fucina di idee che una volta superate i confini della comunità, hanno dato vita a progetti assolutamente innovativi: la nascita del personal computer (Bennato 2002), lo sviluppo tecnico di internet (Hafner e Lyon 1996), Linux e il progetto *Open Source* (Berra e Meo 2001), il progetto *Creative Commons* per una nuova idea di copyright (Lessig 2004).

La stampa si accorge di un nuovo universo da esplorare, quello di internet e delle nuove tecnologie informatiche, e per raccontarlo inventa nuovi generi giornalistici come la caccia all'hacker (Thomas 2004) o la descrizione di un tipo particolare di malati, i computer-fobici e i computer dipendenti (Reed 2002). Insomma l'hacker diventa protagonista di una forma di panico morale (Cohen 1980 applicato agli hacker da Thomas 2005 e da Wark 2006) che radicalizza la visione alterata che il grande pubblico ha della comunità.

Come risposta a questa situazione di normalizzazione dello spazio sociale delle reti e alle tattiche di controllo, la figura dell'hacker è stata soggetta a tutti gli effetti a un meccanismo di costruzione giuridica (Thomas 2002) una volta etichettato l'hacker come deviante, anche se il processo di etichettamento della devianza su internet sia una questione delicata e controversa (Denegri-Knott e Taylor 2005).

Beninteso non tutti gli hacker sono personaggi positivi così come non tutti i malintenzionati presenti in internet sono hacker, ma nonostante questa evidente difficoltà l'equazione "hacker uguale criminale" ha avuto molto successo, tanto da costringere la comunità a un necessario ripensamento del termine e delle sue caratteristiche. Nella lingua italiana il termine hacker viene declinato o in senso negativo (pirata, criminale) o in senso generico (nel senso di "smanettone", persona abile nelle tecnologie informatiche). Mentre per la prima accezione valgono i *caveat* di cui sopra, la seconda accezione è criticabile poiché essere un hacker vuol dire appartenere ad una precisa comunità, idea che si perde nella connotazione di "smanettone" (Di Corinto e Tozzi 2002).

1.2 L'organizzazione sociale della comunità hacker

Quella hacker è un tipo di comunità molto interessante poiché gode di un'organizzazione sociale notevolmente sofisticata con le sue riviste («Phrack», «2600», «Hacker Journal», «Slashdot»), le sue *convention* (*Defcon*, *Hackmeeting*), i suoi ideologi (tra gli altri Richard Stallman, Eric Raymond) e le sue reti di comunicazione (forum, newsgroup). Per comprendere l'estrema articolazione di questa cultura, bisogna ripercorrere rapidamente lo sviluppo storico della comunità poiché mentre l'ideologia alla base può essere considerata pressoché stabile, cambia il modo di intendere l'hacking per via del suo legame molto forte con la tecnologia. Al variare della tecnologia, si modificano di conseguenza le pratiche di appropriazione messe in atto dalla comunità (gli *hacks*) e quindi il modo con cui la cultura hacker si manifesta.

È difficile trovare un termine sociologico in grado di identificare correttamente l'organizzazione sociale della cultura hacker. Noi seguiremo i consigli di alcuni autori che sulla scorta di Anderson (1983) sono soliti parlare di quella hacker come una comunità immaginata (Jordan e Taylor 1998; Taylor 1999) per via della sua dispersione territoriale e per la possibilità per i membri di percepirsi come appartenenti a un gruppo. Altri invece preferiscono definire quella hacker come *computer underground* (Meyer 1989; Sterling 1992; Thomas 2005) in quanto questa etichetta definisce sia il legame con la tecnologia informatica che il suo essere sub-culturale. Anche se il termine sottocultura è quello più utilizzato per descrivere la comunità hacker, alcuni non lo considerano adatto poiché non rende giustizia alla creatività di questa cultura tecnologica (Thomas 2002).

Dal punto di vista più specificamente descrittivo, gli elementi che si riscontrano nelle comunità hacker sono i seguenti: tecnologia, segretezza, anonimato, appartenenza fluida, dominanza maschile, motivazioni (Jordan e Taylor 1998; Taylor 1999).

Come si diceva prima, la componente tecnologica della comunità hacker è quella più evidente in quanto è ciò che connota l'identità hacker. Il modo corretto di intendere il rapporto della comunità con la tecnologia è la capacità di uso creativo che si basa su una forte competenza tecnica.

La segretezza, invece, è relativa alla sanzione normativa che circonda la figura dell'hacker. Data l'illiceità – presunta o reale – delle pratiche di *hacking*, la segretezza è necessaria per proteggere chi appartiene alla comunità. In realtà il rapporto con la segretezza è ambiguo in quanto l'hacker deve trovare delle strategie per «firmare le proprie azioni, in modo da poter essere riconosciuto dai propri pari e guadagnare così prestigio nella comunità.

L'anonimato è relativo alle dinamiche di occultamento della propria identità sociale per evitare ripercussioni legali come conseguenza delle azioni di *hacking*. Di solito un meccanismo tipico per attivare questo occultamento è mettere in atto le pratiche di *hacking* usando un *nickname*, ovvero un nome fittizio che protegga l'identità sociale ma sia riconoscibile dai propri pari. La strategia di creazione di un *nickname* riguarda non solo i singoli hacker ma anche i gruppi più attivi: capita infatti che alcune azioni hacker particolarmente spettacolari siano attribuite a un'identità collettiva (per esempio: *Legion of Doom*, *Cult of the Dead Cow*).

L'appartenenza fluida è una caratteristica tipica della comunità hacker attribuibile a vari fattori. In primo luogo è dovuta al fatto che il mondo hacker (per via dell'etica che informa la loro organizzazione: vedi *infra*) ha poche barriere all'ingresso, quindi è (relativamente) facile sia entrarne che uscirne. In secondo luogo essere un hacker richiede una disponibilità di tempo che diminuisce all'aumentare dell'età, perciò è facile che si diventa hacker da adolescenti e poi via via se ne esce (con l'eccezione di chi diventa «hacker per lavoro come, poniamo, responsabile della sicurezza di un'azienda). In terzo luogo essere un hacker richiede una forte competenza tecnologica che necessita di un continuo aggiornamento sullo sviluppo dell'informatica: anche in questo caso il fattore tempo è cruciale.

La dominanza maschile è un altro tratto tipico della comunità. I processi di socializzazione e di costruzione sociale del genere sessuale, tradizionalmente, rendono più propensi gli uomini ad

appropriarsi della tecnologia rispetto alle donne (Faulkner 2000). Gli hacker intesi come cultura tecnologica non fanno eccezione a questa situazione, anche se in realtà sembrerebbe che le donne hacker pur essendo presenti, siano soggette a un meccanismo di controllo patriarcale che porta a sottodimensionare il ruolo che esse hanno nella comunità hacker (Adam 2005, 128-145).

Per quanto concerne le motivazioni alla base dell'hacking, molteplici sono le spinte individuali che sono state rilevate dalle ricerche empiriche. Le principali sono: la dipendenza dai computer (ovvero passione profonda per la tecnologia), lo stimolo della curiosità, la noia verso il sistema educativo e la conseguente eccitazione nel compiere un'attività illecita, il piacere del potere esercitato sui sistemi informatici (virtuosismo informatico), il riconoscimento dei pari, l'atto politico, il divertimento (Taylor 1999, 48-66; Turgeman-Goldschmidt 2005).

1.3 L'etica hacker

Se quella hacker è una comunità immaginata, l'unico meccanismo di appartenenza è rappresentato dal rispetto dei valori, differenziando così l'hacker dal semplice superesperto informatico. Perciò rifarsi a un insieme di principi etici è una strategia per costruire l'identità hacker. Non è un caso infatti che secondo alcuni quella che viene chiamata etica hacker altro non sia che il risultato di una complessa costruzione di una identità collettiva (Jordan e Taylor 1998).

Esistono diverse declinazioni di quale siano le norme alla base dell'etica hacker. Una delle formulazioni più complete è senza dubbio quella esposta nel pionieristico studio di Steven Levy (1984, 39-49). Secondo il giornalista statunitense, gli imperativi morali alla base dell'etica hacker sono i seguenti: l'accesso al computer deve essere illimitato e totale, l'informazione deve essere libera, bisogna dubitare dell'autorità e promuovere il decentramento, un hacker deve essere giudicato in base al suo operato e non per altri motivi (età, sesso, religione), il computer è una macchina con cui è possibile creare arte e bellezza, i computer possono cambiare la vita delle persone in meglio.

Come si può notare ad esclusione degli ultimi due principi che sono strettamente legati all'artefatto computer, gli altri principi si ricollegano alle norme di comportamento che deve avere l'hacker nei confronti della propria attività e della propria comunità. Questo aspetto è particolarmente importante perché è rivelatorio delle origini dell'etica hacker.

Tutti gli autori che hanno raccontato la storia dell'hacking – tra i più influenti Levy 1984 e Sterling 1992 – insistono nel ricordare che la comunità hacker si forma all'interno dell'ambiente accademico del Mit di Boston e quindi possiamo ipotizzare che alcuni di questi principi siano la traduzione delle norme deontologiche alla base di quello che dovrebbe essere l'idealtipo del ricercatore.

Detto in altro modo ci sono delle notevolissime somiglianze tra l'etica hacker e i valori della scienza accademica.

Secondo Merton (1942) i valori alla base della ricerca scientifica accademica sono: comunitarismo (la conoscenza cui giunge lo scienziato è patrimonio della comunità scientifica), universalismo (la conoscenza scientifica è universale e non dipende da chi l'ha enunciata), disinteresse (la ricerca è svolta per amore del sapere e per ottenere riconoscimento dei pari), originalità (la ricerca deve pervenire a risultati nuovi), scetticismo organizzato (l'atteggiamento dello scienziato deve essere critico verso ogni risultato). Se si confronta l'ethos mertoniano dello scienziato con i fattori alla base dell'etica hacker identificati da Levy, non sarà difficile trovare somiglianze in molti punti.

Altri autori hanno preferito ricondurre la questione dell'etica hacker a un nuovo modo di intendere l'etica del lavoro (tra gli altri Hannemyr 1999; Wark 2006).

Pekka Himanen (2001) rifacendosi esplicitamente a Max Weber, sottolinea gli elementi che traducono l'etica protestante in versione hacker. L'etica hacker è così un costrutto di tre distinte componenti etiche: l'etica del lavoro (passione verso il proprio lavoro e libertà di lavorare secondo i propri ritmi), l'etica del denaro (desiderio di creare qualcosa per la propria comunità e assenza di controllo del proprio prodotto), «netica» (*nethic*) o etica del network (libertà di espressione e la considerazione degli altri come fine), tutto governato dalla creatività intesa come valore in sé.

Esiste un altro motivo per considerare importante l'etica hacker.

Il vero antagonista della comunità hacker è l'industria della sicurezza informatica, ovvero quel settore informatico il cui scopo è creare prodotti in grado di impedire gli attacchi hacker (Taylor e Jordan 1998; Taylor 1999). Quello che è interessante è che i sistemi con cui l'industria della sicurezza informatica mette a punto i propri prodotti sono molto spesso indistinguibili dalle pratiche hacker: testare la sicurezza di un sistema informatico vuol dire usare le stesse strategie di attacco usate dagli hacker. Perciò la demarcazione fra l'hacker e il suo "doppio", ovvero l'esperto di sicurezza informatica, sta nella diversa etica alla base della comunità: apertura e libertà per i

primi, chiusura e controllo per i secondi. Detto questo è facile comprendere come il desiderio di ogni hacker sia quello di diventare un esperto di sicurezza informatica: è l'unico modo che la comunità ha per continuare ad occuparsi della propria passione in maniera legittimata. È ricchissima la casistica di persone che sono stati hacker da adolescenti per poi diventare esperti di sicurezza informatica da adulti (Sterling 1992; Taylor 1999).

2. *Studio di caso. Una comunità di wardrivers italiani*

2.1 *Metodo di ricerca*

La ricerca qui esposta può essere ricondotta all'interno del vasto alveo delle ricerche etnografiche, ovvero l'uso di pratiche di ricerca antropologiche all'interno dei contesti sociali tipici delle società industriali avanzate (Gobo 2001; Dal Lago e De Biasi 2002). In maniera particolare possiamo parlare di una ricerca relativa all'etnografia del consumo dei media (cfr. Boni 2004).

Ci sono due motivi che ci portano a considerare la nostra come una ricerca tipica dell'etnografia dei media.

Il primo motivo è inerente alla storia degli studi sociali del computer. Infatti il computer e tutto l'ambito dei media digitali da molto tempo sono considerati sempre meno artefatti tecnici e sempre più mezzi di comunicazione di massa. L'approccio del consumo dei media (Moore 1993), la scoperta del portato comunicativo delle tecnologie della comunicazione da parte dei *media studies* (si veda il caso dell'*home computer*: Haddon 1992), l'importanza dell'utente – e quindi il pubblico – della tecnologia da parte gli studi sociali della tecnologia (cfr. Oudshoorn e Pinch 2003) sono i momenti chiave che hanno legittimato questo passaggio.

Il secondo motivo che ci porta a classificare la nostra ricerca nel campo dell'etnografia dei media sono le considerazioni metodologiche che hanno guidato la progettazione del nostro disegno della ricerca: gli attori sociali come collettività diversificata, l'interesse nei confronti delle pratiche sociali, l'attenzione al contesto di utilizzazione, l'uso degli strumenti qualitativi di indagine, una riflessione critica sugli stili di consumo tecnologico (Bennato 2000). Particolare attenzione è stata dedicata alle pratiche sociali, inserite nella nostra definizione operativa definendo l'hacker come utente di specifiche strategie di appropriazione basate su pratiche. Secondo alcuni studiosi, è questo ciò che rende interessante l'etnografia dei

media (digitali): i modi con cui tali pratiche divengono significative in contesti locali (Hakken 1999; Hine 2000).

La scelta dell'approccio etnografico è stata anche guidata dal fatto che altre ricerche simili hanno utilizzato questa modalità di indagine (Taylor 1999; Turgeman-Goldschmidt 2005). Le ricerche empiriche sugli hacker evidenziano l'utilità dell'approccio etnografico, non solo perché si presta bene per le ricerche sulle comunità, ma anche perché in quella hacker la significazione delle pratiche è molto diversa da membro a membro.

La nostra ricerca ha avuto come oggetto di studio una comunità di *wardrivers* operante nella provincia di Salerno. Il periodo di osservazione di questa comunità è durato cinque mesi, dal dicembre del 2004 ad aprile del 2005 organizzato in due fasi distinte. Nella prima fase (dicembre 2004-febbraio 2005) è stata utilizzata la tecnica dell'osservazione partecipante grazie a i contatti sociali stabiliti con il leader del gruppo, che ha svolto così anche il ruolo di informatore. Sono state così raccolte 10 sessioni di wardriving, annotando le pratiche in atto (stesura delle note etnografiche) e chiedendo spiegazioni delle situazioni ambigue, rilevate tramite un registratore digitale portatile (*backtalk*: Cardano 1997). Le note etnografiche così rilevate sono state discusse in un secondo momento con il resto del gruppo per garantire la corretta interpretazione delle pratiche. Sono state anche svolte un totale di quattordici interviste di cui tre collettive e tra le interviste singole rimanenti, i soggetti più rappresentativi sono stati intervistati più volte.

I risultati a cui si è giunti in questa prima fase, sono stati utilizzati come base per la stesura della traccia di intervista che è stata utilizzata nella seconda fase (marzo-aprile 2005). In questo caso sono state effettuate altre due sessioni di wardriving, per verificare se i risultati a cui si era giunti fossero corretti. Inoltre è stato svolto un focus group con alcuni membri della comunità per rilevare in dettaglio i resoconti delle proprie pratiche.

2.2 *Analisi della comunità wardriver*

Come dicevamo, la comunità opera nella provincia di Salerno ed ha stretti contatti con un altro gruppo di *wardriver* della città di Campobasso, gruppo che si autodefinisce «pioniere» del *wardriving* in Italia. Nel complesso la comunità è composta da circa 12 individui: i membri chiave sono 5 studenti di informatica che vivono nello stesso appartamento mentre gli altri sono membri meno assidui nelle uscite di wardriving. L'età varia dai 19 ai 27 anni, con una media di

circa 22 anni. Alcuni di loro si conoscono da diverso tempo, ma solo dal 2003 si incontrano per effettuare le sessioni di wardriving: circa un'uscita alla settimana. La data di nascita della comunità è legata all'*Hackmeeting* di Torino del 2003, quando dall'incontro con degli hacker dell'isola d'Elba decisero di diffondere la conoscenza delle pratiche di wardriving anche in Italia. Per accedere al gruppo l'unica conoscenza richiesta è la passione per l'informatica e l'adesione all'etica hacker.

Da quanto descritto si evince come la comunità in esame sia un classico esempio della scena hacker del nostro paese, dato che gli *Hackmeeting* italiani sono dei momenti molto importanti di scambio e di formazione dei diversi hacker presenti sul territorio nazionale. Infatti i corsi di informatica delle università italiane sono il "brodo di cultura" tipico (anche se non l'unico) dal quale nascono alcuni dei personaggi più attivi dell'hacking italiano. Spesso però la competenza informatica fornita dall'università non basta per la costruzione del soggetto hacker. Un ruolo cruciale per il completamento di questo processo sono i momenti di condivisione delle esperienze nel campo dell'hacking reso possibile dai diversi *Lug-Linux Users Group*, esperienze queste sovente incorporate nel panorama dei centri sociali sparsi sul territorio italiano (Di Corinto e Tozzi 2002; Freschi 2002; Fici 2004).

Non è un caso la particolare tipologia di hacking che è stata scelta.

Al di là della novità della pratica, il wardriving permette una forma di appropriazione del territorio che le strategie hacking "tradizionali" non necessitano. Potremmo dire che i wardriver usano le reti internet wireless come meccanismo per riappropriarsi di un luogo che altrimenti non li vedrebbe protagonisti in quanto poco "tecnologico".

Come punto di appoggio delle operazioni di wardriving in cui vengono pianificate e progettate le uscite collettive e dove viene messa a punto la strumentazione tecnica, è stata scelta la casa del leader del gruppo (denominata la base), poiché è l'appartamento dei 5 studenti di informatica. È considerata tale anche dai membri meno assidui della comunità, poiché vengono lasciate le attrezzature tecnologiche dei componenti che non vivono nell'appartamento. Quasi quotidianamente ogni membro della comunità passa per la base. I luoghi sociali della base sono la cucina e le camere da letto. Queste ultime vengono utilizzate come vere e propri laboratori, dato il gran numero di strumentazione tecnica sparsa in giro (cavi, *case* di computer, *router* ecc.).

Per quanto riguarda l'attrezzatura, oltre alla strumentazione classica (computer portatili, antenne), ci sono altri dispositivi tecnici che vengono "cannibalizzati" per costruire altro materiale secondo un preciso rituale di appropriazione.

Ad esempio: in cucina sono presenti svariati tubi di patatine *Pringles*, poiché seguendo i consigli dei più diffusi manuali di hacking delle reti wireless, possono essere usati per costruire antenne direzionali. Una delle antenne fatte in casa è costituita da un vecchio attaccapanni appositamente modificato per lo scopo.

Dato che l'antenna ha un ruolo molto importante per identificare le reti wireless, alcuni membri del gruppo più esperti studiano la composizione delle antenne commerciali per poterle riprodurre in casa usando o materiale di recupero o prodotti reperibili nelle ferramenta. Una volta costruita l'antenna e testata l'efficienza, i risultati vengono messi su internet nella forma di guide.

Dal punto di vista software tutto il gruppo usa Linux per due ordini di motivi: per l'estrema flessibilità di questo sistema operativo che facilita le operazioni di hacking, e per motivi ideologici, dato che Linux con la sua distribuzione *open source* è considerato la migliore alternativa ai software commerciali come *Microsoft Windows*. L'unica occasione d'uso del sistema operativo *Windows* è la caccia alle reti wireless prima di una sessione di wardriving. Infatti il leader della comunità quando passeggia per la città usa un palmare dotato di *Windows PocketPC* con installato un software per lo *sniffing* (identificazione di reti wireless). Le coordinate geografiche della rete così rilevata, vengono annotate su un *TomTom*, un navigatore satellitare.

Ci sarebbe un'altra pratica per segnare la presenza delle reti: l'uso del *warchalking*. Il termine indica l'atto di segnare con un gessetto per terra (o sugli edifici) la presenza di un accesso wireless usando un codice piuttosto particolare (Bennato 2004; Ryan 2004; Sandvig 2004). Si preferisce non usare questa pratica per un motivo etico: non si vogliono indicare vulnerabilità a chi animato da cattive intenzioni.

Questa comunità ha contatti e scambi con altre comunità hacker italiane. Di solito questi gruppi vengono contattati durante gli incontri hacker (come gli *Hackmeeting*, i *LinuxDay*, le riunioni dei *Lug*). I contatti vengono mantenuti online tramite l'uso di forum tematici, canali Irc (*Internet Relay Chat*, uno dei canali chat più usati dagli hacker) e *newsgroup* specializzati: canali spesso usati anche per stabilire contatti con comunità internazionali di wardriver.

L'automobile riveste un'importanza fondamentale in quanto viene usata per trasportare la strumentazione tecnica necessaria alle

operazioni di wardriving, ovvero computer portatili e antenne. L'auto viene organizzata come un micro-luogo domestico in accordo con l'ipotesi della privatizzazione mobile (Williams 1974). Le sessioni di wardriving si svolgono essenzialmente nelle ore notturne (tra le 24.00 e le 1.00, in alcuni casi fino alle 4.00 del mattino) sia per via della non completa liceità della pratica, sia per aumentare l'eccitazione nel compiere un'attività (potenzialmente) illegale.

Altra caratteristica comune col mondo hacker: nella comunità non sono presenti donne. La motivazione addotta è legata al contesto sociale frequentato dai wardriver. I corsi di ingegneria informatica dell'Università e i *Lug*, principali luoghi per il reclutamento e l'evangelizzazione di neofiti verso il wardriving, sono luoghi a bassa frequentazione femminile poiché – in quanto ambienti tecnologici – sono soggetti a una forma di pregiudizio nei confronti delle donne.

Per descrivere i resoconti più interessanti emersi dalla ricerca, si farà riferimento ai fattori interni che le ricerche empiriche sugli hacker hanno identificato (Jordan e Taylor 1998; Taylor 1999) poiché sono stati utilizzati come linee guida in fase di analisi dei risultati delle diverse rilevazioni effettuate.

2.2.1. Tecnologia

Il rapporto instaurato con la tecnologia è tipico della comunità hacker: strategie di appropriazione dell'artefatto tecnologico messe in atto a tutti i livelli, sia nella scelta della strumentazione necessaria per le sessioni di wardriving, sia nella modificazione e costruzione dell'artefatto tecnico.

[...] [Le schede wireless del computer] Di solito le modifichiamo perché è raro trovare schede con attacchi per antenne esterne, visto che comunque una scheda ha un raggio di poche centinaia di metri, utilizzando un'antenna esterna possiamo aumentare di molto i decibel di potenza e quindi prendere degli access point, delle reti anche a distanza di chilometri.

(DonDiego, intervista 6)

[I miei compiti sono vari] Procurare, o fare... che ne so... un'antenna, oppure se c'è bisogno di modificare una scheda. Mi piace molto la parte hardware: è un mio divertimento proprio, modificare dei pezzi, crearne altri.

(MacGiver, intervista 2)

In realtà alcune scelte tecnologiche sono guidate più da motivi legati all'etica hacker che semplicemente alla mera funzionalità. Appropriazione in questo caso può essere declinata come scelta delle tecnologie ritenute compatibili con l'etica hacker, quasi fosse una strategia di appropriazione simbolica.

Linux non è solo un sistema operativo ma è anche una filosofia.
(Pluto, intervista 14)

[Usiamo Linux] Innanzitutto perché è open source. Noi essendo informatici possiamo modificare il sistema operativo a nostro piacimento, adattandolo anche alle nostre necessità. Non utilizziamo Windows perché innanzitutto non sappiamo come è composto perché il codice sorgente di questo sistema operativo non è accessibile a tutti, e poi utilizziamo Linux anche perché è gratis e non ha problemi di licenze e cose varie.
(Fireb, intervista 3)

Tutti i membri della comunità mostrano una vera e propria passione per la tecnologia informatica sia per motivi professionali (sono studenti di informatica e vorrebbero lavorare nel settore) sia perché reputano il computer uno strumento estremamente flessibile e permeabile. Questa passione è anche il collante che tiene insieme il gruppo.

Mi piacciono le infinite possibilità che un computer ti mette davanti, l'idea di poter realizzare qualsiasi cosa mi passi per la testa con costi relativamente modesti.[...] Però ammetto che una delle leve che mi ha spinto a studiare informatica è stata la curiosità di capire come funzionano i videogiochi, nella speranza di poter un giorno scriverne uno anch'io. Intanto però continuo a giocare e, non troppo spesso, a programmare
(MisterC, intervista 4)

Bè comunque ci accomuna la passione per l'informatica quindi in generale ci conosciamo così in un modo o nell'altro sia in ambiente universitario sia perché appunto frequentiamo gli stessi luoghi che hanno a che fare con l'informatica, quindi LUG, associazioni varie, etc etc e ci siamo conosciuti così.
(DonDiego, intervista 5)

La pratica del wardriving è stata scoperta usando i canali di informazione presenti in internet che vengono usati per l'aggiornamento sul mondo sociale del computer.

Su Slashdot e altri siti del genere cominciavano a esserci diverse news riguardanti la moda del wardriving che in America stava andando un casino e allora abbiamo voluto provare. Quando abbiamo cominciato noi in Italia non lo faceva nessuno perché era davvero difficile trovare anche delle schede wireless. È stato difficile trovarle e le abbiamo pagate anche tanto
(DonDiego, intervista 5)

L'esistenza del wardriving in verità non è stata [...] una mia scoperta. Diciamo che documentandoci un po' in generale avevamo sentito parlare sia da amici sia in hacklab si accennava a questa cosa più di due anni fa e ci siamo documentati in merito. [...] Poi tramite Slashdot e altri siti abbiamo scoperto qualcosina in più quando è nato in America.
(Bohemien, intervista 8)

La decisione di praticare il wardriving è attribuibile a un miscuglio di curiosità, circostanze sociali e voglia di condividere le opportunità tecnologiche permesse da questa pratica.

[Pratico il wardriving] Innanzitutto per passione e poi, dato che sono studente di informatica, sono interessato alle nuove tecnologie e alla sicurezza correlata a queste tecnologie [...] La passione è la stessa che mi ha spinto ad avvicinarmi al mondo dell'informatica, quindi una tecnologia nuova, adattabile e che in futuro mi potrà far guadagnare.
(Fireb, intervista 3)

Un aspetto piuttosto interessante è il modo particolare con cui viene preparata una sessione di wardriving, quello che potremmo chiamare “rituale di wardriving”, in quanto ogni aspetto dell'organizzazione viene attentamente pianificato ed eseguito sempre nello stesso modo (o con piccole varianti).

Fenomenologicamente la pratica del wardriving consiste nel trovare una *intranet wireless* e penetrarvi sfruttando le falle di sicurezza di questa tipologia di reti.

Per prima cosa si preparano i computer portatili specificamente dedicati allo scopo, tutti dotati di sistema operativo Linux in quanto

permette di operare anche in modalità amministratore di sistema, condizione necessaria quando occorrerà agire sulla rete wireless. La preparazione consiste nell'aprire diverse finestre di lavoro dentro le quali saranno fatti funzionare i software che servono nelle varie fasi della procedura che sono: identificazione della rete wireless, associazione del portatile alla rete identificata, intrusione nella rete, scansione dei dati per conoscere l'architettura o semplicemente per trovare il computer che consente la navigazione internet.

Di solito le uscite si fanno con un numero variabile di portatili a seconda dei membri del gruppo coinvolti nello svolgere una delle fasi del wardriving.

Sistemati i portatili, vengono preparate le antenne usate per intercettare la rete una volta collegate ai computer usati per il wardriving. Le antenne sono costruite in modo tale da aumentare la potenza di intercettazione, così dai pochi metri delle schede wireless commerciali, si arriva fino a diverse decine di metri delle schede equipaggiate con antenne fatte in casa.

Preparati i computer, lanciati i programmi e sistemate le antenne, si porta tutto in macchina e saliti tutti i partecipanti all'azione di wardriving, si parte alla ricerca delle reti da "bucare"².

L'orario scelto dal gruppo per svolgere questa pratica è tra mezzanotte e l'una del mattino, mentre la durata della sessione dipende da diversi fattori: identificazione delle reti disponibili, velocità della penetrazione nel sistema, affidabilità delle proprie apparecchiature.

In linea generale una sessione non dura più di 3-4 ore.

Il momento di massima eccitazione è quando si analizza la rete wireless in cui si è riusciti ad entrare. Infatti a seconda della rete violata è possibile: rintracciare documenti riservati, navigare in internet utilizzando una connessione molto veloce, trovare materiali insoliti per un ufficio (come cartelle piene di musica e film scaricati tramite *file sharing*) e così via.

2.2.2 Segretezza e anonimato

La segretezza (della pratica) e l'anonimato (dell'identità del wardriver) hanno delle peculiarità che possono essere considerate come tipiche del wardriving. Infatti dato il suo stretto legame con il territorio, questa pratica hacking richiede l'uso di alcune particolari strategie di occultamento.

² Termine gergale per indicare la penetrazione non autorizzata in una rete di computer.

La decisione di praticare il wardriving durante le ore notturne è da collegare alla segretezza, dato che la strumentazione tecnica è piuttosto ingombrante (computer portatile, antenne) e i dispositivi ancora più piccoli – come i palmari – non si prestano bene per gli scopi.

[Il wardriving] Si può fare dove e quando si vuole, però penso che una persona con un portatile in mano, aperto, con un'antenna magari appoggiata sul portatile darebbe nell'occhio camminando per una città

(DonDiego, intervista 6)

Anche l'organizzazione collettiva del wardriving è una precauzione per far sì che la segretezza della sessione venga mantenuta per tutto il tempo.

La pratica viene pianificata in anticipo per recarsi a colpo sicuro nei pressi della rete wireless e dedicare il tempo restante solo alla violazione del sistema.

[Lavoriamo in gruppo così] Abbiamo più coesione e poi magari anche diminuisce la probabilità di essere beccati perché si possono fare degli appostamenti

(Fireb, intervista 3)

Con un dispositivo GPS [...] cerchiamo le reti e ne teniamo traccia su mappe personali, che riutilizziamo per organizzare le uscite di wardriving o per scambiarle con altre comunità amiche.

(DonDiego, intervista 10)

Similmente l'anonimato è vissuto in maniera piena e consapevole.

Considerazione tecniche molto raffinate sono alla base della strategie per far sì che l'anonimato resti tale durante le sessioni di wardriving, poiché non solo la pratica è percepita come illecita, ma anche perché per mantenersi anonimi bisogna possedere un insieme di competenze che sono parte della sfida ingaggiata con gli amministratori delle reti violate.

Il MACaddress serve appunto a identificare una macchina [computer]. Se io con questo MACaddress faccio danni su una rete grande ipoteticamente potrebbero risalire a chi ha fabbricato la mia scheda fino ai rivenditori [...] Innanzitutto io le schede che compro non le compro mai in prima persona e mai in negozio: ho sempre

alternative per comprare in maniera da rimanere anonimo. Comunque cerco di cambiare il MACaddress.
(DonDiego, intervista 12)

È una sfida di menti contro menti: è una sfida personale, perché se l'azienda ha una rete vuol dire che ha anche un amministratore di rete pagato per fare quello e quindi c'è la sfida con lui.
(DonDiego, intervista 15)

Il rapporto con l'anonimato è curato in maniera maniacale, fino a raggiungere in alcuni casi quella che potremmo chiamare "sindrome da sorveglianza", poiché ogni aspetto della propria identità di utenti di computer viene problematizzata rispetto all'impatto che l'artefatto informatico ha nei confronti della privacy.

[Noi] Facciamo tutto nell'anonimato. In genere ognuno di noi ogni volta che va su internet è schedato: lasciamo moltissime tracce quindi è facile risalire [all'identità dell'utente]. In questo modo invece risalire a me utente finale, a me utente della Rete, è praticamente impossibile. [...] Non faccio niente di particolare, ma se anche facessi qualcosa di particolare, non voglio che qualcuno lo sappia, [...] non voglio essere rintracciato, non voglio che il mio IP [indirizzo per la localizzazione del computer su internet] vada in mano a persone che poi lo possono riutilizzare a fini statistici.
(Pluto, intervista 13)

Persino lo stesso wardriving in alcuni casi viene declinato come tecnica tramite la quale salvaguardare la propria identità.

Un altro obiettivo potrebbe essere la connessione a Internet in assoluto anonimato. In questo caso avremmo la sicurezza di essere anonimi al 100% su internet senza poter essere rintracciati, e questo è uno dei motivi principali per cui si fa wardriving
(Pluto, intervista 13)

A differenza della cultura hacker, il wardriving non prevede che vengano lasciate firme degli autori o del responsabile dell'intrusione, infatti la comunità analizzata non ha un nome collettivo che la identifica. Però per rispondere alle diverse interviste, ognuno dei membri ha deciso un *nickname* che rivela la posizione gerarchica all'interno del gruppo e il proprio immaginario di riferimento:

DonDiego, MacGiver, Pluto, Fireb, Over, Speed, Genius, Skara, Lnx, Drive, Pickup, MisterC, Bohemien.

2.2.3 *Appartenenza fluida*

L'appartenenza fluida indica la posizione sociale rispetto al resto del gruppo. Molti affermano che non ci sia un vero e proprio capo, anche se riconoscono in DonDiego e in MacGiver una competenza tecnica tale che entrambi si dividono la leadership della comunità. Nello specifico a DonDiego sono attribuiti compiti di coordinamento e di motore del gruppo, mentre a MacGiver la costruzione di alcune apparecchiature hardware necessarie per le sessioni di wardriving. In questo caso si può vedere messo in atto il principio dell'etica hacker secondo la quale un hacker è giudicato (e valutato) da quello che fa e da quello che sa fare.

Se qualcuno ha da dire qualcosa lo dice e si fa, si prova. Non abbiamo regole quindi facciamo quello che più ci viene, quello che sembra interessante, perché poi se una cosa è interessante è palese.
(DonDiego, intervista 5)

[DonDiego è il capo] Perché è quello più preparato a livello tecnico ed è quello che ha introdotto tutti i membri della comunità a questa pratica. L'unico ruolo che si discosta dal nostro è quello di MacGiver, che è quello che si occupa della parte più tecnica, di assemblare le apparecchiature che usiamo.
(Fireb, intervista 3)

DonDiego non si riconosce in questo ruolo, perchè non ritiene di comportarsi da capo: preferisce far emergere la profonda democraticità del gruppo, anche se dai discorsi del resto dei membri si può dire che eserciti un vero e proprio potere carismatico.

Generalmente coordino io. Diciamo che conosco meglio la pratica e quindi mi capita di gestire la cosa. Però faccio generalmente scegliere gli altri: ad esempio se troviamo alcune reti scegliamo insieme su quale fermarci, su quale no. Queste cose si scelgono insieme poi magari posso dare alcuni compiti: tipo posso dire a qualcuno di fare una cosa, a qualcuno un'altra... sì magari su questo posso coordinare più io, però sulle scelte in generale si prendono tutte insieme
(DonDiego, intervista 5)

La presenza della leadership non viene riconosciuta da MacGiver:

No, non credo [che sia un capo], no.
(MacGiver, intervista 2)

Il motivo della mancata attribuzione/autoattribuzione della leadership deve essere associato a due fattori.

Il primo è che i ruoli sono definiti rispetto alle competenze tecniche, perciò essi variano a seconda dell'andamento delle sessioni di wardriving pur essendoci dei leader "impliciti" per via delle conoscenze che hanno del software (DonDiego) o dell'hardware (MacGiver)

Il secondo fattore è che il gruppo si percepisce come legato da rapporti di amicizia che sono sempre prevalenti rispetto al loro essere membri di una comunità il cui scopo è il wardriving.

[Siamo amici] Perché ci divertiamo insieme, abbiamo interessi comuni, facciamo molte cose in comune.
(Pluto, intervista 14)

[Siamo amici per vari motivi] Ma anche senza fermarci troppo sull'informatica, anche su ciò che è tecnologico, a partire dall'elettronica, per andare a finire alle donne...
(MacGiver, intervista 14)

No, la nostra amicizia [è più importante del wardriving].
(DonDiego, intervista 5)

C'è un'altra accezione dell'appartenenza fluida che possiamo riscontrare nei membri del gruppo. Proiettandosi rispetto al futuro, vorrebbero proseguire in questa loro sperimentazione diventando esperti di sicurezza delle reti, per non perdere il piacere che essi provano praticando il wardriving. Da questa riflessione emergono due temi presenti nella letteratura empirica sugli hacker: il primo è che non si può fare gli hacker per tutta la vita perché è un'attività che richiede una grande quantità di tempo, il secondo è che la differenza fra hacker ed esperti di sicurezza informatica è nei valori e non nelle pratiche.

Ci mandasse lo Stato a fare wardriving! Allora lo Stato ci dice: "c'è questo problema" e dice "andate e per ogni rete aperta che

trovate andate a tenere un seminario su cos'è la sicurezza del wireless". Questo si potrebbe fare: lo stato fa tante campagne di sensibilizzazione e visto che siamo nell'era dell'Information Technology a questo punto si potrebbe fare una cosa del genere.
(DonDiego, intervista 15)

Una delle caratteristiche del gruppo da noi studiato è la sovrapposizione di tre diversi meccanismi di coesione sociale che insieme rendono conto dell'articolazione delle dinamiche di appartenenza dei membri.

Infatti possiamo riconoscere legami amicali, soprattutto tra i fondatori, legami cognitivi fra alcuni membri che partecipano solo alle fasi preparatorie e fanno parte del gruppo per migliorare le proprie conoscenze tecniche, e infine legami che potremmo definire "deboli" che caratterizzano i neofiti che ne sono entrati a far parte grazie ai confini permeabili del gruppo e che sono attratti più dall'atmosfera frizzante che si respira che da un vero interesse profondo per la competenza tecnica e la voglia di sperimentare.

2.2.4 Motivazioni

Piacere, conoscenza, curiosità, sfida: sono questi i temi che tornano più spesso nello descrivere le motivazioni che spingono a praticare il wardriving.

[Pratico il wardriving] Perché è un qualcosa che mi piace, una tecnica interessante – se di tecnica possiamo parlare – ed è un qualcosa che aumenta le mie capacità [...] Il wardriving mi piace in senso professionale ed etico. Professionale nel senso che posso imparare cose da applicare nella vita pratica, etico perché delle tante cose che conosco è una forma di condivisione.

(Pluto, intervista 1)

Praticando wardriving riesco a capire le varie vulnerabilità che può avere un sistema, oltre a capire la stupidità della gente a lasciare dei servizi aperti e molto, molto, molto importanti [...] Per quel che ne faccio io è hacker, non distruggo niente.

(MacGiver, intervista 2)

Si è una sfida. Io sono un amministratore di sistema e trovare comunque una rete fatta male... se io la riesco a violare facilmente è una soddisfazione.

(DonDiego, intervista 6)

[...]Mi piace scoprire le reti non protette se appartengono a privati o meno, perché spesso capita di trovare delle reti wireless non protette che corrispondono ad aziende in generale o ad aziende di informatica e il che è grave.
(Bohemien, intervista 8)

Quello che è interessante è la percezione del wardriving da parte della comunità. Infatti secondo alcuni il wardriving non è una vera e propria pratica hacker, poiché mentre gli *hack* richiedono notevole competenza tecnica, il wardriving richiede una competenza ridotta, e quindi l'accesso alla pratica (potenzialmente) è molto più ampio.

In generale non è una pratica hacker, almeno non sempre, perché se c'è una rete aperta, tranquilla senza protezioni [...]richiede un paio di comandi e quindi non c'è bisogno di uno studio dietro. [...] Tra un annetto o un annetto e mezzo secondo me ci sarà il clou di wardriving in Italia quando i ragazzini di oggi prenderanno la macchina e si metteranno a girare in cerca di reti wireless.
(DonDiego, intervista 6)

Per quanto concerne l'illiceità o meno della pratica, tutta la comunità è d'accordo nel dire che la differenza fra il wardriving lecito e quello illecito sta nelle motivazioni che spingono a compiere le intrusioni. Se l'attività si limita alla sola infiltrazione è considerata come coerente con l'etica hacker e quindi non è sanzionabile.

Diverso il caso dell'infiltrazione con scopi vandalici o illegali (il cosiddetto *cracking*)

Allora il wardriving è da dividere in due cose: generalmente quello che si fa nel wardriving è cercare reti wireless, cercare di collegarsi con queste reti, prendere informazioni oppure sfruttare la linea Internet, eventualmente se c'è, collegata a una rete. [...] Magari nelle reti più complesse, [il wardriving] potrebbe essere una tecnica hacker. Generalmente se usata con i fini sbagliati il wardriving è [invece] una tecnica cracker.
(DonDiego, intervista 6)

Assolutamente no, usare [il wardriving] per fare danni non è proprio nostra intenzione. Fare danni è da stupidi: meglio non fare niente. Quello che facciamo è per studiare e per imparare, non

vogliamo fare danni, anche se studiando questa cosa capiamo che chi vuole fare danni facilmente ne può fare e anche tanti.

(Pluto, intervista 13)

Ovviamente il potere tecnico derivante dal wardriving potrebbe essere usato per compiere attività illecite, ma tali comportamenti se solo vengono accennati sono duramente sanzionati dai leader della comunità.

Sì ogni tanto c'è qualcuno che ha la tentazione [di compiere attività illegali] ma quando ci sono io non mi va questo. Mi piace più che altro controllare, sapere che io ci sono riuscito [...] questo mi basta perché ipoteticamente potrei fare tutto il resto, ma praticamente mi basta sapere che posso, cioè mi basta aver avuto la prova che posso farlo.

(DonDiego, intervista 6)

Tutti inoltre sono d'accordo a considerare il “vero” wardriving (cioè coerente con l'etica hacker) solo quello che si pratica in gruppo. Non è neanche concepibile la possibilità di fare wardriving “in solitaria”, perché in quel caso si sospettano scopi non leciti.

[Il wardriving da solo non è vero wardriving] No perché non c'è lo spirito di gruppo, penso per lo più siano i mercenari [a praticare il wadriving in solitaria]. [...] Sì perché non ci vedo una filosofia dietro, ci vedo più una questione di soglia di illegalità.

(DonDiego, intervista 14)

[Fare wardriving in gruppo] Influisce fortemente. Il wardriving è un pretesto per stare insieme, poi come tutti gli attacchi di hacking che vengono effettuati, anche questo, quando si è in gruppo, la probabilità di successo aumenta.

(Fireb, intervista 3)

Nonostante la percezione di gruppo dominante che il wardriving sia lecito per imparare di più sulla sicurezza delle reti, un membro non la pensa in questo modo e solleva forti dubbi sul fatto che l'attività non sia solo illegale, ma profondamente immorale.

[Non pratico il wardriving] Perché penso che sia una palese violazione della privacy, ma devo ammettere che la pratica è interessante. [...] Credo che la violazione della privacy non sia

semplicemente un reato, ma una vera e propria intrusione negli "affari privati" di una persona. Stesso discorso nel caso di reti aziendali, anzi forse in questo caso il discorso è aggravato dal fatto che l'intrusione può comportare anche un danno economico.
(MisterC, intervista 4)

[Riferendosi agli altri membri della comunità] Una cosa che io mi chiedo: ma andare a curiosare nei fatti degli altri è una cosa che non vi crea nessun problema? [...] Ma se c'è gente che il wireless non lo sa usare perché non suonate a quelli che hanno le reti aperte e gli dite "abbiamo trovato questa falla nella tua rete"?
(MisterC, intervista 15)

3. Conclusioni

Da una ricognizione della letteratura sul tema dell'hacking e dai risultati della ricerca compiuta sui wardriver italiani, possiamo trarre due diverse considerazioni: una relativa alla specificità della comunità rispetto alla più ampia comunità hacker, l'altra relativa agli elementi che rendono interessante il wardriving rispetto alla dimensione sociale più generale.

Per quanto riguarda i rapporti del wardriving con la comunità di appartenenza, possiamo tranquillamente dire che è a tutti gli effetti una pratica hacker da tre diversi punti di vista.

In primo luogo perché i membri si considerano non solo appartenenti alla "comunità immaginata" degli hacker, ma anche alla cultura del computer e della sua specifica organizzazione sociale. Hacking nel senso di cultura tecnologica.

In secondo luogo perché le pratiche di wardriving – così come quelle hacking – sono strategie di appropriazione che richiedono competenze tecniche non banali e una capacità di comprensione dell'aspetto sociale delle reti informatiche in cui si penetra, facendo a gara con le competenze del responsabile tecnico della rete violata. Hacking inteso come sfida intellettuale.

In terzo luogo perché tutte le strategie di coesione della comunità wardriver e le pratiche performative e di significazione sono ispirate ai principi di apertura, libertà e condivisione che formano le regole dell'etica hacker. Hacking come sistema di valori e stile di vita.

A ben vedere però la comunità dei wardriver mostra due importanti differenze che la rendono una cultura tecnologica emergente.

La prima differenza è nella modalità di svolgimento della pratica. Se gli attacchi hacker sono pratiche svolte in maniera individuale che solo in rari casi vengono attuate collettivamente, il wardriving invece è un'attività essenzialmente collettiva che trova la sua realizzazione come azione di gruppo. Non solo. Come emerso da più parti della nostra analisi, chi pratica wardriving in solitaria non è considerato parte della comunità hacker, anzi si sospetta che siano solo mercenari o persone che non aderiscono all'etica hacker. Sbaglia chi pensa che la performatività di gruppo sia conseguenza del rituale di wardriving che chiede la disponibilità di computer appositamente preparati – spesso con strategie da *bricoleur* – e l'uso di un veicolo per muoversi sul territorio. Ciò non è vero non solo perché esistono attacchi hacker complessi che richiedono preparazioni, appostamenti e lunghe pianificazioni, ma anche perché la penetrazione del wardriver nella rete (la cosiddetta associazione) viene fatta a veicolo fermo, quindi in una situazione che potrebbe essere gestita da soli. La domanda a questo punto è: quale il motivo della collettivizzazione della pratica?

La risposta ci porta alla seconda differenza del wardriving rispetto all'hacking.

La differenza cruciale sta nelle strategie di appropriazione del territorio. L'hacking infatti è un tipo di strategia “statica” che si svolge prevalentemente da una stanza di una casa o di un ufficio. Invece il wardriving è un'attività che richiede una ricognizione del territorio: è una attività legata al movimento, all'identificazione di flussi di dati nello spazio. Questa strategia di appropriazione del territorio dà alla pratica una dimensione nomadica, che nelle strategie hacking “classiche” è sempre stata una dimensione narrativa. La frase “entrare in una rete”, mentre nell'hacking è solo una metafora, nel wardriving invece diventa concreta: se non altro perché per entrare nella rete sotto attacco bisogna quantomeno trovarsi fisicamente nei suoi pressi. Alla *flânerie* digitale dell'hacking, possiamo contrapporre la fluidità territoriale dei wardrivers. Ed è in questo che si rivela la dimensione collettiva della pratica. Nella costruzione discorsiva del wardriver, lo spazio fisico è anche uno spazio digitale da esplorare, quindi è necessaria un'organizzazione che faccia del gruppo l'unità di riferimento. Se il viaggio è un'esperienza individuale (tipica dell'hacker), l'esplorazione è un'esperienza collettiva (tipica del wardriver) perché necessita della condivisione delle scoperte.

Per comprendere l'interesse del wardriving rispetto ai processi della *network society*, dobbiamo isolare alcune dimensioni che la

rendono una cultura tecnologica profondamente calata nel nostro tempo.

La prima cosa che risalta è lo spazio sociale all'interno del quale si colloca il wardriving. Infatti è un tipo di pratica che sfrutta a proprio vantaggio i limiti tecnologici – i problemi relativi alla sicurezza – della connettività internet di tipo wireless. La conseguenza è che questa tipologia di hacker mostra come quella del wireless sia ancora una tecnologia in corso di miglioramento e suscettibile di riconfigurazione. Usando il linguaggio teorico tipico della costruzione sociale della tecnologia (Bijker 1995) le reti di computer wireless sono in una situazione di flessibilità interpretativa in cui i wardriver ricoprono il ruolo di gruppi sociali pertinenti in quanto gli sviluppi futuri devono tener conto dei problemi legati alla sicurezza. Questa riflessione mostra – qualora ce ne fosse ancora bisogno – la straordinaria importanza del ruolo dell'utente nel processo di sviluppo tecnologico, posizione questa che sta assumendo un ruolo chiave negli studi sociali della tecnologia (Silverstone, Hirsch e Morley 1991; Oudshoorn e Pinch 2003).

Un altro elemento è che il wardriving incarna le proprietà dei soggetti sociali che nascono dall'integrazione della tecnologia nella vita quotidiana. Appropriazione, esplorazione (ovvero uso creativo dell'artefatto) e incorporazione di valori nell'uso della tecnologia sono le caratteristiche che noi possiamo trovare non solo in una classe di utenti sofisticati come i wardriver, ma anche negli utenti di altre tecnologie d'uso quotidiano. Si pensi ad esempio alle recenti ricerche sull'uso del telefonino da parte degli adolescenti (Scifo 2005) o agli studi volti ad analizzare i modi in cui internet viene incorporato nelle pratiche di significazione della vita quotidiana (Bakardjieva 2005).

Il terzo elemento che definisce il wardriving come vero laboratorio culturale di comportamenti sociali emergenti è la strategia di consumo del territorio (Urry 1995). Il wardriving esiste grazie all'infrastruttura tecnologica che si è completamente incorporata nello spazio fisico creando una dimensione ibrida per cui lo spazio assume delle proprietà profondamente diverse. La dimensione topografica tipica dello spazio fisico e la dimensione topologica tipica dello spazio digitale si fondono in una nuova dimensione spaziale che altrove abbiamo chiamato "luogo tecnologico", che gode di proprietà specifiche e incarna processi sociali che le sono propri (Bennato 2004). Il wardriving con il suo uso congiunto di computer e automobili mostra come sia possibile accedere alla dimensione territoriale utilizzando due punti di accesso: fisico e digitale.

È ormai da qualche tempo che molti autori sottolineano come sia la fluidità dello spazio una delle componenti più interessanti della società delle reti (Castells 1996), sarebbe infatti la mobilità la condizione tipica del cittadino del XXI secolo (Urry 2000). La trasformazione dello spazio ad opera dei processi sociali e tecnologici è una tematica molto presente nella riflessione teorica degli ultimi anni sia a livello micro nell'analisi della mobilità, sia a livello macro nella ricerca sulle traiettorie dei flussi economici e culturali della globalizzazione. È in questo contesto che lo studio dei wardriver assume un significato sociologico più ampio: sono la prima cultura tecnologica che cerca di collocarsi in questo nuovo modo di concepire i rapporti fra spazio fisico, dimensione sociale e reti tecnologiche: le loro strategie di appropriazione non fanno altro che rivelare una modalità emergente nell'uso dei luoghi che possiamo trovare *in nuce* nell'uso sociale della telefonia mobile. Se non venissero così contestualizzate le pratiche dei wardriver, sarebbe difficile capire perché sono interessanti risultati all'apparenza modesti come curiosare in una rete aziendale o sfruttare in modo non autorizzato una connessione internet. Uno sguardo poco accorto potrebbe concludere che la montagna (il rituale di wardriving) abbia partorito il topolino (curiosare in una rete riservata). In realtà se si prende considerazione il ruolo strategico del luogo tecnologico, allora il comportamento dei wardriver assume un significato e un'importanza completamente diversi.

Infine la dimensione innovativa di questa pratica hacker è l'essere portatrice di un nuovo tipo di valore: quello dell'accesso. Tutta la cultura hacker è stata veicolo dell'idea che l'accesso fosse un valore in sé: non a caso l'etica hacker è organizzata intorno a principi di accesso e apertura. Ma il wardriving estende enormemente la portata del concetto. Nel momento in cui accesso vuol dire capacità di entrare in rete in qualunque punto del territorio ci si trovi, assume una connotazione politica non indifferente: la necessità di accedere allo spazio sociale digitale di internet e delle tecnologie della connettività. È questa una ulteriore conseguenza dell'incorporazione dello spazio digitale nello spazio fisico. Nel momento in cui il wardriver "buca" una rete per usare la connessione internet senza vincoli fisici, sta affermando il proprio diritto di poter accedere allo spazio sociale digitale rappresentato da chat, siti web, forum eccetera. Se c'è un valore di cui i wardriver sono portatori, questo è l'accesso diffuso e delocalizzato allo spazio sociale digitale.

Concludendo possiamo dire che è vero che i wardriver sono una piccola parte della comunità hacker, ma con la loro voglia di

appropriarsi dello spazio sociale e digitale del territorio esprimono una cultura tecnologica emergente intesa nel doppio significato del termine: che parte dal basso e che va crescendo di importanza, poiché è molto vicino il momento in cui le problematiche dell'accesso da loro sollevate interesseranno ognuno di noi.



RIFERIMENTI BIBLIOGRAFICI

- Adam, A. (2005) *Gender, Ethics and Information Technology*, Basingstoke, Palgrave Macmillan.
- Anderson, B. (1983) *Imagined Communities. Reflections on the Origin and Spread of Nationalism*, London, Verso; trad. it. *Comunità immaginate. Origini e fortuna dei nazionalismi*, Roma, Manifestolibri, 1996.
- Bakardjieva, M. (2005) *Internet Society. The Internet in everyday life*, London, Sage.
- Bennato, D. (2000) *Elementi per un'etnografia del pubblico dei media*, in M. Sorice, *Le comunicazioni di massa. Storia, tecniche, teorie*, Roma, Editori Riuniti, pp.283-295.
- Bennato, D. (2002) *Le metafore del computer. La costruzione sociale dell'informatica*, Roma, Meltemi.
- Bennato, D. (2004) *Wireless e comportamenti sociali emergenti*, in G. Frezza e M. Sorice (a cura di), *La TV che non c'è*, Salerno, Edizioni 10/17, pp. 175-190.
- Berra, M. e Meo, A. R. (2001), *Informatica solidale. Storia e prospettive del software libero*, Torino, Bollati Boringhieri.
- Bijker, W. (1995) *Of Bicycles, Bakelites and Bulbs*, Cambridge, Mit Press; trad. it. *La bicicletta e altre innovazioni*, Milano, McGraw-Hill, 1998.
- Boni, F. (2004) *Etnografia dei media*, Roma-Bari, Laterza.
- Cardano, M. (1997) *La ricerca etnografica*, in L. Ricolfi (a cura di), *La ricerca qualitativa*, Roma, La Nuova Italia Scientifica, pp. 45-92.
- Caronia, A. e Gallo, D. (1997) *Houdini e Faust. Breve storia del cyberpunk*, Milano, Baldini e Castoldi.
- Castells, M. (1996) *The Rise of the Network Society*, Oxford, Blackwell; trad. it. *La nascita della società in rete*, Milano, Università Bocconi Editore, 2002.

- Chandler, A. (1996) *The Changing Definition and Image of Hackers in Popular Discourse*, in «International Journal of the Sociology of Law», vol. 2, n. 24, pp. 229-251.
- Cohen, S. (1980) *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, London, Routledge.
- Dal Lago, A. e De Biasi, R. (a cura di) (2002) *Un certo sguardo. Introduzione all'etnografia sociale*, Roma-Bari, Laterza.
- Denegri-Knott, J. e Taylor, J. (2005) *The Labelling Game. A Conceptual Exploration of The Deviance in the Internet*, in «Social Science Computer Review», vol. 23, n. 1, pp. 93-107.
- Di Corinto, A. e Tozzi, T. (2002) *Hacktivism. La libertà nelle maglie della rete*, Roma, Manifestolibri.
- Faulkner, W. (2000) *The Power and the Pleasure? A Research Agenda for "Making Gender Stick" to Engineers*, in «Science Technology & Human Values», vol. 25, n. 1, pp. 87-119.
- Fici, A. (2004) *Mondo hacker e logica dell'azione collettiva*, Milano, Franco Angeli.
- Freschi, A. C. (2002) *La società dei saperi. Reti virtuali e partecipazione sociale*, Roma, Carocci.
- Gibson, W. (1984) *Neuromancer*, New York, Ace Science Fiction Books; trad. it. *Neuromante*, Milano, Editrice Nord, 1986.
- Gobo, G. (2001) *Descrivere il mondo. Teoria e pratica del metodo etnografico in sociologia*, Roma, Carocci.
- Haddon, L. (1992) *Explaining ICT Consumption: the Case of the Home Computer*, in R. Silvertone e E. Hirsch (a cura di), *Consuming Technologies: Media and Information in Domestic Spaces*, London, Routledge, pp. 82-96.
- Hafner, K. e Lyon, M. (1996) *Where Wizards Stay Up Late: The Origins of the Internet*, New York, Simon and Schuster; trad. it. *La storia del futuro. Le origini di Internet*, Milano, Feltrinelli, 1998.
- Hakken, D. (1999) *Cyborg@Cyberspace. An Ethnographer Looks to the Future*, London, Routledge.
- Halbert, D. (1997) *Discourses of Danger and the Computer Hacker*, in «The Information Society» vol. 13, n. 4, pp. 361-374.
- Hannemyr, G. (1999) *Technology and Pleasure. Considering Hacking Constructive*, in «First Monday», vol. 4, n. 2, disponibile all'indirizzo internet <http://www.firstmonday.org/issues/issue4_2/gisle/index.html>

- Himanen, P. (2001) *The Hacker Ethic and the Spirit of the Information Age*, New York, Random House; trad. it. *L'etica hacker e lo spirito dell'età dell'informazione*, Milano, Feltrinelli, 2003.
- Hine, Ch. (2000) *Virtual Ethnography*, London, Sage.
- Jordan T. e Taylor, P. (1998) *A Sociology of Hackers*, in «Sociological Review», vol. 4, n. 46, pp. 757-780.
- Lessig, L. (2004) *Free Culture*, New York, Penguin; trad. it. *Cultura libera*, Milano, Apogeo, 2005.
- Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*, Harmondsworth, Penguin; trad. it. *Hackers. Gli eroi della rivoluzione informatica*, Milano, Shake, 1999.
- Mackay, H. e Gillespie, G. (1992) *Extending the Social Shaping of Technology Approach: Ideology and Appropriation*, in «Social Studies of Science», vol. 22, pp. 685-716.
- MacKenzie, D. e Wajcman, J. (a cura di) (1999) *The Social Shaping of Technology (second edition)*, Buckingham, Open University Press.
- Merton, R. K. (1942) *The Normative Structure of Science*; trad. it. *La struttura normativa della scienza*, in ib., *La sociologia della scienza*, Milano, Franco Angeli, 1981, pp. 349-359.
- Meyer, G. R. (1989) *The Social Organization of the Computer Underground*, Master's thesis, Northern Illinois University, DeKalb.
- Moore, Sh. (1993) *Interpreting Audiences. The Ethnography of Media Consumption*, London, Sage; trad. it. *Il consumo dei media. Un approccio etnografico*, Bologna, Il Mulino, 1998.
- Nissenbaum, H. (2004) *Hacker and the Contested Ontology of Cyberspace*, in «New Media & Society», vol. 6, n. 2, pp. 195-217.
- Oudshoorn, N. e Pinch, T. (a cura di) (2003) *How Users Matter: The Co-Construction of Users and Technology*, Cambridge, Mit Press.
- Reed, L. (2002) *Governing (through) the Internet. The Discourse on Pathological Computer Use as Mobilized Knowledge*, in «European Journal of Cultural Studies», vol. 5, n. 2, pp. 131-153.
- Ryan, P. S. (2004) *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, in «Virginia Journal of Law & Technology», vol. 9, n. 7, pp. 1-57.

- Sandvig, Ch. (2004) *An Initial Assessment of Cooperative Action in Wi-Fi Networking*, in «Telecommunications Policy», vol. 28, pp. 579-602.
- Scifo, B. (2005) *Culture mobili. Ricerche sull'adozione giovanile della telefonia cellulare*, Milano, Vita e Pensiero.
- Silverstone, R., Hirsch, E. e Morley, D. (1991) *Listening to a Long Conversation. An Ethnographic Approach to the Study of Information and Communication Technologies at Home*, in «Cultural Studies», vol. 5, n. 2, pp. 204-227.
- Sterling, B. (1992) *The Hacker Crackdown. Law and Disorder on the Electronic Frontier*, London, Bantam; trad. it. *Giro di vite contro gli hacker*, Milano, Shake, 1996.
- Taylor, P. A. (1999) *Hackers. Crime in the Digital Sublime*, London, Routledge.
- Thomas, D. (2002) *Hacker Culture*, Minneapolis, University of Minnesota Press.
- Thomas, D. (2004) *Rethinking the Cyberbody: Hackers, Viruses, and Cultural Anxiety*, in M. Sturken, D. Thomas e S. Ball-Rokeach (a cura di), *Technological Visions. The Hopes and Fears that Shape New Technologies*, Philadelphia, Temple University Press, pp. 219-239.
- Thomas, J. (2005) *The Moral Ambiguity of Social Control in Cyberspace: a Retro-Assessment of the Golden Age of Hacking*, in «New Media & Society», vol. 7, n. 5, pp. 599-624.
- Turgeman-Goldschmidt, O. (2005) *Hacker's Accounts. Hacking as a Social Entertainment*, in «Social Science Computer Review», vol. 23, n. 1, pp. 8-23.
- Turkle, S. (1984), *The Second Self: Computers and the Human Spirit*, New York, Simon & Schuster; trad. it. *Il secondo io. Il computer e lo spirito umano*, Milano, Frassinelli, 1985.
- Urry, J. (1995) *Consuming Places*, London, Routledge.
- Urry, J. (2000) *Sociology Beyond Societies: Mobilities for the Twenty-First Century*, London, Routledge.
- Wark, M. (2006) *Hackers*, in «Theory Culture & Society», vol. 23, n. 2-3, pp. 320-322.
- Weizenbaum, J. (1976) *Computer Power and Human Reason. From Judgement to Calculation*, New York, W. H. Freeman; trad. it. *Il potere del computer e la ragione umana*, Torino, Edizioni del Gruppo Abele, 1987.

- Williams, R. (1974) *Television: Technology and Cultural Form*, London, Fontana; trad. it. *Televisione. Tecnologia e forma culturale*, Roma, Editori Riuniti, 2000.
- Williams, R. e Edge, D. (1996) *The Social Shaping of Technology*, in «Research Policy», vol. 25, pp. 856-899.