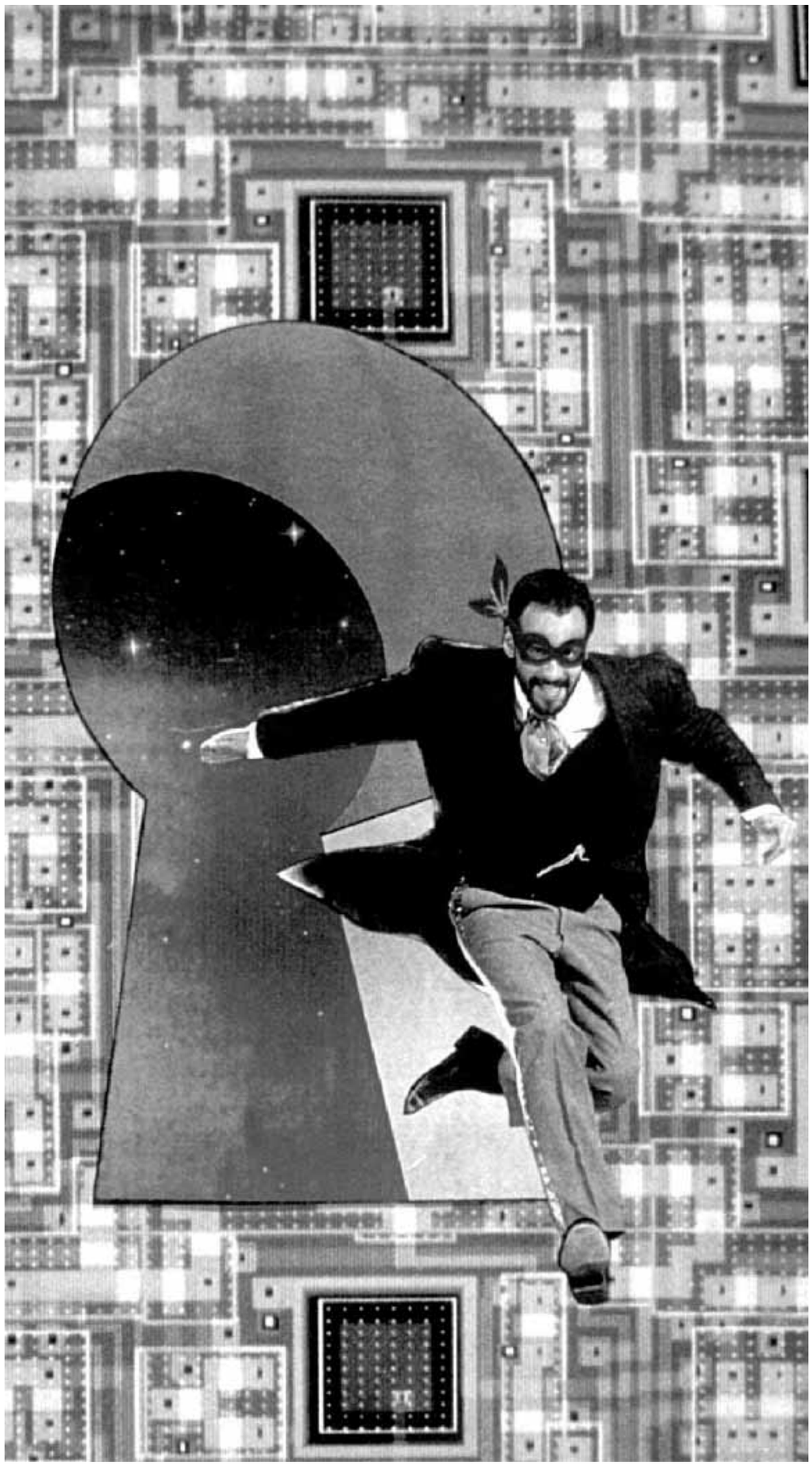

pagine web è stata tra le cause della grande visibilità che gli *hackers* hanno assunto nell'opinione pubblica mondiale negli utlimi due anni. Per qualche tempo clamorosi errori di gestione dei siti Internet, anche di istituzioni importanti, hanno permesso a chiunque fosse dotato di un po' di intelligenza informatica e di qualche risorsa tecnica di fare e disfare praticamente tutto. Così gli *hackers* sono riusciti a modificare i siti della Cia, della Nasa, dell' Aeronautica militare statunitense, del governo indonesiano per protestare contro la repressione a Timor Est e persino il sito del pellicciaio Kriegsman, invaso da technoanimalisti.

Anche in Europa ci sono stati attacchi motivati politicamente contro siti Internet, come quelli, in Gran Bretagna, contro le pagine dei Laburisti e dei Conservatori. Ma si tratta di episodi tutto sommato isolati, almeno a livello di opinione pubblica. In Europa il fenomeno *hacker* non ha assunto in modo così aperto quell'aspetto di sfida alla società organizzata che ha invece negli Stati Uniti. O meglio si è sviluppato in modo diverso, e l'attenzione delle polizie (ma anche dei servizi segreti) si è focalizzata più sull'uso delle reti da parte dei gruppi cosiddetti «antagonisti» che sugli *hackers* veri e propri. In effetti prima con le BBS (Boarding Board System, un sistema di comunicazione elttronica tramite computer ancora molto diffuso), poi con Internet i gruppi della sinistra radicale europea e quelli di una parte della destra anche eversiva hanno creato una ragnatela di rapporti e relazioni che hanno preoccupato i governi al punto che, in una relazione al Parlamento di un paio d'anni fa sull'attività dei nostri servizi di sicurezza, un capitoletto era esplicitamente dedicato all'uso dei sistemi di comunicazione elettronica da parte di questi attivisti.

Non che l'Europa sia stata immune da fenomeni analoghi a quelli dell' hackerismo statunitense. Hanno avuto soltanto minore notorietà per varie ragioni. Prima di tutto perché sono stati complessivamente sottovalutati, poi perché le opinioni pubbliche europee, e quella italiana in particolare, sono meno sensibili alla fascinazione dei technofuorilegge. Kevin Mitnick e Tsutomu Shimomura sono i protagonisti di un *feuilletton* gettonatissimo negli Usa, protagonisti di almeno tre libri (*Takedown* scritto dallo stesso Tsutomu Shimomura con John Markoff, *The Fugitive Game* di Jonathan Littman e *The Cyberthief and The Samurai* di John Goodell), centinaia di articoli, servizi televisivi e probabilmente un film. Eppure sono rispettivamente solo un *hacker* particolarmente abile (sfuggito per anni alle ricerche di Secret Service, Fbi e innumerevoli altri corpi di polizia) e un esperto di sicurezza informatica nel cui computer al San Diego Supercomputer Center Mitnick riuscì ad entrare in segno di sfida il giorno di Natale del 1994. Questa intrusione gli costò l'arresto, dopo essere stato localizzato da Shimomura a conclusione di due mesi di inseguimenti nel ciberspazio.

In Europa, il pathos di storie come questa è poco percepito a livello sociale, e questo fa sì che il fenomeno *hacker* sia relegato a poco più di un affare per specialisti. Ma il raduno degli *Hackers In Progress* di Amsterdam dimostra che non siamo affatto di fronte ad episodi marginali o transitori, né a fenomeni sporadici. L'antagonismo sociale di molti *hackers* si accompagna infatti sempre ad una formazione tecnica superlativa, ne fa vere e proprie avanguardie che, come tutte le avanguardie, portano in loro i germi della devianza ma anche e soprattutto quelli del cambiamento.

Un'immagine fantasiosa di uno «scorridore» della rete informatica. Gli "hackers" si sono riuniti in convegno mondiale pochi giorni fa. «Isolare chi con il suo computer vuole sabotare: noi siamo rivoluzionari»

Ecco perché ad Amsterdam, ma anche al contemporaneo raduno di New York (intitolato *Beyond HOPE*, che vuol dire «oltre la speranza» ma dove HOPE è anche una sigla che sta per *Hackers On Planet Earth*, *hackers* sul pianeta Terra), l'enfasi di molti partecipanti era sul distinguersi dai *crackers*, quelli che entrano nei computer con intenzioni puramente distruttive.

«Chiunque può far saltare un computer. È più intelligente trovare il modo per non farlo saltare» ha dichiarato al *New York Times* "Cheshire", uno dei partecipanti al raduno di New York. "Cheshire" è uno pseudonimo, perchè gli *hackers*, anche quando fanno cose perfettamente legittime, preferiscono identificarsi con le personalità che assumono quando sono al computer. C'è chi si chiama "Binary", una parola alla portata della comprensione di chiunque, ma anche c'è una "Terrorisct", in un gioco di parole difficilmente comprensibile agli iniziati che mette insieme *terrorist* e RISC, la sigla che indica l'architettura di un particolare tipo di processore. Questo bisogno di legalità è anche la conseguenza di un gap generazionale che si è creato all'interno del mondo *hacker*. I primi *hacker* sono ormai signori che stanno entrando nella età di mezzo, come John Draper, un 54enne americano conosciuto anche come *Cap'n Crunch*, il nome di uno snack per bambini nelle cui confezioni anni addietro c'era un fischietto. Modificando quel fischietto Draper era riuscito ad imitare il tono di chiamata a 2600 Hz del sistema telefonico ATT, facendo così telefonate gratis in tutto il mondo. Altri sono invece entrati a pieno titolo nel mondo della produzione come lo stesso organizzatore del campeggio *hacker*, Maurice Wessling, socio di XS4All, uno dei maggiori fornitori Internet olandesi. E anche molti degli *hacker* più giovani hanno un occhio di riguardo per le grandi società. Sanno di essere in qualche modo sulla linea di partenza giusta per ben remunerate carriere come consulenti di sicurezza e testatori di sistemi. Un *business* che sta affaermandosi tra gli *enfant prodige* del ciberspazio. Ma l'elemento di alterità resiste forte in molti gruppi che si compiacciono nel restare in bilico sulla sottile linea che li divide dai *crackers*. Come quei tedeschi che hanno messo a punto delle tecniche per sfruttare i buchi nella sicurezza della tecnologia ActiveX della Microsoft per intercettare le transazioni bancarie. O quell'altro gruppo, sempre tedesco, che sul giornalino *on line* di *Hackers In Progress* spiega il suo progetto per scoprire il codice attraverso il quale le banche europee elaborano il PIN (Personal Identification Number, il codice segreto che dovete battere quando usate la carta di credito per prelevare contanti dai distributori automatici) che garantisce la sicurezza dei loro clienti.