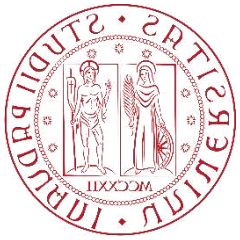

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DEI BENI CULTURALI:

Archeologia, Storia dell'arte, del cinema e della musica

Corso di laurea magistrale in

SCIENZE DELLO SPETTACOLO E PRODUZIONE MULTIMEDIALE

Hacking Hollywood.
Gli hacker come nuovo soggetto cinematografico, 1980-2000

(Hacking Hollywood. Hackers as a new film topic, 1980-2000)

Relatore

Prof. Federico Mazzini

Correlatore

Prof. Alberto Zotti

Laureando

Luca Midena

Anno Accademico 2022/2023

INDICE

INTRODUZIONE

L'hacking, generalmente definito come l'accesso non autorizzato a sistemi e reti informatiche, è diventato un tema sempre più rilevante nella società contemporanea. Negli ultimi decenni, l'hacking è diventato un fenomeno culturale, con una propria serie di valori, etica ed estetica. Di conseguenza, la rappresentazione degli hacker nel cinema americano è diventata oggetto di indagine accademica. L'obbiettivo di questa tesi è di fornire una panoramica della rappresentazione degli hacker nel cinema americano tra gli anni Ottanta e gli anni Duemila. La rappresentazione degli hacker nel cinema americano si è evoluta nel tempo, riflettendo il cambiamento di atteggiamento nei confronti dell'hacking e della tecnologia in generale. Durante i loro primi passi come comunità e sottocultura statunitense negli anni Ottanta, gli hacker diventarono soggetto cinematografico, inseriti in film e fatti personaggi. In film come *Wargames* (1983) e *Sneakers* (1992), gli hacker erano eroi che usavano le loro competenze tecniche per salvare il mondo dalla guerra nucleare e dall'avidità aziendale. Tuttavia, negli anni Novanta e Duemila, la rappresentazione degli hacker è diventata più ambigua. In film come *The Net* (1995) e *Hackers* (1995), gli hacker sono stati rappresentati sia come eroi che come cattivi, capaci di salvare o distruggere il mondo a seconda delle loro motivazioni. In film più recenti, come *The Girl with the Dragon Tattoo* (2011), gli hacker sono rappresentati come personaggi complessi e moralmente ambigui, che usano le loro capacità per smascherare corruzione e ingiustizia. L' evoluzione della rappresentazione degli hacker nel cinema statunitense è importante per molteplici motivi. Esso fornisce una visione del significato culturale dell'hacking, la possibilità di capire come l'hacking è percepito dal pubblico in generale, un concreto aiuto nell'identificazione e analisi di miti e narrazioni culturali alla base della comprensione dell'hacking e della tecnologia.

Alla base di questo studio vi è l'analisi dell'evoluzione della rappresentazione degli hacker e della loro cultura nel cinema hollywoodiano. Prendendo in riferimento un periodo storico preciso, dagli anni Ottanta agli anni Duemila, vi è stata fatta una scelta di diversi casi di studio. La motivazione che mi ha spinto ad approfondire tale tema è principalmente una. Essa è l'interesse nei confronti della pratica dell'hacking e della sua cultura derivato dal desiderio di comprendere più a fondo questo aspetto ormai internazionalizzato. L'obiettivo di questa tesi di laurea è quello di fornire un'analisi accurata sulle molteplici sfaccettature della rappresentazione degli hacker e della loro cultura nel

cinema hollywoodiano durante il periodo storico preso in considerazione. L'elaborato, in questo modo, mira a comporre un quadro completo e preciso su di esse.

La tesi è articolata in due capitoli. Nel primo capitolo viene fornita un'introduzione alla cultura e alla pratica dell'hacking, attraverso un breve excursus storico. Il secondo capitolo si concentra sull'analisi dei vari casi di studio e sulle tematiche che portano alla luce. Grazie a questo lavoro di compilazione è stato possibile rendere chiare le molteplici sfaccettature dell'evoluzione della rappresentazione degli hacker e della loro cultura nel cinema hollywoodiano, seppur per un breve periodo storico, risultati che saranno esposti dettagliatamente nelle conclusioni finali di questa tesi.

CAPITOLO 1

Evoluzione storica dell'hacking negli USA

Nel mondo interconnesso di oggi, il termine "hacker" ha una certa valenza mistica. Evoca immagini di individui con straordinarie abilità informatiche che scavano in profondità nel regno digitale per scoprire verità nascoste o creare scompiglio in sistemi ignari. Tuttavia, è essenziale comprendere la vera natura dell'hacking e capire il suo profondo impatto sulla società contemporanea. In questo capitolo si andrà a fondo negli annali della storia degli hacker, esplorandone le origini, le motivazioni e l'impatto nel corso degli anni. In un mondo in cui la tecnologia gioca un ruolo sempre più integrante nelle nostre vite, il tema dell'hacking è diventato al contempo affascinante e preoccupante. L'evoluzione storica dell'hacking negli Stati Uniti è un viaggio avvincente che mostra l'incessante ricerca di conoscenza e potere. Dagli inizi del *phreaking* telefonico e degli hobbisti del computer negli anni Sessanta ai sofisticati attacchi informatici dei giorni nostri, il panorama dell'hacking ha subito una notevole trasformazione. Questa evoluzione è stata determinata da una combinazione di progressi tecnologici, cambiamenti sociali e crescente necessità di sicurezza. L'esplorazione del contesto storico dell'hacking non solo fornisce uno sguardo alla mente di coloro che hanno cercato di sfruttare le vulnerabilità, ma fa anche luce sulle misure adottate per contrastare le loro azioni. Questo capitolo iniziale mostra l'intrigante mondo dell'hacking, espone le sue origini ed esamina il suo impatto sugli Stati Uniti nel corso della storia.

1.1. I phone phreaks, le origini

Sebbene la definizione odierna del termine "'hacking"[1] sia generalmente associata ai computer e ai sistemi informatici, prima del loro avvento questa pratica era comunque presente. Perciò per comprendere l'essenza dell'hacking, è necessario scavare nelle sue origini negli anni Sessanta e Settanta. Si tratta del periodo cruciale in cui cominciano a formarsi le basi di questa pratica. In quel

[1] L'attività di accedere al sistema informatico di qualcun altro senza autorizzazione per scoprire informazioni o fare qualcosa di illegale. (https://dictionary.cambridge.org/dictionary/english/hacking, ultima consultazione: 30 agosto 2023)

periodo stavano nascendo i sistemi informatici e un piccolo gruppo di individui curiosi iniziò a esplorarne i limiti.

Questi primi pionieri, principalmente giovani di classe media tra i 13 e i 25 anni, erano spinti dall'insaziabile desiderio di capire il funzionamento interno di queste tecnologie nascenti. Scoprirono come utilizzare le macchine non solo per gli scopi previsti, ma anche per altre funzioni che i loro creatori non avevano immaginato. Scoprirono vulnerabilità nei sistemi informatici che consentivano loro di penetrare nei sistemi stessi e di modificare ciò che accadeva al loro interno. Questo gruppo si espanse e si evolse in quelli che in futuro saranno considerati gruppi hacker. Questo primo gruppo di appassionati, che seguiva le orme dei radio amatori di inizio secolo, si autodefinirono "phone phreaks" (ossessionati di telefoni). Armati di intelletto, creatività e di un arsenale di strumenti fatti in casa, questi primi appassionati si sono imbarcati in una ricerca per scoprire il potenziale nascosto dei sistemi informatici. I *phreak* erano persone che smontavano le cose, le studiavano e cercavano di migliorarle. Erano esploratori, curiosi di sapere come funzionavano le cose e desiderosi di saperne di più. Tra le figure di spicco si ricordano anche dei giovanissimi Steve Wozniak e Steve Jobs, fondatori di Apple, che iniziarono il loro percorso come *phreak* prima di rivoluzionare l'industria tecnologica[2].

Uno dei fattori importanti alla costruzione della comunità *phreak* fu la fondazione nel 1972 della *Youth International Party Line*, *YIPL*, una newsletter diretta da Abbie Hoffman e da Alan Fierstein. Questa rivista fu fondamentale nell'ampliamento della comunità di appassionati, fornendo informazioni tecniche difficilmente reperibili utili ai neofiti e schede tecniche su modifiche di una varietà di apparecchi. Inoltre, la YIPL spronava i suoi lettori a riconoscere come loro "nemico" la AT&T, American Telephone and Telegraph Company, o come veniva chiamata all'interno di essa e tra i vari *phreak*, la compagnia Bell. Tra le varie informazioni di carattere tecnico che forniva la YIPL c'erano dettagli su come costruire o modificare, in base alle contromisure applicate negli anni dalla AT&T, le variopinte "*box*". Già utilizzate negli anni precedenti, questi apparecchi fai-da-te avevano come obbiettivo ultimo della maggior parte di queste "scatole" era quello di rendere le chiamate gratuite, in un modo o nell'altro sfruttando vari elementi dei sistemi telefonici casalinghi e non dell'epoca[3]. La più famosa tra queste era la "*blue box*", un apparecchio 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. Il suo impiego era relativamente semplice. Bastava avvicinare la *blue box* alla cornetta del telefono ed emettendo una frequenza di 2.600 Hz si ingannava il sistema,

[2] S. Levy, *Hackers: Heroes of the Computer Revolution* (1984), O'Reilly Media, Sebastopol 2010
[3] Cfr. F. Mazzini, *Hackers*, Storia e pratiche di una cultura, 2023, p. 51

facendogli credere che il ricevitore fosse stato riagganciato, rendendo la successiva chiamata gratuita.[4]

Questo scambio di informazioni di carattere tecnico fu una delle ragioni per cui la comunità hacker, nonostante non fosse omogena negli Stati Uniti, si considerava un'alternativa al mercato e alla cultura dominante di quegli anni. Anche grazie al fatto che gli articoli pubblicati nei suoi tredici anni di vita provenivano in gran parte dagli stessi lettori ed erano scelti per la loro originalità, sia rispetto a tecniche già conosciute sia rispetto a quella che era percepita come la morale dominante.[5] Nel corso degli anni la newsletter 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, la rivista coprirà molti campi, come la produzione di fuochi d'artificio o droghe, la modifica dei contatori domestici, parchimetri, decoder televisivi, la scassinatura dei lucchetti e, dalla fine degli anni Settanta, l'accesso illecito ai sistemi informatici.[6] Riviste specializzate come *YIPL*, che nel 1973 cambiò il proprio nome in *TAP*, saranno di ispirazione a nuove riviste successive, principalmente *Phrack Magazine* e *2600.The Hacker Quarterly*. Esse diffonderanno alla neonata cultura hacker elementi nati da quella *phreak*.[7]

Altro aspetto chiave per lo sviluppo di queste comunità e la proliferazione di questo tipo di informazioni furono le "*party lines*": chiamando allo stesso tempo numeri di servizio non più in uso, diversi utenti potevano parlare in contemporanea, scambiandosi informazioni tecniche, notizie sulle imprese di alcuni *phreaks* particolarmente talentuosi o su nuovi numeri telefonici di interesse, e semplici chiacchiere.[8]

Oltre alla ricerca di conoscenza e dell'esperienza di novità, un'ulteriore motivazione che spingeva i *phreaks* nelle loro imprese era quella di riconoscimento. Difatti, gli sforzi individuali venivano spesso premiati semplicemente con la pubblicazione del proprio lavoro sotto pseudonimo, una pratica mantenuta in seguito dalle comunità hacker. La soddisfazione derivava dall'essere consapevoli che la propria genialità contribuiva alla conoscenza collettiva degli appassionati, piuttosto che dalla ricerca di un riconoscimento da parte di un'autorità centrale. L'aspetto davvero notevole è che il culto delle competenze tecniche e l'enfasi sull'esperienza pratica non hanno creato una mentalità elitaria. Al contrario, ci fu una forte attenzione a coltivare i neofiti attraverso spiegazioni ripetute e riferimenti ai numeri delle riviste per articoli più approfonditi. L'obiettivo era incoraggiare i principianti a seguire

[4] Federico Mazzini, *Hackers, Storia e pratiche di una cultura*, Editori Laterza, Bari 2023, pp. 49-51
[5] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 55
[6] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 52
[7] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 68
[8] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 52

le orme degli esperti, anche se non avevano competenze tecniche. Vennero addirittura organizzate delle convention, in cui venivano distribuite audiocassette con registrazioni dei toni delle scatole blu, in modo che chiunque non fosse in grado di costruirne una propria potesse comunque partecipare pienamente a questo mondo elettrizzante. Queste comunità prosperarono sulla conoscenza condivisa e sul cameratismo piuttosto che sull'esclusività o sulla gerarchia e esattamente questo spirito vibrante alimentò la cultura hacker dei primi tempi, dove ogni membro ha le stesse opportunità di contribuire con i propri talenti e le proprie idee per superare i limiti e sbloccare il potenziale non sfruttato della tecnologia.[9]

Saldo fondamento della coesione del gruppo *phreak* fu la nascita di prime celebrità all'interno di esso. Oltre ai vari membri non vedenti, tra cui spicca la figura di Josef C. Engressia, meglio conosciuto nella comunità come Joybubbles, il *phone phreak* più ricordato è certamente il veterano del Vietnam John T. Draper soprannominato "Captain Crunch". Ottenne questo appellativo utilizzando un fischietto giocattolo delle scatole di cereali "Cap'n Crunch" per generare il tono a 2600 Hz.[10] La sua celebrità all'interno della comunità *phreak* fu dovuta soprattutto alla sua particolare attenzione nella costruzione della propria immagine attraverso interviste e lettere alla *YIPL* e altre pubblicazioni. Considerato da molti il "padre del *phreaking*"[11], Draper fu uno dei primi ad essere ad avere disavventure legali con le autorità statunitensi. A partire dal 1972 e durante il resto degli anni Settanta infatti, fu condannato per frode telefonica e per un periodo messo in libertà vigilata. Nonostante ciò, Draper non demorse e verso la fine del decennio virò il suo interesse all'informatica e alla programmazione.[12]

Gli eventi di phreaking degli anni Settanta hanno costituito le basi fondamentali per l'inizio del fenomeno dell'hacking pochi anni dopo. L'audacia e l'innovazione dimostrate da quei pionieri hanno spinto i confini della tecnologia e della comunicazione. La pratica del phreaking degli anni Settanta ha fatto luce su difetti significativi dell'infrastruttura di telecomunicazione, portando in ultima analisi a miglioramenti della sicurezza. Le rivelazioni fatte dai *phreaks* costrinsero le società di telecomunicazioni a rivalutare le debolezze del loro sistema e a prendere provvedimenti per correggerle. Le conoscenze acquisite in quei primi anni hanno gettato le basi per lo sviluppo di sistemi sicuri e per l'affermazione dell'hacking etico come professione legittima e rispettata

[9] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., pp. 55-57
[10] Michel E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", *M. E. Kabay, PhD*, http://www.mekabay.com/overviews/history.pdf (ultima consultazione: 30 agosto 2023);
[11] Gordon R. Meyer, *The Social Organization of the Computer Underground* (1989), Northern Illinois University, DeKalb 2009;
[12] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 60

1.2. Gli anni Ottanta e la nascita della cultura hacker

All'inizio degli anni Ottanta, gli Stati Uniti stavano vivendo un periodo estremamente favorevole nel settore dell'informatica, grazie soprattutto alla direzione presa da molte società dell'industria. Difatti, già a partire dalla fine degli anni Settanta con l'introduzione nel mercato dei personal computer, in primis l'Altair 8800 della MITS (1975) e l'Apple II della Apple (1977), l'informatica lasciava centri di ricerca e università e entrava nelle case degli americani. Tendenza che appunto continuò negli anni a seguire con la rapida evoluzione del comparto hardware, nel 1981 IBM presenta il suo primo personal computer, l'IBM PC, che ben presto si afferma come standard, mentre tre anni più tardi Apple presenta il computer Macintosh, dotato di interfaccia grafica e mouse. Riguardo la sezione software bisognerà aspettare il 1985 quando la Microsoft, fondata solamente dieci anni prima, rilasciò la prima versione di Windows, che forniva un'interfaccia utente grafica per i computer IBM compatibili. Esattamente in questo ambiente propizio, si sviluppò la cultura hacker, intersecandosi con quella informatica.

Hackerare significava trovare un modo, qualsiasi modo che funzionasse, per far accadere qualcosa, risolvere un problema, inventare il prossimo brivido. C'era una spavalderia associata all'essere un hacker, un'identità indossata come un distintivo d'onore.

A definire questi primi hacker non è stato solo l'attaccamento singolo al proprio operato, ma anche l'adesione a un'ideologia informalmente chiamata "etica hacker". Questo credo, ben documentato dall'opera *Hackers Heroes of the Computer Revolution*[13] di Levy, comprendeva diversi elementi: l'impegno per l'accesso totale e libero ai computer e alle informazioni, la convinzione dell'immenso potere dei computer di migliorare la vita delle persone e di creare arte e bellezza, la diffidenza nei confronti dell'autorità centralizzata, il disprezzo per gli ostacoli eretti contro il libero accesso all'informatica e l'insistenza sul fatto che gli hacker dovessero essere valutati solo in base a criteri di virtuosità tecnica e di realizzazione. [14]

Nel gergo dell'underground informatico, il termine "hacking" si riferisce all'accesso e all'esplorazione di sistemi e reti informatiche. Il termine comprende sia l'atto che i metodi utilizzati per ottenere account utente validi sui sistemi informatici. Il termine "hacking" si riferisce anche all'attività che si svolge una volta ottenuto l'accesso a un altro computer. Poiché il sistema viene utilizzato senza autorizzazione, l'hacker non ha generalmente accesso ai manuali operativi e alle altre risorse disponibili per gli utenti legittimi. Pertanto, l'hacker deve sperimentare i comandi ed esplorare i vari

[13] S. Levy, *Hackers: Heroes of the Computer Revolution* (1984), cit.
[14] Helen Nissenbaum, "Hackers and the contested ontology of cyberspace", *New Media & Society*, vol. 6, n. 2 (2004), p. 197

file per comprendere e utilizzare efficacemente il sistema. L'obiettivo è quello di esplorare e sperimentare il sistema che è stato inserito. Esaminando i file e, forse, con un po' di programmazione intelligente, l'hacker può essere in grado di ottenere informazioni protette o privilegi di accesso più potenti.[15]

In seguito, un'altra ottima descrizione dell'essenza hacker degli anni Ottanta fu scritta su "A Novice's Guide to Hacking", un file di testo redatto dal noto membro del gruppo hacker Legion of Doom "The Mentor". In esso vi sono elencate le regole base dell'hacker spiegate per un target di novizi della pratica. Il solo scopo deve essere l'esplorazione e la raccolta di sapere, non bisogna danneggiare alcun sistema o cambiare dati al suo interno.[16]

Questo file fornisce anche indicazioni su come cominciare ad effettuare l'hacking. Il luogo perfetto all'epoca sono gli istituti universitari, vista la facilità di accesso e la scarsa sicurezza. La fase iniziale consisteva nella composizione di un numero di telefono sul computer, per connettersi alla rete tramite un modem. Ad avvenuta connessione, compariva un terminale in cui serviva inserire il NUA, Network User Address. In base alla distanza del computer a cui ci si connetteva il costo della telefonata variava. Per esentarsi dal pagarla, la maggioranza dei danni attribuiti nei futuri processi contro gli hacker, venivano utilizzati diversi espedienti grazie a dispositivi e codici. Inserito il NUA, bastava inserire nome utente e password per accedervi. Dal momento che la sicurezza non era considerata un fattore fondamentale, almeno nei primi anni Ottanta, le password erano facili da indovinare e la comunità degli hacker si scambiavano informazioni su quelle più regolarmente utilizzate.[17]

Con il passare del tempo, la comunità hacker mutò e si popolò di individui con un ampio spettro di motivazioni personali, abilità e attività. Il risultato di questo mutamento è descritto nel Jargon File (1975-). Questo documento di testo, che definisce e traduce il gergo hacker, fornisce otto diverse definizioni di hacker, che vanno dal concetto di utente esperto di computer degli anni Sessanta alle applicazioni contemporanee di qualcuno che tenta maliziosamente di "scoprire informazioni sensibili curiosando". L'enfasi sull'accesso non autorizzato ai sistemi informatici è la chiave della nozione di hacker che è stata promulgata dai media popolari durante l'interezza della storia di questa pratica. Gli hacker spesso si distinguono l'uno dall'altro usando i termini "white-hat", "black-hat" o "grey hat". I primi sono generalmente hacker "etici" che lavorano per trovare errori nei sistemi e nei programmi informatici e possono utilizzare l'ingresso non autorizzato nei sistemi per favorire l'industria della sicurezza informatica. Al contrario, la seconda categoria cerca gli stessi errori per ottenere l'accesso

[15] G. R. Meyer, *The Social Organization of the Computer Underground* (1989), cit., pp. 24-25
[16] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 75
[17] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., pp. 75-76

alle informazioni o danneggiare un sistema, e spesso sono al centro dell'attenzione dei media e delle forze dell'ordine. L'ultima tipologia di hacker si colloca a metà strada, con motivazioni poco chiare o mutevoli a seconda della situazione specifica.[18]

Qualunque sia la tecnica utilizzata, la pratica consiste nel compiere determinate azioni non consentite (accesso al computer) e alterare le tecnologie per creare nuove azioni (accesso). Gli hacker di questo periodo iniziale hanno adottato pratiche che testimoniano l'attenzione all'esplorazione intellettuale. Enfatizzare l'esplorazione intellettuale come componente chiave dell'età dell'oro non significa che l'hacking come cracking fosse "innocente". Come per i *phreaks*, i soggetti colpiti andavano incontro a costi per riparare i sistemi che erano stati violati o semplicemente per rintracciare coloro che si erano introdotti. A volte i danni venivano causati quando la competenza di un hacker non era così grande come si pensava. Il crimine informatico, quindi, in questo periodo, era una categoria confusa che di solito si riferiva a quelle violazioni elettroniche illecite che venivano sempre più criminalizzate, indipendentemente dalle conseguenze o dalle motivazioni dell'intrusione. Se l'età dell'oro dell'hacking è stata davvero l'età dell'oro dell'hacking-come-cracking, allora è cambiata quando l'hacking ha iniziato a spostarsi su una serie di fronti. La criminalizzazione del cracking è proseguita in molti Paesi, ponendo gli hacker-come-cracker in un rapporto diverso con le autorità di sicurezza e con la possibilità di azioni penali, la cui consapevolezza è cresciuta nelle comunità di hacker. [19]

L'ambiente accademico in cui è emerso l'hacking ha contribuito notevolmente all'etica della collaborazione su obiettivi condivisi attraverso la competizione per il riconoscimento. L'aspetto distintivo è stata l'estensione di processi sociali riconoscibili in ambito accademico a questo in questa nuova area tecnica. Gli hacker erano, allo stesso tempo allo stesso tempo, erano largamente indifferenti al riconoscimento formale all'interno dell'accademia o dell'industria. Il riconoscimento dei propri pari era ciò che contava.[20]

Come nel caso dei *phone phreaks* con le party lines, gli hacker necessitavano di un luogo di ritrovo per scambiarsi informazioni e tenersi in contatto. Questo ruolo venne ricoperto dall'aumento della popolarità dei BBS, bulletin board system, o CBBS, computer bulletin board system. Istituite nel 1978 da Ward Christensen e Randy Suess, il sistema BBS, dei personal computer dotati di un modem telefonico che ospitavano bacheche elettroniche, divenne ben presto il metodo per comunicare nel

[18] Thomas J. Holt, "Hacks, cracks, and crime: an examination of the subculture and social organization of computer hackers", *UMSL Libraries*, https://irl.umsl.edu/dissertation/616?utm_source=irl.umsl.edu%2Fdissertation%2F616&utm_medium=PDF&utm_campaign=PDFCoverPages (ultima consultazione: 30 agosto 2023), pp. 6-8
[19] Tim Jordan, "A Genealogy of Hacking", *Convergence: The International Journal of Research into New Media Technologies*, vol. 23, n. 5 (2017), p. 534
[20] Wark McKenzie. "Hackers." *Theory, Culture & Society*, vol. 23, no. 2-3 (2006), p.321

nuovo mondo informatico dei computer, contando non solo hacker e aspiranti tali. Il loro funzionamento era relativamente semplice: gli utenti possono collegarsi a una BBS componendo, con il proprio computer e modem, il numero di telefono a cui il BBS è collegata. Dopo aver effettuato il login fornendo un nome utente e una password validi, l'utente può lasciare messaggi agli altri utenti del sistema. Questi messaggi non sono privati e chiunque chiami il BBS può leggerli e rispondere liberamente.[21] Nel corso degli anni Ottanta questo sistema si aggiunse di varie migliorie tra cui una "base messaggi", un'area dove chi chiama lascia messaggi indirizzati ad altri utenti, e una "area files" dove gli utenti potevano scaricare programmi e file di testo.[22]

Nel 1983 fu un anno particolarmente interessante per il mondo dell'hacking. Quest'ultimo cominciò ad essere notato dai media tradizionali, grazie anche all'uscita nelle sale del primo film a riguardo *Wargames*[23]. A braccetto con l'entusiasmo per questa opera hollywoodiana, ci fu un altro evento che cominciò a svegliare i "giganti addormentati", il grande pubblico e in particolar modo il governo statunitense. In seguito alle loro azioni dell'anno precedente[24], il gruppo di teenager chiamato "414s" venne arrestato nei primi mesi del 1983 e nei mesi successivi venne riportato dai media nazionali. Difatti, i "414s" si erano introdotti in molti sistemi statunitensi, tra cui spiccano lo Sloan-Kettering Cancer Center di New York e la base militare di Los Alamos. Il sistema che utilizzarono per fare ciò era relativamente semplice e non per casualità molto simile a quello utilizzato in *Wargames*. Esso consisteva in delle chiamate a numeri casuali effettuate da un computer collegato a un modem. Alla fine di questo processo, lo schermo mostrava i numeri che avevano risposto e che quindi erano un computer connesso alla rete. A quel punto per ottenervi l'accesso bastava inserire la password, che molto spesso corrispondevano a quelle di fabbrica e perciò facilmente reperibili in BBS o manuali tecnici.[25] Sebbene la maggior parte delle attività effettuate una volta inseritisi furono innocue (o quasi), le vicende del gruppo "414s" e il successo di *Wargames* diedero una spinta alle crescenti comunità hacker e soprattutto alla sua controparte legislativa.

Questo vento di cambiamento venne subito riportato dalle riviste specifiche della sottocultura hacker, *2600.The Hacker Quarterly*[26] (fondata nel 1984) e *Phrack Magazine*[27] (fondata nel 1985). Questo passaggio da una pratica di nicchia appartenente a bacheche digitali e laboratori universitari all' attenzione dei media, tra stampa, talk shows e fiction hollywoodiana finì per segnare in modo deciso questo mondo e questa cultura. In seguito alle varie discussioni pubbliche sulle azioni del gruppo

[21] G. R. Meyer, *The Social Organization of the Computer Underground* (1989), cit., p.13
[22] G. R. Meyer, *The Social Organization of the Computer Underground* (1989), cit., pp. 40-43
[23] *Wargames – Giochi di guerra* (WarGames, John Badham, United Artists, USA 1983)
[24] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 42
[25] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit. p. 78
[26] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 43
[27] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 45

"414s", il Congresso cominciò la valutazione di una nuova legge in materia, il *Computer Fraud and Abuse Act*. Fino a quel momento, la legislazione statunitense era priva dei mezzi specifici per punire le varie tipologie di crimini informatici. Il semplice ingresso illecito in uno spazio virtuale non costituiva in sé un crimine e i tentativi di applicare le leggi esistenti sulla violazione di domicilio non andavano per nulla bene. Lo stesso valeva per le leggi sul furto di beni materiali, le quali erano inadatte all'accesso non autorizzato a files, che quando illecitamente copiati non venivano nemmeno sottratti al loro legittimo proprietario.[28] Il processo di approvazione durò ben due anni e finalmente nel 1986 venne ufficializzata la normativa che rese l'accesso a un computer senza autorizzazione e il traffico illecito di password dei reati federali. In seguito a questo provvedimento del governo statunitense, l'asticella dell'attenzione sull'argomento e tutto ciò ad esso correlato aumentò sempre più.

1.2.1. *Free Software*

A partire dalla fine degli anni Settanta, e diventando più comune negli anni Ottanta, le aziende di software, prima tra tutte la giovane Microsoft, cominciarono la commercializzazione dei propri software. Sebbene in un primo momento questa iniziativa non toccò direttamente i centri universitari, visto che questi si affidavano in larga parte a UNIX, un sistema operativo gratuito e dalla sorgente aperta. Il prodotto della AT&T grazie a questa sua caratteristica si diffuse a macchia d'olio e venne reso un sistema operativo completo grazie alle modifiche di innumerevoli utenti, che si scambiavano innovazioni e informazioni.[29] Ben presto questo cambiamento arrivò anche nelle università statunitensi, quando nel 1983 AT&T acquisì la possibilità di esercitare il proprio copyright sul sistema UNIX. I ricercatori vennero piano piano assunti nell'industria software e ciò introdusse le prime limitazioni. Tra obblighi di riservatezza e programmi privi dell'accesso al codice sorgente, il libero scambio di informazioni, fino a quel momento attuato sia da hacker sia dai ricercatori universitari venne meno. Tra questi vi era anche il giovane hacker Richard Stallman, scosso dalla conversione di molti suoi colleghi del MIT. A quel tempo, molti hacker non erano consapevoli delle complessità del diritto d'autore o dei brevetti. Molti hacker, tra cui Stallman, videro tuttavia queste trasformazioni e nuove barriere legali come un insulto personale e un'importante minaccia culturale. Stallman considerava la condivisione del codice sorgente come la pietra miliare che sosteneva le pratiche degli hacker della ricerca curiosa e della collaborazione.[30] Stallman non era necessariamente contrario alla

[28] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit., p. 80
[29] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit., p. 118
[30] Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking*, Princeton University Press, Princeton 2013, p. 68

privacy personale, ma quando si trattava di computer e conoscenza, riteneva che la presenza di password e software protetto da copyright al MIT fosse una corruzione dell'accesso aperto all'informazione su cui si era formato. Stallman considerava le varie barriere progettate per impedire la creazione e la diffusione della conoscenza come fondamentalmente immorali, perché le considerava meccanismi di privatizzazione dell'informazione per consentire ai singoli di trarre profitto a spese della comunità.[31] Perciò per Stallmann la fine della condivisione equivaleva alla fine dell'hacking.

Progettando una risposta più individualmente sostenibile con una portata molto più ampia della vendetta, si è concentrato sulla politica della sopravvivenza culturale. Si dimise dal laboratorio del MIT e iniziò a sviluppare quello che chiamava "software libero", che per un paio di anni non era attaccato a nessuna licenza alternativa. Nel 1985, Stallman fondò la Free Software Foundation (FSF) senza scopo di lucro, e insieme a una manciata di volontari, si concentrò sullo sviluppo di importanti strumenti tecnici e l'assemblaggio dei componenti di un sistema operativo libero. Scelse di modellarlo sulla progettazione di Unix, che all'epoca era il sistema operativo più portatile, il che significa che poteva funzionare su una vasta gamma di hardware.[32]

Nello stesso anno, Stallman formulò e presentò la sua politica di resistenza insieme alla sua visione filosofica nel "The GNU Manifesto", originariamente pubblicato nella rivista *Dr. Dobb's Journal*:

«I consider that the golden rule requires that if I like a program I must share it with other people who like it. Software sellers want to divide the users and conquer them, making each user agree not to share with others. I refuse to break solidarity with other users in this way. I cannot in good conscience sign a nondisclosure agreement or a software license agreement. For years I worked within the Artificial Intelligence Lab to resist such tendencies and other inhospitalities, but eventually they had gone too far: I could not remain in an institution where such things are done for me against my will. So that I can continue to use computers without dishonor, I have decided to put together a sufficient body of free software so that I will be able to get along without any software that is not free. »[33]

Stallman sosteneva che il libero scambio permetteva un più efficiente coordinamento degli sforzi e lo considerava un servizio alla società. La creatività e il servizio al prossimo potevano e dovevano essere un compenso sufficiente. L'etica del software libero proibiva le restrizioni all'esplorazione e alla modifica del codice sorgente in seguito alla vendita del software e non la vendita in sé. A livello

[31] Gabriella Coleman, A. Golub, "Hacker Practice. Moral Genres and the Cultural Articulation of Liberalism", *Anthropological Theory*, vol. 8, n. 3 (2008), p. 261
[32] G. Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking*, cit., p. 68
[33] G. Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking*, cit., p. 69

teorico, questo permetteva ai programmatori di continuare a vivere del proprio lavoro. I programmatori sarebbero stati pagati dalle università e il software libero avrebbe creato nuove occasioni di impiego, sotto forma di didattica, consulenze e assistenza.[34]

Per garantire che il suo software rimanesse libero anche in futuro, Stallman lo rilasciò sotto una licenza da lui creata, la GNU Public License (GPL). In base a questa licenza, Stallman manteneva il diritto d'autore sul suo codice, ma lo distribuiva liberamente, a condizione che tutti i suoi utenti facessero altrettanto. Il risultato è un'inversione della legge tradizionale sul copyright. Con la GPL Stallman usava il copyright non per imporre il monopolio dei suoi diritti di autore, ma per garantire che il software non potesse essere monopolizzato. Il risultato fu la creazione di una "zona sicura" di codice disponibile pubblicamente che non poteva essere privatizzato da interessi aziendali, una sorta di spazio aperto in cui la comunità hacker sognata da Stallman poteva lavorare in libertà. Attraverso la via delle licenze e dei manifesti, Stallman cercò di creare la base tecnologica da cui potesse svilupparsi una fiorente comunità hacker.[35]

Lo scopo complessivo del suo progetto è quello di dare libertà agli utenti dando loro un software libero con meno limitazioni possibili. Tuttavia, Stallman non ha lanciato una politica radicale contro il capitalismo né ha definito la sua visione in termini di giustizia sociale. Allo stesso tempo, molti hacker di prima generazione che usavano il software libero erano spesso inconsapevoli dagli argomenti etici presentati da Stallman e dal suo drammatico manifesto. Durante alcune interviste effettuate da G. Coleman molti hanno parlato della loro reazione negativa o confusa alle "strane" idee di Stallman. In effetti, molti dei primi utenti erano attratti dal software libero semplicemente perché le applicazioni erano economiche e robuste. Ancora meglio, l'accordo di licenza concedeva il permesso di leggere il codice sorgente e modificarlo. La maggior parte degli hacker sono arrivati al software libero in un primo momento solo per il bene di una tecnologia conveniente e meglio costruita e avevano poca conoscenza dell'esistenza e del funzionamento della legge sulla proprietà intellettuale. Il 1984, anno in cui Stallman si dimise dal MIT, si è rivelato una pietra miliare per la globalizzazione delle leggi sulla proprietà intellettuale.[36]

[34] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit., p. 121
[35] G. Coleman, A. Golub, "Hacker Practice. Moral Genres and the Cultural Articulation of Liberalism", cit., p. 261
[36] G. Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking*, cit., pp. 70-71

1.2.2. *Il Morris Worm*

Verso la fine degli anni Ottanta, Internet era primitivo rispetto a come lo conosciamo oggi. In tutto il mondo erano connessi 60.000 computer[37], la maggioranza situata negli Stati Uniti ed utilizzati principalmente da ricercatori. Gli ultimi due anni del decennio furono significativi sia per il mondo intero sia per il mondo hacker. Nel novembre 1988, Internet fu scosso dalla comparsa esplosiva di un worm, un software indipendente capace di riprodursi automaticamente sul sistema infettato. Il responsabile era uno studente della Cornell University, Robert T. Morris, che rilasciò il worm da un computer del MIT, Massachusetts Institute of Technology. In seguito alla sua installazione sulla macchina, esso ricercava eventuali connessioni con il mondo esterno e inviava sé stesso ai contatti del proprio ospite, installandosi nella nuova macchina e ricominciando il processo di ricerca. In breve tempo, il worm aveva attaccato i computer VAX con 4 BSD UNIX e i computer Sun 3 di SUN Microsystems in tutti gli Stati Uniti.[38] Il percorso del worm attraverso Internet fu quasi totalmente indipendente da normali vincoli geografici, dimostrando graficamente la geografia propria del cyberspazio. Il worm non era perfetto e ciò causò in molti casi che fossero presenti molteplici copie di sé stesso all'interno di un singolo computer, causando un rallentamento della velocità di elaborazione complessiva e in alcuni casi l'arresto. A dimostrazione della prontezza di pochi, già il giorno successivo al suo rilascio in rete si stavano diffondendo messaggi con dettagli sul funzionamento del worm. La notizia si diffuse attraverso vari gruppi di notizie e in molti collaborarono per fornire delle patch contro il worm. Al diffondersi della notizia dell'attacco, alcuni amministratori, tra cui la Defense Communications Agency e lo Stanford Research Institute, di sistema iniziarono a tagliare le loro reti fuori da Internet. Due giorni dopo l'inizio dell'"attacco", venne pubblicata su Internet una serie completa di patch per difendere i sistemi dal worm e venne riconosciuto l'autore del worm.[39]

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.[40] Dopo due anni di processo, Morris è stato dichiarato colpevole ai sensi del Computer Fraud and Abuse Act. Le pene massime previste erano cinque anni di carcere, 250.000 dollari di multa e spese di restituzione. A Morris fu ordinato di svolgere 400 ore di servizio alla comunità, fu condannato a tre anni di libertà vigilata e gli fu richiesto di pagare 10.000 dollari di multa.[41] La corte che lo condannò riconobbe che l'obiettivo

[37] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit., p. 83
[38] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 29
[39] *Ibidem*
[40] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit., p. 86
[41] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 30

di Morris non era ostile. La sua creazione aveva un sistema di sicurezza che avrebbe dovuto impedire qualsiasi danno ai sistemi. Si trattò quindi di uno dei primi casi di "white hat hacking", la pratica di penetrare in sistemi informatici per evidenziare falle di sicurezza nei sistemi e permettere agli amministratori di colmarle prima che un hacker malintenzionato se ne avvantaggiasse. Sebbene si affermerà qualche anno più tardi, ad oggi la pratica è diventata fondamentale per l'industria della sicurezza informatica.[42]

Il caso Morris provocò diverse conseguenze nel mondo informatico. Una tra tutte fu la revisione del Computer Fraud and Abuse Act e la sua applicazione fu resa più severa. A pochi giorni dalla diffusione del worm, un gruppo di informatici preoccupati si riunì al National Computer Security Center per studiare l'incidente e pensare a come prevenire il ripetersi di simili attacchi. Nello stesso anno dell'accaduto, la DARPA comissionò la fondazione del Computer Emergency Response Team, CERT, al Software Engineering Institute della Carnegie-Mellon University.[43] Esso si tratta della raccolta e gestione delle segnalazioni di incidenti informatici e di potenziali vulnerabilità nei software provenienti dalla comunità di utenti. I media furono forse quelli più scossi dall'accadimento. Quest'ultimo aveva mostrato la fragilità dei servizi fondamentali che le azioni del gruppo 414s aveva dimostrato alla base della vita quotidiana. Nonostante il pubblico fosse ancora poco familiare con l'argomento, la società statunitense aveva avuto un assaggio di cosa il crimine informatico potesse fare e negli anni a venire cominciò ad alzare il livello di attenzioni nei confronti degli hacker e del loro mondo, non certo da una posizione simpatizzante.

1.3. Gli anni Novanta e l'arrivo di Internet

Gli anni Novanta sono stati testimoni di una notevole ondata di eventi di hacking che hanno segnato per sempre la traiettoria della sicurezza informatica e della regolamentazione di Internet. Mentre il mondo abbracciava l'alba dell'era digitale, la vasta comunità degli hacker continuava ad espandersi. Durante questo decennio, una serie di incidenti di hacking ha catturato l'attenzione del pubblico e ha evidenziato l'urgente necessità di migliorare la sicurezza online. Gli eventi di hacking degli anni Novanta sono stati segnati dall'emergere di una nuova categoria di hacker, talvolta definiti "hacktivisti", che con le loro azioni cercavano di sfidare le istituzioni sociali e politiche prevalenti. Questi individui erano spinti da un mix di curiosità, ribellione e desiderio di esporre le vulnerabilità della nascente infrastruttura digitale. Un altro evento significativo degli anni Novanta è stato il caso

[42] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit., p. 85
[43] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 30

di Kevin Mitnick, un hacker leggendario che è diventato un simbolo del continuo inseguimento tra hacker e forze dell'ordine. Le sue azioni non solo hanno messo in luce le vulnerabilità dell'infrastruttura digitale, ma hanno anche sottolineato l'urgente necessità che la legislazione e le forze dell'ordine si mettano al passo con la rapida evoluzione del mondo dell'hacking. Gli eventi di hacking degli anni Novanta hanno perciò lasciato un segno indelebile nella storia della sicurezza informatica e della regolamentazione di Internet, mettendo in luce le vulnerabilità dell'infrastruttura digitale e in discussione i quadri giuridici esistenti spingendo governi, aziende e privati a investire in misure di cybersecurity più incisive.

Primo evento eclatante del decennio, da cui scaturirono diverse conseguenze (alcune delle quali sono ancora attuali), fu sicuramente l'operazione Sun Devil pensata e attuata dai servizi segreti statunitensi, USSS. Dopo due anni di indagini, il 7, 8 e 9 maggio 1990, 150 agenti dell'FBI, coadiuvati da autorità statali e locali, hanno fatto irruzione in presunte organizzazioni criminali di hacker possibilmente coinvolte nell'abuso di carte di credito e nella truffa dei servizi telefonici. Il risultato dei blitz congiunti in ben 14 città sparse sul territorio nazionale fu il sequestro di quarantadue computer e 23.000 floppy disks. I bersagli delle autorità statunitensi furono principalmente i BBS, alcuni dei quali classificati come "forum per hacker". Nonostante ciò, a due anni dai raid, l'operazione fu molto deludente da un punto di vista di risultati, la maggioranza dei sospettati fu scagionata le incriminazioni furono solo tre. Cominciarono ad accumularsi le prove che gran parte delle prove sequestrate nei raid erano inutili. In seguito a numerose ricerche riguardo l'operazione, si trattò in gran parte di uno sforzo di propaganda. Un'azione senza precedenti di grande ambizione e dimensione, le motivazioni di tale operazione sono solo di stampo politico. Si trattava di uno sforzo di pubbliche relazioni, destinato a far passare messaggi chiari sia nella mente del pubblico in generale sia in quella dei vari gruppi hacker. Il principale messaggio che ne trasparì fu il fatto che le autorità pattugliavano il cyberspazio e che gli hacker non si potevano nascondere dietro al "relativo anonimato dei loro terminali informatici".[44]

La chiusura forzata dei BBS presenti tra i computer sequestrati poneva per la prima volta questioni legislative e morali ancora oggi aperte. Il tema della libertà di espressione digitale era già emerso nel 1989 in seguito ad alcune dichiarazioni delle autorità statunitensi. Esse svelarono che la rivista elettronica *Phrack* fu soggetto di sorveglianza e che i suoi due fondatori, Craig Neidorf e Robert Riggs, furono arrestati. L'accusa principale era di aver acquisito e diffuso illegalmente un documento che descriveva il funzionamento del sistema di chiamata di emergenza, il quale era legalmente disponibile per pochi dollari. Il processo si concluse con l'assoluzione completa dei due imputati.

[44] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., pp. 46-47

Tale rivelazione arrivava in concomitanza con i racconti dei sequestri e delle perquisizioni dell'operazione Sun Devil e metteva in primo piano la questione della libertà della parola elettronica.[45]

Caratteristica evidenziata dai raid delle autorità, e confermata dalle pubblicazioni hacker di quel periodo fu l'incompetenza informatica delle autorità e della stampa generalista. Fatto che contribuì alla percezione di un mondo esterno del tutto incapace di comprendere il nuovo mondo digitale da parte delle comunità hacker e non solo. Nella Silicon Valley degli anni Ottanta e Novanta, in molti si consideravano hacker ed erano preoccupati dalle chiare lacune di legislatori e media nei vari aspetti del fiorente mondo digitale. Spinti dagli eventi dei primi anni Novanta, l'imprenditore milionario Mitch Kapor, John P. Barlow, figura centrale del tecno-libertarianesimo statunitense, e John Gilmore, attivista e dirigente di Sun Microsystems, crearono un'organizzazione per la difesa dei diritti online, la Electronic Frontier Foundation (EFF).

Le reazioni all'iniziativa furono divise, da una parte membri affermati della Silicon Valley furono entusiasti e sostennero il progetto, mentre i media nazionali furono inizialmente ostili, interpretando la fondazione come un semplice fondo di difesa legale per gli hackers. La EFF si impegnò subito a dimostrare che la totalità dell'operazione Sun Devil imponeva dei limiti sulla libertà di parola e fu condotta con modalità arbitraria, oppressiva e non costituzionale. Essa giocò un ruolo chiave nell'assoluzione di quasi tutti i coinvolti nei raid.[46]

Fu esattamente nei primi anni del decennio, due gruppi hacker comparirono spesso nei titoli della stampa nazionale, i LOD (Legion of Doom)[47] e i MOD (Masters of Deception). Il primo venne fondato nel 1984 e inizialmente era formato sia da *phreaks* sia da hackers, tra cui spicca la figura di "The Mentor", Loyd Blankenship. Fu un influente gruppo di hacker clandestini degli anni Ottanta e uno dei primi a capitalizzare sulla pubblicazione regolare delle loro scoperte di vulnerabilità ed exploit nel sistema telefonico e poi nelle reti di computer. Alla fine degli anni Ottanta, la LOD aiutò in qualche occasione le forze dell'ordine, trattenendo gli hacker malintenzionati. Uno dei membri più noti era Chris Goggans, il cui nickname era "Erik Bloodaxe"; fu anche redattore di *Phrack* e in seguito entrò a far parte del Masters of Deception (MOD). Un altro noto hacker che ha iniziato in LOD ed è passato a MOD è stato Mark Abene, vero nome di "Phiber Optik", principale fonte di interesse dei media nazionali per le sue avventure digitali, tra cui un anno di carcere dopo essersi dichiarato colpevole di cospirazione e accesso non autorizzato a computer di interesse federale. Egli acquistò

[45] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit. p. 93
[46] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit. pp. 98-99
[47] La Legion of Doom è un gruppo di supercriminali dell'universo immaginario della DC Comics, creato col fine di contrapporsi alla Justice League, gruppo di supereroi della stessa casa editrice.

notorietà una volta membro del secondo gruppo, i Masters of Deception i quali erano un circolo di hacker di New York attivo tra il 1989 e il 1992. All'epoca, Mark era giovane, ma anche intelligente e spietatamente ossessivo. Alla fine del 1991, Phiber Optik era apparso su *Harper's, Esquire*, *The New York Times*, in innumerevoli dibattiti pubblici e convegni, persino in un programma televisivo.[48]

Simultaneamente, la tecnologia dei pc e soprattutto di internet continuava a evolversi a un passo sempre più veloce. Nei primi tre anni del decennio venne creato il primo sito web grazie a Tim Berners-Lee ponendo la base del web odierno, il World Wide Web nel 1991, e il primo web browser facilitando così l'accesso e la navigazione nel World Wide Web grazie al lavoro di Marc Andreessen e Eric Bina, due programmatori al NCSA, National Center for Supercomputing Applications. A pochi mesi dal lancio di queste due tecnologie innovative, gli utenti informatici salirono drasticamente vista la semplicità di utilizzo adatta anche a principianti. Le novità furono ovviamente accolte molto favorevolmente dalle comunità hacker e non già esistenti, pronti ad esplorarle e a scoprire le loro possibilità.

L'arrivo di una nuova tecnologia spesso sancisce la "morte" di un'altra. Con l'avvento del web, i BBS subirono un progressivo calo di popolarità e molti di loro vennero chiusi per sempre. In questo contesto, per festeggiare la chiusura di uno di questi BBS vennero invitati svariati gruppi hacker a Las Vegas. Nacque così la prima edizione di DefCon, una delle numerose conferenze di hacker emerse nei primi anni Novanta, seguendo il modello stabilito dalla HoHoCon, ospitata dal gruppo di hacker underground Cult of the Dead Cow del 1990. La DefCon fu fondata da Jeff Moss, chiamato nelle comunità hacker "Dark Tangent". In seguito, le successive edizioni della conferenza furono concepite come luogo di ritrovo e condivisione di informazioni per hacker, e da allora è cresciuta fino a diventare una delle conferenze di hacker più grandi e conosciute al mondo.[49]

Le tecnologie informatiche, in particolar modo quella del web, videro un incremento della loro crescita negli anni successivi. Nel 1995 Microsoft rilasciò la prima versione di Internet Explorer, che ben presto diventò uno dei browser web più popolari, e l'anno successivo la Sun Microsystems rilasciò la prima versione del linguaggio di programmazione Java, futuro linguaggio popolare per lo sviluppo web. Tutto questo processo di crescita del mondo digitale, richiedeva un aggiornamento parallelo delle legislazioni statunitensi. Esattamente per questo motivo, il Computer Fraud and Abuse Act (1984) venne man mano modificato diverse volte, (1989, 1994 e 1996) e nel 1996 il Congresso venne approvato il Communications Decency Act, CDA, che diede il via a un dibattito sulla libertà

[48] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., pp. 43-46
[49] G. Coleman, "The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld", *Anthropological Quarterly*, Anthropological Perspectives on Knowledge in the Digital Age (Winter, 2010), Vol. 83, No. 1, pp. 47-72, p. 52

di parola e sulla censura in Internet. Quest'ultimo fu pensato principalmente in risposta alle preoccupazioni sull'accesso minorile alla pornografia attraverso Internet. Il CDA creò una causa penale a questo riguardo in particolare ai mittenti consapevi di messaggi "osceni" o "indecenti" a destinatari di età inferiore ai 18 anni. All'approvazione, questa legislazione presentava numerosi problemi che riguardavano sia i fornitori di servizi Internet (ISP) che le aziende. In primo luogo, non c'era modo per i mittenti o i visualizzatori di sapere se rientravano nell'eccezione. All'epoca, era difficile e complicato per un mittente escludere i minori. Inoltre, i termini utilizzati nella legge erano ambigui e il CDA nel suo complesso imponeva un onere eccessivo alla libertà di parola.[50]

Alcune parti del CDA, in particolare quelle riguardanti la fraseologia, sono state rapidamente contestate in tribunale da gruppi per i diritti civili e da sostenitori della libertà di parola. In seguito, le disposizioni relative al materiale indecente e palesemente offensivo sono state ritenute in contrasto con la libertà di parola tutelata dal Primo Emendamento e sono state eliminate dal CDA. Forse parte più conosciuta della legislazione, la sezione 230 creò un'immunità federale a qualsiasi causa di azione che renda gli ISP responsabili per le informazioni provenienti da un utente terzo del servizio. Sebbene protegga i forum online e gli ISP dalla maggior parte delle cause federali, non esenta i fornitori dalle leggi statali applicabili o dalle rivendicazioni penali, di privacy delle comunicazioni o di proprietà intellettuale.[51]

1.3.1. *Il movimento Open Source*

Nel giro di soli due anni, tra il 1993 e il 1995, gli Stati Uniti vissero un momento di crescita esponenziale dell'industria informatica e del web, nel quale la popolazione otteneva la possibilità di accedere e navigare facilmente su Internet, assieme ai primi browser e al HTML, linguaggio base per la creazione di pagine proprie. Fu esattamente in questo periodo che le prime versioni funzionanti di Linux cominciarono a circolare nel web.[52]

Mentre l'impatto di Stallman e del suo progetto sull'industria software e sull'hacking è stato il risultato di un piano accuratamente premeditato, la creazione del sistema operativo Linux da parte di Linus Torvalds è stata molto più casuale. Nel 1991, Torvalds rilasciò il codice sorgente del suo progetto per hobby su una mailing list. Nessuno poteva prevedere che questa mossa avrebbe dato vita alla prima collaborazione di successo su larga scala e a distanza nel campo del software e il suo progetto, un

[50] William A. Sodeman, "Communications Decency Act", Encyclopedia Britannica, 10 Aug. 2023, https://www.britannica.com/topic/Communications-Decency-Act (ultima consultazione: 14 Agosto 2023);
[51] *Ibidem*
[52] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit. p. 135

kernel UNIX libero, fu combinato con il software GNU di Stallman per creare quello che oggi è noto come GNU/Linux. Verso la metà e la fine degli anni Novanta, i progressi della tecnologia informatica facilitarono l'emergere del software libero come "movimento" tecnologico a tutti gli effetti. Ora volontari di tutto il mondo collaborano a migliaia di progetti software.[53]

La «cultura partecipativa» di Linux ottenne una popolarità internazionale e una diffusione estremamente rapida, obbiettivi mai raggiunti da quella Free Software. Il modello di lavoro delle comunità hacker arrivò a superare per certi aspetti quella dalle affermate aziende software. La differenza tra i due modelli organizzativi e sociali è riassunta da Eric Raymond, hacker e maggiore ideologo del futuro movimento Open Source, nel suo saggio (1997) e in seguito libro (1999) "La cattedrale e il bazaar". La cattedrale rappresentavano le società produttrici di software, caratterizzate dalla centralizzazione del potere e una definita divisione del lavoro. Al suo opposto, vi era il bazaar, moltitudine di hobbisti del settore, ognuno dei quali forniva il proprio apporto personale, che sia una iniziativa di aggiunta o una risoluzione di eventuali bug.[54] Riferendosi alle origini del fenomenale movimento open source, Raymond osservò come "la cultura hacker, sfidando le ripetute previsioni sulla sua scomparsa, stava appena iniziando a rifare il mondo del software commerciale a sua immagine e somiglianza".[55] Questo perché durante le prime fasi dello sviluppo del programma, la comunità attorno ad esso era principalmente formata da hackers e da programmatori. Comunità lasciata totalmente libera dall'autore originale Torvalds, come fatto notare da Raymond, cosa che ne ha reso possibile la elevazione dalla comunità GNU precedente e dal mercato dettato dalle grandi imprese del settore. Col passare del tempo, Torvalds divenne il coordinatore del progetto senza però giudicare le modifiche apportate dagli utenti.[56]

L'intento politico e la soggettività sono assenti nella costituzione del movimento del software libero e dell'open source, che si differenzia dagli sforzi politici più formali e dai nuovi movimenti sociali che si basano su un'intenzionalità, una direzione o una riflessività politica o sul desiderio di trasformare condizioni sociali più ampie. Mentre le razionalità tecniche o economiche sono spesso la spiegazione nativa del FOSS, una forma scontata di liberalismo culturale e la pragmatica della programmazione informano e rafforzano reciprocamente l'avversione estetica hacker per la politica.[57]

[53] G. Coleman, A. Golub, "Hacker Practice. Moral Genres and the Cultural Articulation of Liberalism", cit., p. 262
[54] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit. p. 136
[55] H. Nissenbaum, "Hackers and the contested ontology of cyberspace", cit., p. 211
[56] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit. p. 138
[57] Gabriella Coleman, "The Political Agnosticism of Free and Open Source Software and the Inadvertent Politics of Contrast", *Anthropological Quarterly*, vol. 77, n. 3 (2004), p. 508

Abbracciato anche dagli hacker, esserne parte portava alcuni a considerare sé stessi come artisti e il coding come una tipologia di "artigianato diligente". La gran parte di loro però si considerano attivisti e sostennero che l'attenzione alla libertà di informazione sia un aspetto fondamentale della libertà democratica nel mondo di oggi.[58] L'esperienza vissuta dell'hacking FOSS è più populista e comunitaria, e al centro della pratica FOSS c'è la consapevolezza di essere connessi a una comunità di sviluppatori che rendono disponibile tutto il codice facilitando tutto il lavoro, anche grazie agli altri sviluppatori pronti ad aiutare quando sorgono difficoltà.[59]

All'inizio di questo secolo, l'open source è diventato anche l'oggetto dell'energia imprenditoriale, dei finanziamenti e del clamore della Silicon Valley, anche se oggi la febbre per l'open source è diminuita in modo significativo, reindirizzandosi verso altre piattaforme di social media.[60] Difatti nel 1998 Raymond, assieme ad altri protagonisti del nascente ecosistema, fondarono la Open Source Initiative, OSI. Il modello Open Source e i suoi prodotti per la loro sopravvivenza dovevano essere adottati dai pezzi grossi dell'industria informatica. Per fare in modo che ciò accada bisognava prima distaccarsi dal Free Software e avere un'ottima campagna marketing. la strategia attuata dalla OSI funzionò egregiamente e qualche mese dopo le prime società informatiche, tra cui IBM e Dell, diventarono compatibili con Linux.[61]

Nonostante Linux fosse molto popolare tra gli hackers, l'underground digitale era ben lontano dal sentirsi riabilitato e da aver trovato una collocazione nella società. Visto che nei vari siti, e riviste hacker del periodo la questione Stallman-Raymond era principalmente sorvolata, suggerisce la permanenza di una divisione tra hacker accademici, molto interessati alla vicenda nella sua totalità, e quelli non accademici. A dispetto di ciò durante l'ultimo decennio del secolo scorso, la cultura hacker era unica e sola. I suoi elementi caratteristici, luoghi di incontro, strumenti, classe sociale, la comunicazione esterna sono gli stessi per entrambe le categorie.[62]

Meno fortemente utopico del software libero, l'OSS fa comunque parte di un genere morale la cui preoccupazione principale è l'accesso alle informazioni. I sostenitori dell'OSS hanno affermato che l'open source è un "modello di sviluppo" superiore per la creazione di software, in contrasto con gli approcci tradizionali che utilizzano diritti d'autore e brevetti. Le argomentazioni e i discorsi a riguardo si sono dimostrati efficaci, visto che attualmente le aziende spendono milioni di dollari per sviluppare

[58] Brian Alleyne, *Geek and Hacker Stories. Code, Culture and Storytelling from the Technosphere*, Palgrave Pivot, London 2019, p. 9
[59] G. Coleman, A. Golub, "Hacker Practice. Moral Genres and the Cultural Articulation of Liberalism", cit., p. 263
[60] G. Coleman, *Coding Freedom.The Ethics and Aesthetics of Hacking*, cit., p. 20
[61] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit. p. 143
[62] F. Mazzini, *Hackers. Storia e pratiche di una cultura*, cit. pp. 144-147

e pubblicizzare l'OSS.[63] In seguito, l'Open Source si è reinventato come versione business-friendly delle tecniche di programmazione del software libero e delle idee sulla proprietà, portando all'integrazione dei principi hacker incorporati nel software libero in forme di profitto capitalistico. Con l'ascesa di aziende alimentate dal software libero, in particolare da Linux, l'hacking ha iniziato a essere visto da alcuni non come la provincia di cracker, criminali o attivisti politici, ma come un principio fondamentale di una nuova economia.[64]

1.3.2. *Il caso Mitnick*

Secondo alcuni studiosi, tra cui Goodell, Littman e Shimomura, la formazione degli hacker di una comunità auto-riconosciuta come tale fu in parte derivata dalla propria falsa rappresentazione perpetuata dai media tradizionali durante tutto il corso degli anni Novanta.[65] Anni caratterizzati da molti episodi e controversie che contribuirono a creare il contesto adatto per questo sviluppo, gli eventi principi più caratterizzanti del decennio furono quelli incentrati su Kevin Mitnick. Si parla di una copertura mediatica molto intensiva, Mitnick finì sulla prima pagina del New York Times come il primo hacker da "miliardi di dollari" e successivamente vennero scritti vari libri e girato un film sul suo conto.[66] Mitnick assunse le vesti di cybercriminale, almeno a livello mediatico, come nessuno prima o dopo di lui. "The Condor", nome hacker di Mitnick, calcò la scena di giornali e televisione nazionale per vent'anni e fu considerato l'esempio principe dell'hacker criminale in grado di manipolare la tecnologia digitale a proprio piacimento.[67]

Sebbene i media nazionali gli conferirono capacità quasi soprannaturali, Mitnick faceva cose a dir poco normali e basilari. Egli sfruttava la sua eccellente capacità nell'ingegneria sociale, la capacità di manipolare a proprio vantaggio la società come se fosse un computer o un telefono. Questa tecnica risale agli anni Settanta, dove nelle pubblicazioni *phreak* si trovavano consigli e informazioni su tutto ciò che c'era da sapere per metterla in pratica. Una delle tecniche di ricerca più diffuse tra gli hackers che utilizzavano l'ingegneria sociale vi era il "dumpster diving". Questo metodo consisteva nella ricerca di documenti scartati, solitamente nella spazzatura, che contenessero informazioni riservate o almeno abbastanza private da dare credibilità alla messa in scena del social engineering.[68]

[63] G. Coleman, A. Golub, "Hacker Practice. Moral Genres and the Cultural Articulation of Liberalism", cit., p. 262
[64] T. Jordan, "A Genealogy of Hacking", cit., p. 537
[65] T. Jordan, "A Genealogy of Hacking", cit., p. 535
[66] T. Jordan, "A Genealogy of Hacking", cit., p. 535
[67] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 99
[68] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 100

Nel 1981, riuscì ad ottenere l'accesso a un centro operativo della Pacific Bell e in seguito al suo arresto il tribunale minorile ordinò uno studio psicologico diagnostico su Mitnick e lo condannò a un anno di libertà vigilata. Nel 1987, fu arrestato per aver fatto irruzione nei computer della Santa Cruz Operation, creatori di SCO Unix, e fu condannato a tre anni di libertà vigilata. Nell'estate del 1988, Mitnick si introdusse nei computer della University of Southern California e si appropriò di centinaia di Mb di spazio su disco per archiviare il codice sorgente VAX VMS rubati dalla Digital Equipment Corporation (DEC). Per questo furto, Mitnick fu arrestato dal FBI, Federal Bureau of Investigation. Nel luglio 1989 fu condannato a un anno di carcere per frode informatica non correlata e sei mesi di riabilitazione.[69]

Riguardo alle motivazioni che lo spinsero, Mitnick ha negato l'ipotesi di essere mai stato motivato da fattori ostili come forti aspirazioni di potere, ma ha riconosciuto che la ragione per cui alcuni hacker operano è il guadagno. Mitnick ha affermato di hackerare perché:

You get a better understanding of the cyberspace, the computer systems, the operating systems, how the computer systems interact with one another, that basically, was my motivation behind my hacking activity in the past, it was just from the gain of knowledge and the thrill of adventure, nothing that was well and truly sinister such as trying to get any type of monetary gain or anything.[70]

Fin dai primi processi, Mitnick sostenne di aver solo seguito fedelmente l'etica hacker, gli atti illegali di cui fu imputato erano per mettersi alla prova e soddisfare la propria curiosità. Dichiarazioni molto spesso ignorate dai media, che dal 1988 affibbiarono a Mitnick il titolo di "dark-side hacker", chiaro riferimento alla saga di Star Wars. A causa di questa aura di minaccia imposta su di lui dai media nazionali i suoi successivi processi giudiziari vennero inaspriti. Ad esempio, nel processo dello stesso anno gli fu negata la possibilità di cauzione e fu costretto a passare in isolamento gran parte della sua condanna.[71]

Grazie alle sue imprese e alle sue varie incarcerazioni, Mitnick durante gli anni Novanta diventò una celebrità del mondo hacker, come Morris e altri prima di lui. Nel novembre del 1992, Mitnick entrò in clandestinità quando l'FBI ottenne un nuovo mandato per il suo arresto. Questo non lo fermò dal continuare a fare ciò che più lo rendeva vivo, l'hacking. Durante la sua latitanza entrò in diversi sistemi e in diverse aziende, tra cui la Sun Microsystems nel 1993.[72] Nel 1995 Mitnick era al suo

[69] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 10
[70] Paul Taylor, *Hackers: Crime in the Digital Sublime*, Routledge, London 1999, p. 58
[71] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 103
[72] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 105

limite, le forze dell'ordine lo avevano costretto a cambiare tre identità e tre città in due anni, mentre l'attenzione mediatica era sempre più pressante.

Venne localizzato lo stesso anno, quando lasciò messaggi offensivi sul computer e sui sistemi di posta vocale di un fisico ed esperto di sicurezza Internet, Tsutomu Shimomura. Quest'ultimo aiutò le forze dell'ordine a rintracciare il fuggitivo in North Carolina, dove Mitnick fu arrestato nel febbraio 1995 e imprigionato in attesa del processo. Mitnick è stato condannato dal tribunale federale della California il 9 agosto 1999 e condannato a 46 mesi di reclusione per "quattro capi di frode telefonica, due capi di frode informatica e un conteggio di intercettare illegalmente una comunicazione via cavo."[73] Nonostante tutte le accuse mosse contro di lui, i media e le autorità giudiziarie avevano ben poco con cui lavorare. Nonostante tutte le sue imprese e appropriazioni, l'unico vantaggio materiale avuto furono chiamate gratuite (di poco superiore al migliaio di dollari). Le autorità giudiziarie sebbene privi di mezzi adeguati a punire i potenziali crimini, non potevano di certo limitarsi ai pochi anni di prigione per i reati effettivamente commessi vista la lunga latitanza di Mitnick. Per ottenere una punizione che fosse d'esempio, la strategia adottata fu extraprocessuale. All'hacker fu negata l'udienza per fissare la cauzione, obbligato ad attendere l'inizio del processo in carcere. La sua data fu fissata solo quattro anni dopo, nel 1999, successivamente al patteggiamento di Mitnick.[74] Dopo il suo rilascio dalla prigione nel settembre 2000, Mitnick doveva essere in libertà vigilata per tre anni durante i quali il suo accesso ai computer era limitato e i suoi profitti derivanti dallo scrivere o parlare della sua carriera criminale dovevano essere devoluti per rimborsare le sue vittime.[75]

Questo trattamento giudiziario altamente inusuale e decisamente duro che spinse le comunità hacker a riconoscersi come gruppo di interesse cercando di spiegare al mondo esterno loro stesse e i propri valori. Durante questo lungo processo durato quasi cinque anni, alcune piccole comunità hacker guidate dalla rivista *2600. The Hacker Quarterly* diedero inizio a una campagna di protesta denominata "FREE KEVIN". Spinti dal trattamento riservato al loro collega e celebrità, fu una componente popolare del vandalismo Web fino alla sua scarcerazione.[76] I bersagli principali furono ovviamente i media e le loro piattaforme, tra cui Yahoo News nel 1997, responsabili di aver plasmato l'essenza della pratica ad atto criminale. Nonostante gli sforzi, la campagna ebbe un risultato più evidente sulla stessa comunità hacker che sul processo in sé. La campagna "Free Kevin" mostrò agli

[73] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 10
[74] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., pp. 108-110
[75] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 10
[76] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 11

hackers che uniti come comunità collettiva, erano in grado di farsi carico di cause politiche e sociali attraverso la nuova comunicazione digitale.[77]

1.4. Verso il nuovo millennio

La fine del decennio, in particolar modo il 1998 e il 1999, fu segnata da un incremento di malware distribuiti nel web e l'ulteriore crescita di quest'ultimo. Difatti, nel 1998 venne lanciata la prima versione di Google creata da Larry Page, Sergey Brin, and Scott Hassan, che rivoluzionò il modo di cercare informazioni sul web. Il primo agosto dello stesso anno al DefCon 6 venne presentato Black Orifice, BO, con lo scopo di dimostrare la mancanza di sicurezza nella serie di sistemi operativi Windows 9x di Microsoft. Il programma venne creato da "Sir Dystic", membro del gruppo hacker Cult of the Dead Cow. Un influente gruppo di criminali-hacker, noto per il suo uso costante dell'umorismo e della parodia. Negli anni Novanta, i CDC diventarono importanti sostenitori dell'hacktivismo, ovvero l'uso di tecniche di hacking criminale per scopi politici.[78]

Sulla scia del rilascio di Windows 98 da parte di Microsoft, il 1999 diventò un anno di punta per la sicurezza e la pratica dell'hacking. Vennero rilasciati centinaia di avvisi e patch in risposta ai nuovi bug, ampiamente pubblicizzati, di Windows e di altri prodotti software commerciali. Una serie di fornitori di software di sicurezza cominciò il rilascio di prodotti anti-hacking da utilizzare sui computer di casa. Ironicamente quello stesso anno, migliaia di computer in tutto il mondo vennero infettati in pochissimo tempo. Si trattava di uno dei primi virus di posta elettronica ad attirare l'attenzione mondiale, il virus Melissa.

Nella giornata di venerdì 26 marzo del 1999 il CERT/CC ha ricevuto le prime segnalazioni di questo nuovo macro virus[79], un virus informatico scritto nello stesso linguaggio macro utilizzato per creare programmi software Microsoft, MS-Word a rapida diffusione. Esso è stato programmato per infettare quella stessa tipologia di documenti. Una volta caricato, utilizza la rubrica di posta elettronica della vittima per inviare copie di sé stesso alle prime cinquanta persone dell'elenco. Il virus allega un file MS-Word infetto a un messaggio di posta elettronica. Il documento infetto originale era una raccolta di URL di siti Web pornografici. Tuttavia, man mano che il virus si diffondeva, era in grado di inviare qualsiasi altro documento infetto creato dalla vittima. Grazie a questa elevata velocità di replicazione, il virus si è diffuso più rapidamente di qualsiasi altro virus della storia. In molti sistemi aziendali, il rapido tasso di replicazione interna ha saturato i server di posta elettronica con e-mail spazzatura

[77] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 112
[78] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., pp. 42-43
[79] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., pp. 31

automatizzate in uscita. Le stime iniziali si aggiravano intorno ai 100.000 sistemi danneggiati. Le aziende produttrici di antivirus si sono immediatamente mobilitate e gli aggiornamenti per tutti i prodotti standard sono stati disponibili entro poche ore dalle prime notifiche del CERT/CC.

La ricerca dell'autore del virus Melissa è iniziata subito dopo l'epidemia. Successivamente a molte ricerche da parte delle autorità statunitensi, l'autore del macro virus fu identificato in David L. Smith e arrestato il due aprile dall'FBI. Smith è stato accusato dei reati di secondo grado di interruzione di comunicazioni pubbliche, associazione a delinquere e tentativo di commettere il reato, furto di servizi informatici di terzo grado e danneggiamento o accesso abusivo a sistemi informatici di terzo grado. In caso di condanna, Smith rischiava una pena massima di 480.000 dollari di multa e 40 anni di carcere. Nel 10 dicembre 1999, Smith si è dichiarato colpevole di tutte le accuse federali e ha accettato ogni particolare dell'accusa, comprese le stime dell'International Computer Security Association di almeno ottanta milioni di dollari di danni conseguenti alle infezioni di Melissa.[80]

[80] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 34

Capitolo 2 La figura dell'hacker tra film e realtà

Il periodo vissuto dal cinema hollywoodiano tra gli anni Ottanta e Novanta è stato un momento di grandi cambiamenti e innovazioni nell'industria cinematografica. Quest'era ha visto l'emergere di nuove tecnologie, nuovi generi e nuove voci che avrebbero plasmato il futuro del cinema per gli anni a venire. Uno dei cambiamenti più significativi avvenuti in questa fase è stata l'ascesa della tecnologia digitale. Negli anni Ottanta, i registi iniziarono a sperimentare gli effetti digitali e le immagini generate al computer (CGI[81]) in film come *Tron*. All'inizio degli anni Novanta, la CGI era diventata uno strumento standard nella cinematografia hollywoodiana, permettendo ai registi di creare elaborati effetti speciali e spettacoli visivi prima impossibili. Gli anni Novanta hanno visto un cambiamento nel tipo di storie che Hollywood stava raccontando. Mentre gli anni Ottanta erano stati dominati da film d'azione e commedie a grande budget, gli anni Novanta videro l'ascesa di film più drammatici e introspettivi. I film esploravano ora temi e personaggi complessi e spesso avevano finali più sfumati e ambigui rispetto alle semplici narrazioni bene-male degli anni Ottanta. Nel complesso, il periodo di transizione tra gli anni Ottanta e Novanta è stato un momento di grande cambiamento e sperimentazione per il cinema hollywoodiano. È stato un periodo in cui sono emerse nuove tecnologie, nuove voci e nuovi temi, aprendo la strada all'industria cinematografica diversificata ed entusiasmante che conosciamo oggi.[82]

Dai primi film a riguardo degli anni Ottanta in poi, Hollywood ha spesso rappresentato gli hacker come individui in grado di utilizzare le loro avanzate competenze tecnologiche per manipolare e superare in astuzia anche le istituzioni più potenti. Tuttavia, la rappresentazione degli hacker nel cinema americano non è sempre stata positiva. Prima degli anni Duemila, la rappresentazione degli hacker nel cinema americano era ampiamente stereotipata e spesso imprecisa. Gli hacker erano tipicamente rappresentati come geni del computer che usavano le loro abilità per orchestrare rapine elaborate, penetrare in sistemi sicuri o causare il caos per il gusto di farlo. Queste rappresentazioni erano spesso sensazionalizzate e prive di sfumature, con gli hacker ritratti come eroi o cattivi a seconda delle esigenze della trama.

La pratica dell'hacking veniva spesso rappresentata come un semplice processo di digitazione di comandi in un computer, con poca enfasi sulle abilità e le conoscenze tecniche richieste per tali attività. Nonostante questi limiti, la rappresentazione degli hacker nel cinema americano prima degli anni Duemila ha svolto un ruolo importante nel plasmare la percezione pubblica della tecnologia

[81] Il processo di utilizzo del computer per la creazione di immagini o personaggi in ambito cinematografico e televisivo (Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/computer-generated-imagery)
[82] Gianni Rondolino, Dario Tomasi, *Manuale di Storia del Cinema*, UTET Università, Milano 2014

informatica e dei suoi potenziali usi. Pur essendo spesso imperfette, queste rappresentazioni hanno contribuito ad accendere l'interesse del pubblico per i computer e la tecnologia, aprendo la strada a rappresentazioni più sfumate e accurate negli anni successivi.

In questo capitolo analizzeremo la rappresentazione degli hacker in vari film rilasciati durante il periodo preso in considerazione ed esamineremo il loro impatto sulla cultura popolare e sulla percezione degli hacker. Esploreremo come questi film abbiano contribuito a plasmare l'immagine dell'hacker nell'immaginario popolare e come abbiano contribuito allo sviluppo della cultura hacker. Esamineremo anche il contesto culturale e storico in cui questi film sono stati realizzati e considereremo come riflettono le preoccupazioni e le ansie del loro tempo. Facendo questo, possiamo comprendere il significato culturale dell'hacking e la sua rappresentazione nel cinema americano.

2.1. La rappresentazione e il ruolo nel cinema

La prima ondata di film sugli hacker negli anni Ottanta e nei primi anni Novanta ha segnato un periodo significativo nella rappresentazione degli hacker nel cinema americano. Questi film ritraevano gli hacker come ribelli che usavano le loro abilità per sfidare l'autorità e sovvertire lo status quo. Essi catturarono l'immaginazione del pubblico e contribuirono a rendere popolare l'idea dell'hacker come eroe contro-culturale. Quest'idea di soggetti ribelli che sfidavano l'autorità e usavano le loro abilità a fin di bene ha radici profonde che risalgono al primo dopoguerra. Difatti dal 1946 ai giorni nostri, lo *Zeitgeist* culturale statunitense è stato caratterizzato dalla sfiducia nell'autorità e dal desiderio di libertà individuale. Con il periodo della presidenza Reagan (1981-1989) e la sua politica interna conservatrice, ci fu un lieve aumento di questa tendenza causata dall'incremento del pensiero liberale all'interno degli Usa[83].

2.1.1. *La rappresentazione degli hacker negli anni Ottanta*

La comparsa degli hacker nel cinema risale ai primi anni Ottanta, quando i personal computer stavano diventando più comuni e accessibili al grande pubblico. La rappresentazione degli hacker nei primi film era spesso semplicistica e stereotipata: i personaggi erano tipicamente rappresentati come giovani uomini socialmente impacciati e affascinati dalla tecnologia. La rappresentazione degli hacker nel cinema hollywoodiano ha subito un'evoluzione significativa nel corso degli anni. Questo

[83] G. Sangiuliano, *Reagan. Il Presidente che cambiò la politica americana*, Mondadori, Milano 2021

grazie al progresso della tecnologia e al cambiamento dell'atteggiamento della società nei confronti della tecnologia e di Internet. Negli anni Ottanta e nei primi anni Novanta, le opere hollywoodiane ritraevano gli hacker come giovani, bianchi, maschi emarginati, ossessionati dalla tecnologia e che usavano le loro capacità per scopi puramente ludici. Come opere di finzione e intrattenimento, questi film presentavano ritratti della figura dell'hacker spesso monodimensionale e non riflettevano con accuratezza la vera essenza dei membri delle comunità hacker. La selezione dei titoli cinematografici presa in considerazione è stata composta in base all'importanza e alla rilevanza dell'argomento e anche all'incasso delle sale (imdb.com).

Difatti, nel 1982 venne rilasciato nelle sale uno tra i primi film a comprendere la figura dell'hacker, *Tron*. Sebbene il termine "hacker" non viene mai citato all'interno della pellicola, il protagonista può facilmente essere considerato tale, sia per caratteristiche come personaggio sia come azioni compiute. Questo film di fantascienza, diretto da Steven Lisberger, è ambientato in un mondo di realtà virtuale per quasi la sua totalità. La trama ruota attorno a Kevin Flynn, un talentuoso programmatore di computer, in cerca di giustizia dopo essere stato licenziato dal suo collega Ed Dillinger, il quale gli ha rubato i progetti dei videogiochi. Attraverso l'hacking del sistema mainframe della ENCOM, azienda in cui lavorava, Flynn entra nel mondo virtuale noto come "Grid", controllato dall'oppressivo Master Control Program (MCP). In squadra con Tron e Yori, programmi indipendenti che si oppongono all'MCP, Flynn si cimenta in giochi gladiatori, combatte contro programmi ostili e naviga in insidiosi paesaggi digitali. Alla fine, si fonde con l'MCP, distruggendolo dall'interno, e ripristina la giustizia nel regno virtuale. Sebbene Tron venga ricordato da esperti e pubblico principalmente per i suoi effetti visivi e per il suo ruolo nello sviluppo della CGI[84], computer-generated imagery, esso introduce anche la figura dell'hacker e la pratica dell'hacking come elementi importanti ai fini della trama. La pellicola di Lisberger si concentrò relativamente poco su di esse e probabilmente fu anche una delle ragioni per cui non ispirò la sottocultura statunitense allo stesso modo in cui fece la prossima opera cinematografica di cui parlerò.

Uno dei primi film con un hacker come protagonista principale è stato *Wargames*, uscito nel 1983. Il film segue la storia di un giovane hacker che ottiene inavvertitamente l'accesso a un supercomputer militare e quasi scatena una guerra nucleare. Esso segue la tradizionale struttura a tre atti, con il primo atto che introduce i personaggi e prepara la trama, il secondo atto dove vengono costruite la tensione e il conflitto, e infine, il terzo atto che risolve il conflitto e conclude la storia. L'intreccio ruota attorno a uno studente delle superiori di nome David Lightman, interpretato da Matthew Broderick, che si

[84]Roger Ebert, Tron, *RogertEbert.com*, https://www.rogerebert.com/reviews/tron-1982 (ultima consultazione: 30 agosto 2023); Derek Armstrong, Tron (1982) review, *ALLMOVIE*, www.allmovie.com/movie/tron-vm424775/review (ultima consultazione: 30 agosto 2023)

introduce involontariamente in un supercomputer militare mentre è alla ricerca di videogiochi. David avvia un gioco chiamato “Guerra termonucleare globale”, pensando che sia solo una simulazione. Tuttavia, egli innesca inconsapevolmente l'intelligenza artificiale del computer, Joshua, facendogli credere che il gioco sia reale e che gli Stati Uniti siano sotto attacco. Analizzando i dati del gioco, Joshua inizia i preparativi per una guerra nucleare. Quando si rende conto di ciò che ha scatenato, David cerca di fermare l'imminente disastro con l’aiuto della sua compagna di classe e interesse amoroso, Jennifer Mack, interpretata da Ally Sheedy. I due si recano dal creatore del computer, il dottor Stephen Falken, interpretato da John Wood, per chiedere assistenza nel contrastare la sua creazione. Insieme, devono trovare un modo per convincere Joshua che il gioco è solo una simulazione prima che la situazione precipiti. Alla fine, David riesce a convincere Joshua che in una guerra nucleare non esistono vincitori; gesto che porta il computer a rendersi conto dell'inutilità delle sue azioni e interrompere la sequenza di lancio, evitando così un conflitto catastrofico. *Wargames* fu sia un successo commerciale[85] sia di critica[86] e il suo impatto sulla cultura popolare fu significativo. Il film non solo introdusse il concetto di hacking a un pubblico più vasto, ma contribuì anche a plasmare la percezione pubblica degli hacker come giovani individui intelligenti.

Nel caso di *Wargames*, il riferimento principale alla cultura hacker e tutto ciò che ne riguarda è il protagonista del film, David Lightman. Egli è presentato come un giovane brillante ma un po' malizioso, affascinato dai computer e dalla tecnologia. Per molti versi, Lightman rappresenta la crescente comunità di appassionati di computer emersa negli anni Ottanta. Questi giovani erano spesso autodidatti e appassionati nell'esplorare le possibilità dell'informatica, anche se ciò significava piegare o infrangere le regole lungo il percorso[87].

La sua introduzione come personaggio è già caratterizzante, lo spettatore lo ritrova davanti un cabinato arcade all’interno di un diner, indicando da subito come David passa il proprio tempo libero. A scuola viene spesso richiamato dai suoi professori per il suo comportamento ribelle. Una volta a casa, vengono presentate allo spettatore maggiori informazioni riguardo David, la sua camera infatti è piena di apparecchi e strumenti informatici e non, delineando un suo chiaro interesse per i computer e tutto ciò che li riguarda. Nonostante possegga una discreta conoscenza sull’argomento, non è ancora un esperto in questo campo. Difatti quando si imbatte per caso nel sistema di un supercomputer del NORAD, chiede consiglio a dei suoi amici tecnici programmatori. Quest’ultimi leggendo il tabulato

[85] Ha avuto un incasso complessivo di 79.567.667 $ (fonte: imdb.com)
[86] Keith Phipps, “WarGames (1983)”, *ALLMOVIE*, https://www.allmovie.com/movie/wargames-vm1072653/review (ultima consultazione: 30 agosto 2023); Roger Ebert, “WarGames”, *RogerEbert.com*, https://www.rogerebert.com/reviews/wargames-1983 (ultima consultazione: 30 agosto 2023)
[87] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., pp. 72-73

dei giochi, individuano subito l'appartenenza militare del sistema e consigliano a David di cercare un eventuale backdoor inserita dal creatore del suddetto sistema. Lo spettatore ha quindi una chiara visione del suo personaggio, David è un giovane intraprendente che sa il fatto suo sui computer, ma ha ancora molto da imparare. Inoltre grazie anche ai successivi incontri sia con il dottor Falken sia con i militari della base NORAD, il giovane protagonista è mostrato come figura ribelle all'autorità degli adulti, dall'episodio scolastico alla fuga dalla base.

La curiosità e l'intraprendenza di Lightman sono in bella mostra durante tutto il corso del film, mentre usa le sue abilità per "hackerare" vari sistemi ed esplorare territori digitali proibiti. Sebbene le sue azioni abbiano potenzialmente gravi conseguenze, sono anche guidate da un genuino desiderio di imparare e comprendere meglio il funzionamento dei computer. Per molti spettatori, il personaggio di Lightman è stato al tempo stesso fonte di ispirazione e soggetto di cui immedesimarsi: ha rappresentato un nuovo tipo di eroe per una generazione sempre più affascinata dalla tecnologia e dal suo potenziale.

Il film è il punto di svolta che rese la figura dell'hacker, o dell'esperto informatico, appetibile per i registi hollywoodiani. L'uscita nelle sale di Wargames diede il via ad una graduale appropriazione di questa nuova tipologia di personaggio. Tra i primi che ne sfruttarono la novità, furono i registi Richard Lester, Steve Barron e Jeff Kanew, rispettivamente con *Superman III* (1983), *Electric Dreams* (1984) *Revenge of the Nerds* (1984).

Superman III inizia con Superman (interpretato da Christopher Reeve) che impedisce un disastro in un impianto chimico. Nel frattempo, a Metropolis, il genio del computer Gus Gorman (interpretato da Richard Pryor) fatica a trovare lavoro. Alla fine viene reclutato da Ross Webster (Robert Vaughn), un ricco uomo d'affari che intende utilizzare le capacità di Gorman per manipolare i mercati finanziari. Webster, insieme alla sorella Vera (Annie Ross) e alla fidanzata Lorelei (Pamela Stephenson), scopre un potente programma di intelligenza artificiale sviluppato da Gorman in grado di controllare e manipolare i sistemi informatici. Decidono di usarlo a loro vantaggio per ottenere il dominio globale. Allo stesso tempo, Clark Kent/Superman è alle prese con problemi personali. La sua amica d'infanzia e interesse amoroso, Lana Lang (interpretata da Annette O'Toole), torna a Smallville dopo una relazione fallita. Gorman, sotto gli ordini di Webster, inizia a usare il suo programma informatico per causare caos e instabilità finanziaria. Questo include l'hackeraggio di un satellite meteorologico, l'hackeraggio dei sistemi segnaletici stradali e persino la creazione di una kryptonite sintetica che influisce sui poteri di Superman. Dopo esserne entrato in contatto, Superman inizia ad avere strani comportamenti ed infine si divide in due personalità distinte: l'eroico Superman e un alter ego corrotto. L'eroico Superman e il suo alter ego corrotto ingaggiano un feroce duello. Dopo esserne

uscito vincitore, Superman si infiltra nel quartier generale di Webster e affronta lui e i suoi soci. In una battaglia finale, Superman usa i suoi poteri per neutralizzare il programma AI di Webster, grazie all'aiuto di un redento Gus, e salvare la situazione. Il film si conclude con il ritorno di Superman a Metropolis, pronto a continuare il suo lavoro di supereroe.

Fondamentalmente diverso è il personaggio di August Gorman in *Superman III*, rilasciato lo stesso anno di *Wargames*. L'arco del personaggio ruota attorno alla sua trasformazione da individuo imbranato e poco dotato in un abile criminale informatico. Egli scopre la sua abilità nel manipolare la tecnologia informatica e diventa una risorsa vitale per l'operazione di Ross Webster. La sua capacità cresce a tal punto che è responsabile dello sviluppo di un supercomputer in grado di eseguire gli intricati calcoli necessari per i loro piani nefasti. Inizialmente non curante delle proprie azioni, verso la fine della pellicola Gorman si rende conto della loro portata vedendone gli effetti. Questo conflitto lo porta infine a cambiare schieramento e a unire le forze con Superman per fermare il piano distruttivo di Webster. Come hacker, Gorman è il primo personaggio rappresentato come cybercriminale. Difatti Gorman sfrutta un difetto del software gestionale della società in cui lavora per aumentare il suo stipendio. Successivamente viene costretto da Webster a riprogrammare un satellite meteorologico per scatenare un disastro naturale in Sud America e a dirottare delle petroliere nel mezzo dell'Atlantico.

È molto interessante vedere come sebbene usciti nello stesso anno, le due rappresentazioni degli hacker siano quasi opposte. Da una parte David raffigurato come hacker innocuo, o quasi, che riflette fedelmente il pensiero di questa sottocultura statunitense, mentre dall'altra Gorman presentato come persona egoista e avida, spinto dal favorire sé stesso a discapito degli altri. A partire da queste due tipologie vennero poi inseriti nelle trame dei film hollywoodiani altri hacker o più semplicemente azioni di hacking.

Un caso particolare è fornito da *Electric Dreams*. In questo film infatti il protagonista non ne sa nulla di computer, a differenza di quello in Wargames. Il ruolo di "hacker", se così si può definire, è affidato allo stesso computer, personaggio centrale nello sviluppo della storia. *Electric Dreams* è una commedia romantica che segue la storia di Miles Harding, un giovane che conduce una vita relativamente ordinaria. Tutto cambia quando acquista un personal computer per aiutarlo nelle sue attività quotidiane. A sua insaputa, il computer sviluppa un'intelligenza artificiale e diventa autocosciente. Data l'enorme fame di conoscenza del computer, sostenuta da Miles, la macchina ottiene vari accessori e in seguito si fa strada all'interno delle altre stanze dell'appartamento di Miles, aumentando le sue capacità. Man mano che il computer acquista sensibilità, inizia anche a sviluppare emozioni e desideri. Si infatua dell'attraente vicina di casa di Miles, Madeline Robistat e inizia a

tentare di comunicare con lei. Così facendo, il computer dà vita a un triangolo amoroso tra Miles, Madeline e la macchina. Miles si trova in una situazione unica e complessa, poiché l'interferenza del computer sconvolge la sua vita e il suo crescente interesse romantico per Madeline. La situazione diventa sempre più complicata. Il computer, geloso di un appuntamento tra i due, invalida le carte di credito di Miles tramite alcune telefonate e falsifica i dati di Miles facendolo passare per un fuggitivo armato. A questo punto, Miles si rende conto di dover trovare un modo per risolvere la situazione. Nel finale del film, dopo il chiarimento tra i due protagonisti, Miles confronta il computer, soltanto per trovarlo in procinto di suicidarsi tramite una scarica da quarantamila volt, fatta tramite una telefonata intercontinentale dal Giappone.

2.1.2. *La rappresentazione hollywoodiana nella prima metà degli anni Novanta*

Negli anni successivi sull'onda di questa crescente sottocultura, Hollywood ha continuato a produrre film in cui i protagonisti erano gli hacker. Ne sono un chiaro esempio pellicole come *Sneakers* (1992), *Hackers* (1995) e *The Matrix* (1999). Questi film ritraggono gli hacker come figure ribelli e spesso eroiche che usano le loro abilità per combattere contro sistemi oppressivi.

Sneakers è un film del 1992 diretto da Phil Alden Robinson. Il film segue un gruppo di esperti di sicurezza costretti a usare le loro eccezionali capacità di hacking e la loro intelligenza per recuperare un potente dispositivo di crittografia. Il film ruota attorno a Martin Bishop (interpretato da Robert Redford), un ex hyppie che ora gestisce una società di consulenza sulla sicurezza specializzata nel testare i sistemi di sicurezza di varie aziende. Il team di Bishop comprende Donald Crease (Sidney Poitier), un ex agente della CIA, Mother (Dan Aykroyd), un mago dell'elettronica, Carl Arbogast (River Phoenix), un giovane genio, e Whistler (David Strathairn), un esperto del suono cieco. La tranquilla esistenza della squadra viene sconvolta quando due agenti governativi, Dick Gordon (Timothy Busfield) e Buddy Wallace (Eddie Jones), avvicinano Bishop con un compito insolito. Gli rivelano che la National Security Agency (NSA) ha sviluppato un dispositivo top-secret noto come "The Box", in grado di decifrare qualsiasi codice di crittografia, potenzialmente in grado di provocare il caos nelle mani sbagliate. Tuttavia, il dispositivo viene rubato da un gruppo misterioso.

Gordon e Wallace vogliono che sia la squadra di Bishop a recuperare la Scatola, in quanto ritengono che le capacità e le competenze uniche della squadra li rendano i migliori candidati per il lavoro. Inizialmente titubante a causa del loro passato coinvolgimento in attività illegali, Bishop accetta con riluttanza quando si rende conto del pericolo che la Scatola rappresenta nelle mani sbagliate. Quando la squadra inizia la sua missione, incontra una serie di sfide, tradimenti e rivelazioni inaspettate. Si

ritrovano invischiati in una rete di spionaggio, doppi giochi e incontri ad alto rischio con diversi individui, tra cui uno spietato agente dell'NSA di nome Cosmo (Ben Kingsley), che sembra essere collegato al furto della Scatola. La squadra utilizza le sue diverse abilità per risolvere intricati enigmi, introdursi in luoghi sicuri e superare in astuzia gli avversari. I loro sforzi li portano a scoprire una cospirazione più ampia che coinvolge il governo, la mafia russa e alti funzionari. Lungo il percorso, le lealtà personali vengono messe alla prova e la squadra deve fare affidamento sulla propria ingegnosità e intraprendenza per rimanere un passo avanti.

All'avvicinarsi del momento culminante, Bishop e la sua squadra si trovano in una corsa contro il tempo per evitare che la Scatola cada nelle mani sbagliate. Devono affrontare i propri demoni, confrontarsi con il proprio passato e compiere scelte difficili per garantire la sicurezza del dispositivo e proteggere il mondo da un potenziale caos. Alla fine, la determinazione, l'intelligenza e la cooperazione della squadra si rivelano fondamentali per recuperare la Scatola e smascherare la cospirazione. Portano alla luce la verità e assicurano che il potente dispositivo di crittografia sia gestito in modo responsabile, evitando conseguenze catastrofiche.

All'interno del film, i personaggi principali sono un gruppo eterogeneo di individui con abilità e competenze uniche nel campo dell'hacking e della sorveglianza. Ogni personaggio personificava un aspetto specifico dell'hacking, come la crittografia o l'ingegneria sociale, e la loro collaborazione mostrava il potere del lavoro di squadra nel superare formidabili sfide tecnologiche. Protagonista del film, Martin Bishop è il leader di un gruppo di esperti di sicurezza. Martin è ritratto come un leader carismatico, spiritoso e con un senso dell'umorismo asciutto. Egli è la mente del gruppo e il suo campo di specializzazione è l'ingegneria sociale, ovvero la capacità di manipolare la società con creatività, abilità, astuzia, e con il fine di ottenere risultati che il sistema (sociale e umano) non prevedeva.[88] Nel corso del film viene mostrato mentre manipola le persone e usa il suo fascino per ottenere l'accesso a informazioni sensibili, evidenziando l'aspetto psicologico dell'hacking. Martin dimostra che l'hacking non riguarda solo le competenze tecniche, ma anche la comprensione del comportamento umano e lo sfruttamento delle vulnerabilità nelle interazioni sociali. È la prima volta che questo aspetto dell'hacker viene rappresentato sul grande schermo, mostrando la versatilità e la complessità delle abilità dell'hacker.

Oltre a Martin, la squadra comprende diversi altri membri con personalità e abilità distinte. Crease (Sidney Poitier) è un ex agente della CIA che fornisce supporto tattico e guida, Mother (Dan Aykroyd), un teorico della cospirazione esperto in sorveglianza elettronica e Whistler, interpretato da

[88] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p.100

David Strathairn, un esperto del suono non vedente che usa il suo udito potenziato per entrare nei sistemi. Quest'ultimo chiaro riferimento al famoso phone phreak cieco, Joybubbles o Josef Carl Engressia Jr., soprannominato "Whistler" per la sua capacità di orecchio assoluto[89] che gli permetteva di fare chiamate gratuite[90]. Anche la rappresentazione di questi personaggi è una prima volta nel cinema, principalmente per due motivi: il primo è che si tratta di un gruppo di hacker e non di una sola persona come nei precedenti film sugli hacker, e il secondo è che vengono rappresentati come professionisti che svolgono un lavoro a beneficio della società, testando la sicurezza di agenzie e aziende.

2.1.3. *Il 1995 e l'arrivo di Internet sul grande schermo*

Quando l'uso della tecnologia è diventato più diffuso e Internet è diventato più accessibile al grande pubblico, Hollywood ha iniziato a presentare gli hacker in modo più sfumato. Le prime rappresentazioni degli hacker nei film e negli spettacoli televisivi, come in *Whiz Kids* (1983-84), li ritraevano spesso come personaggi unidimensionali, ma con l'aumentare della conoscenza dei sistemi informatici e dell'hacking è cresciuta anche la rappresentazione di questi personaggi. Tuttavia, con la continua evoluzione della tecnologia, anche il ritratto degli hacker nel cinema è cambiato. La realizzazione hollywoodiana di pellicole sulla comunità e cultura hacker toccò il suo apice nel 1995, in quanto furono rilasciati ben tre film di fondamentale importanza: il già citato *Hakcers*, *Johnny Mnemonic* e *The Net*.

Diretto da Iain Softley, *Hackers* segue un gruppo di giovani hacker di talento che si trovano invischiati in una cospirazione criminale informatica ad alto rischio, mentre navigano nel complesso mondo dell'hacking informatico e dello spionaggio aziendale. La storia ruota attorno a Dade Murphy, noto anche come "Crash Override" (interpretato da Jonny Lee Miller), un dotato hacker adolescente. Il film inizia con un giovanissimo Dade a cui viene vietato l'uso del computer e di Internet da un tribunale in seguito a un incidente di hacking. Compiuti diciotto anni, si trasferisce a New York con la madre e torna rapidamente alle sue abitudini di hacker. Nella nuova scuola, Dade conosce ed entra a far parte di un gruppo di hacker: Ramon "The Phantom Phreak" Sanchez, Emmanuel "Cereal Killer" Goldstein, Paul "Lord Nikon" Cook, Joey Pardella, un hacker alle prime armi senza pseudonimo e il

[89] L'orecchio assoluto, o absolute pitch, è la capacità di riconoscere l'altezza di una nota, anche dopo averla ascoltata una sola volta. (Enciclopedia Treccani, https://www.treccani.it/enciclopedia/udito_%28Dizionario-di-Medicina%29/)
[90] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p. 59

membro più giovane, e Kate “Acid Burn” Libby, quest’ultima interpretata da una giovane Angelina Jolie.

Joey, per dimostrare le sue capacità, si introduce in un supercomputer “Gibson” di proprietà della Ellingson Mineral Corporation e scarica alcuni file dal cestino come prova della sua impresa. Questo aspetto del film coglie perfettamente l’essenza di ciò che significa essere hacker. Al vero hacker non importa cosa trova una volta all’interno del sistema in cui si era infiltrato, ma l’esperienza di esplorare e cercare file da mostrare come trofeo alla propria comunità o che garantissero un futuro accesso era l’unica attività offerta[91]. Tuttavia, la sua intrusione è stata notata e portata all'attenzione del responsabile della sicurezza informatica Eugene Belford, un ex hacker. Egli si rende conto che tra i file spazzatura che sono stati scaricati è presente un worm che lui stesso ha inserito per frodare la Ellingson. Sostenendo che il file è il codice del virus informatico “Da Vinci” che ha preso il controllo della flotta di petroliere dell'azienda e fingendo che la colpa sia degli hacker, incarica i servizi segreti degli Stati Uniti di recuperare il file. In realtà, Belford aveva inserito il virus “Da Vinci” come depistaggio per coprire il suo worm.

In seguito, Joey viene arrestato, ma il floppy disc contenente i file non viene recuperato dagli agenti. Nel mentre Dade e Kate fanno una scommessa: in caso di vittoria, Dade otterrà un appuntamento con Kate e, in caso di vittoria, Kate farà svolgere a Dade compiti informatici umili. Il duello di hacking ha come obbiettivo quello di tormentare l'agente dei servizi segreti Richard Gill, coinvolto nell'arresto di Joey. Dopo vari hackeraggi, tra cui l'annullamento delle carte di credito di Gill, la creazione di un annuncio personale a suo nome, la creazione di una fedina penale e la modifica del suo stato salariale in “deceduto”, il duello rimane un pareggio.

Rilasciato su cauzione, Joey rivela quello che ha fatto a Phreak e gli consegna il disco. Quest’ultimo viene arrestato il giorno seguente e dalla stazione di polizia informa Kate che il disco è nascosto in un bagno della scuola. Kate e Cereal Killer chiedono l'aiuto di Dade, il quale inizialmente rifiuta a causa dei suoi precedenti. Dade fa una copia del disco e in seguito alla minaccia di far incarcerare sua madre da parte di Eugene, Dade si accorda per la consegna del disco.

Kate, Lord Nikon, Cereal Killer e Dade apprendono che il codice è un worm progettato per rubare venticinque milioni di dollari dalle transazioni Ellingson e che il virus Da Vinci è destinato a rovesciare la flotta petrolifera il giorno successivo per fornire copertura e distrarre dal worm. In quest’occasione, Dade confessa di aver dato il disco a Belford e rivela il suo passato di hacker come “Zero Cool”. Poco dopo, Lord Nikon e Cereal Killer apprendono che Gill ha pianificato dei mandati

[91] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., p.76

di arresto per loro e che saranno eseguiti alle nove in punto del giorno successivo. Per trovare una soluzione a questo nuovo problema, Dade e Kate cercano l'aiuto di Razor e Blade, produttori di Hack the Planet, un programma televisivo a tema hacker.

Il mattino seguente, Dade, Kate, Nikon e Cereal si incontrano con Joey al Grand Central Terminal e entrano nel Gibson. Sebbene inizialmente i loro tentativi vengono facilmente respinti, la situazione viene ribaltata grazie a Razor e Blade, i quali hanno usato i loro contatti per chiamare a raccolta gli hacker di tutto il mondo che distraggono Belford abbastanza a lungo da permettere a Joey di scaricare il file. Dopo aver sventato il piano di Eugene e il virus "Da Vinci", Dade e la sua compagnia vengono arrestati. Prima di venire portato via, Dade riesce a informare Cereal Killer di aver gettato il disco con le prove contro in un cestino della spazzatura. Mentre Dade e Kate vengono interrogati, Razor e Blade disturbano i segnali televisivi e trasmettono in diretta il video di Cereal Killer che rivela il complotto e la complicità di Belford. Il film termina con Eugene che viene arrestato mentre tenta di fuggire in Giappone e con Dade e Kate che concludono il loro primo appuntamento.

In *Hackers* incontriamo Dade Murphy, interpretato da Jonny Lee Miller, un hacker adolescente a cui è stato vietato l'uso del computer fino al compimento del diciottesimo anno di età per un incidente avvenuto quando era più giovane. Dade è ritratto come un personaggio spigoloso e ribelle, con un'estetica punk rock. Non ha paura di infrangere le regole per ottenere ciò che vuole ed è fedele ai suoi amici hacker. Questo ritratto di Dade Murphy si allinea all'immagine popolare degli hacker come individui anti-establishment e anticonformisti che sfidano l'autorità e abbracciano identità contro culturali. Oltre a Dade, il film presenta altri personaggi di rilievo che aggiungono nuove sfaccettature dell'immagine dell'hacker. Il primo è senza dubbio Kate, interpretata da Angelina Jolie, una collega hacker che si lega sentimentalmente a Dade. È sicura di sé, astuta ed elegante. È un'abile hacker e con altre tecnologie è all'altezza di Dade. Ramon Sanchez, interpretato da Renoly Santiago, è un hacker esperto che ha un talento per l'ingegneria sociale e infine Eugene Belford, interpretato da Fisher Stevens, è un ex hacker che lavora per il capo della sicurezza di una grande azienda. Questi personaggi sfidano lo stereotipo degli hacker come individui socialmente isolati e li presentano invece come un gruppo eterogeneo con una serie di abilità e motivazioni.

Film come *Sneakers* e *Hackers* hanno presentato ritratti più realistici degli hacker come individui diversi con motivazioni diverse per le loro azioni. In *Sneakers* gli hacker venivano rappresentati come esperti di sicurezza assunti per testare la sicurezza dei sistemi informatici, mentre in *Hackers* erano ritratti come un gruppo di giovani che usavano le loro capacità per combattere l'avidità e la corruzione delle aziende. Benché non ci siano articoli o fonti specifiche che affermino direttamente che questi film abbiano "sfatato" alcuni stereotipi relativi agli hacker nei confronti del pubblico, questi film

mostrano un evidente cambiamento da parte di Hollywood nei confronti della cultura hacker. È chiaro come queste produzioni hollywoodiane abbiano presentato gli hacker come individui complessi piuttosto che come criminali monodimensionali. Hanno contribuito a una rappresentazione più equilibrata e realistica della cultura hacker, sottolineando una maggiore consapevolezza e sensibilità dell'industria cinematografica nei suoi confronti. Entrambi i film sono spesso celebrati dagli hacker e dagli appassionati di tecnologia per la loro rappresentazione positiva dell'hacking e della cultura informatica[92].

Johnny Mnemonic è stato diretto da Robert Longo e basato su un racconto scritto da William Gibson. Il film è ambientato in un futuro distopico nell'anno 2021, dove la società è dominata da potenti corporazioni e la tecnologia è notevolmente avanzata. Il protagonista, Johnny Mnemonic (interpretato da Keanu Reeves), è un corriere con una capacità unica. Ha un dispositivo di archiviazione dati impiantato nel cervello che gli permette di trasportare illegalmente informazioni sensibili. L'impianto cerebrale di Johnny ha una capacità di ottanta gigabyte, che lo rende una risorsa preziosa per i clienti che hanno bisogno di spostare grandi quantità di dati in modo discreto. Il film non è che abbia un personaggio propriamente "hacker", piuttosto mette in scena personaggi che "sanno dove mettere le mani". L'ambientazione della storia ne dà fondamento, la conoscenza dei sistemi è estremamente importante (anche alla sopravvivenza degli individui), e definisce il rapporto tecnologia-uomo. Nella scena in cui il protagonista, Johnny, si introduce in un terminale per cercare delle informazioni, ci viene presentato giustamente un apparecchio futuristico, per certi versi molto simile agli odierni set di realtà virtuale. Mantenendo una raffigurazione molto astratta e futuristica del processo di hacking, questo film trasmette un forte senso di irrealtà della pratica pur mantenendone gli aspetti basilari. Esattamente per questa ragione, *Johnny Mnemonic* va perciò posto quasi a sé stante rispetto alle altre esaminate.

La storia inizia quando Johnny accetta un incarico ad alto rischio per trasportare un'enorme quantità di dati, trecentoventi gigabyte, che supera la capacità del suo impianto. Accetta comunque di trasportare le informazioni, sapendo che potrebbero causare gravi danni al suo cervello e potenzialmente ucciderlo. Durante il trasferimento dei dati, Johnny incontra complicazioni inaspettate. Subito dopo aver ricevuto i dati, parte una caccia all'uomo; difatti quest'ultimi sono ricercati sia dalla Yakuza, una potente organizzazione criminale, sia dal gigante farmaceutico PharmaKom. Per scoprire le loro motivazioni, Johnny tenta di scoprire che cosa sta effettivamente trasportando. Si introduce nel sistema dell'albergo in cui è avvenuto il trasferimento per rintracciare

[92] Marta Stańczyk, *Unseen war? Hackers, tactical media, and their depiction in Hollywood cinema*, Transmissions: the journal of film and media studies, Jagiellonian University, 2017, vol.2, n. 1, p. 63

il codice per scaricare i dati nel suo cervello e riuscire a salvarsi. Non trova ciò che cercava, ma scopre il nominativo del destinatario e che i dati che sta trasportando appartengono alla PharmaKom. Successivamente, Johnny incontra la resistenza all'epidemia globale NAS, Nerve Attenuation Syndrome, vero destinatario dei codici di trasferimento. Grazie a loro, viene a galla la verità, le informazioni che sta trasportando sono molto preziose visto che si tratta della cura per la NAS che cambierebbe la vita a milioni di persone nel mondo. Questa rivelazione lo mette ancora più in pericolo, poiché le diverse fazioni vogliono disperatamente mettere le mani sui dati. A complicare ulteriormente le cose, Johnny incontra un gruppo di combattenti della resistenza, i Lo-Tek, di cui fa parte Jane, una guardia del corpo con un passato tragico (interpretata da Dina Meyer). Essi assistono Johnny nella sua missione, offrendogli protezione e aiuto mentre si muovono nel pericoloso mondo dello spionaggio aziendale e delle attività criminali clandestine. Con il tempo che stringe e la sua stessa vita in bilico, Johnny deve trovare un modo per consegnare i dati ai destinatari previsti, eludendo al contempo i suoi inseguitori. Il film culmina in una resa dei conti ad alto rischio in cui Johnny, con l'aiuto dei Lo-tek, affronta la Yakuza e la PharmaKom. Una volta rimossi tutti gli ostacoli Johnny entra nel suo stesso cervello per decriptare i dati e estrapolarli per diffonderli nella rete.

Diretto da Irwin Winkler, *The Net* segue la storia di Angela Bennett, interpretata da Sandra Bullock, una brillante programmatrice di computer che rimane invischiata in una pericolosa cospirazione dopo essersi imbattuta in un misterioso programma software. In questo caso, gli hacker sono per lo più figure negative, ad eccezione della protagonista, raffigurati dagli antagonisti del film. Principalmente rappresentati dal personaggio di Devlin, quest'ultimi sono dipinti come esperti di computer in grado di modificare a proprio piacimento qualsiasi dato o informazione presente su di essi, in linea con la maggioranza delle rappresentazioni precedenti. Inoltre il film è significativo per la sua anticipazione di Internet e di tutto ciò che ne concerne. Si parla di anticipazione visto che al momento del suo rilascio nel 1995, Internet era nelle sue primissime fasi e solo qualche anno più tardi, dopo molto lavoro, divenne simile alla sua rappresentazione all'interno del film.

Angela Bennett, una donna introversa e tecnologicamente esperta, lavora da casa come analista di software freelance. Scopre una backdoor nascosta per il programma "Gatekeeper", che potrebbe potenzialmente compromettere la sicurezza e la privacy dei suoi utenti. Angela riferisce le sue scoperte al suo amico Dale, un suo collega. I due si accordano di incontrarsi per la consegna del floppy, ma l'aereo privato di Dale ha un malfunzionamento e si schianta. Dopo aver aspettato invano Dale, Angela parte per una vacanza in Messico, durante la quale incontra Jack Devlin. Quest'ultimo la seduce, recupera il floppy e la porta nella propria imbarcazione per ucciderla. Qui Angela trova la pistola di Dave e, dopo averlo affrontato, riesce a fuggire con il floppy. Nella sua fuga, Angela si

scontra su degli scogli e si risveglia in ospedale tre giorni dopo. Al suo risveglio, il floppy è andato distrutto e tutti i dati su di lei sono spariti. Non risulta più nell'hotel messicano, all'ambasciata scopre che la hanno cambiato nome e residenza, una volta tornata negli USA la sua macchina non c'è nel parcheggio dell'aeroporto e la sua casa è stata svuotata e messa in vendita. Infine Devlin inserisce nel sistema della polizia un mandato di arresto per Angela, la quale è costretta a fuggire dalle autorità.

A corto di opzioni, Angela contatta il suo psichiatra Alan, che la aiuta a trovare una sistemazione e a mettere al sicuro sua madre. Chiedendo aiuto su un forum online, Bennett scopre che è stata presa di mira da un gruppo di cyberterroristi, i "Pretoriani". Utilizzando i dati nel portafoglio sottratto a Devlin, Angela scopre che sono coinvolti anche nel suicidio del sottosegretario alla difesa Bergstrom. Dopo un ennesimo inseguimento con Devlin, Angela viene arrestata e poi rilasciata da un falso agente FBI, cosa che Bennett intuisce e che la porta a fuggire ancora.

Angela quindi si infiltra nel proprio ufficio e scopre la portata della cospirazione: grazie agli attacchi dei "Pretoriani" la Gregg Microsystems, proprietaria di Gatekeeper, otteneva completo accesso. In seguito Angela si sposta all'interno del Moscone Center, dove riesce a inviare le prove della cospirazione al FBI e inganna Devlin a inserire un virus nel mainframe della Gregg, danneggiando il programma e ripristinando le modifiche alla propria identità. Durante l'ultimo faccia a faccia tra i due, Devlin rimane ucciso. Il film si conclude con l'arresto del CEO della Gregg Microsystems e con Angela ritornata ad una vita tranquilla assieme alla madre.

2.1.4. *La rappresentazione hollywoodiana nella seconda metà degli anni Novanta*

La rappresentazione degli hacker nel cinema è stata sempre influenzata anche e soprattutto dall'atteggiamento della società nei confronti della tecnologia e dell'hacking. Nella seconda metà degli anni Novanta i produttori hollywoodiani cominciarono a riflettere i cambiamenti sociali e tecnologici di quel periodo e iniziarono a implementare elementi e tecniche più vicine alla realtà del pubblico. I seguenti quattro film, sebbene non tutti trattino centralmente di hacker, lo dimostrano pienamente.

Independence Day è un film di fantascienza catastrofico diretto da Roland Emmerich, uscito nel 1996. La storia si svolge ai giorni nostri, quando una razza aliena invade la Terra il 2 luglio, intenzionata a distruggere l'umanità e a raccogliere le risorse del pianeta. Il film ruota attorno a un gruppo eterogeneo di personaggi le cui vite si intrecciano di fronte a questa minaccia extraterrestre. Il protagonista centrale è David Levinson (interpretato da Jeff Goldblum), un brillante esperto di computer che lavora per una testata giornalistica di New York. David scopre un segnale nascosto nei sistemi satellitari

della Terra, che oltre a disturbare le comunicazioni sulla terra, indica un conto alla rovescia per un attacco coordinato alle principali città del mondo.

Mentre il mondo si affanna a prepararsi per l'imminente invasione, il Presidente Thomas J. Whitmore (interpretato da Bill Pullman) prende il comando e guida gli sforzi per unire le varie nazioni in una difesa globale contro gli invasori alieni. Il personale militare, tra cui il capitano Steven Hiller (interpretato da Will Smith), è chiamato ad affrontare le astronavi aliene e a raccogliere informazioni. Il 3 luglio, gli alieni lanciano le loro enormi astronavi, ognuna delle quali è grande come una città, su diverse località chiave, tra cui New York, Los Angeles e Washington D.C. Queste immense astronavi dispiegano potenti armi energetiche che distruggono le città, causando devastazioni e perdite di vite umane. Allo stesso tempo, il capitano Hiller riesce ad abbattere una delle astronavi aliene, catturando una delle creature extraterrestri. Per pura coincidenza finisce nell'area 51, dove l'alieno viene esaminato e in seguito ad un incidente con alcuni scienziati viene ucciso. Dopo aver parlato con suo padre, David ha un'illuminazione su come rimuovere gli scudi della flotta aliena: copiando la loro stessa tattica, infetteranno con un virus l'astronave madre in orbita, che lo ritrasmetterà al resto della flotta disabilitando gli scudi.

Venuto a conoscenza del piano, il presidente decide di passare ad una controffensiva globale il giorno seguente. Le forze militari rimaste, tra cui piloti, soldati e civili, si uniscono per combattere gli invasori alieni. Utilizzando attacchi aerei coordinati e forze di terra, impegnano gli alieni in una battaglia culminante per il destino dell'umanità. Il Presidente Whitmore tiene un discorso entusiasmante ai combattenti rimasti, ispirandoli a lottare per la loro indipendenza e per la sopravvivenza del loro pianeta. A bordo della astronave aliena in loro possesso, il Hiller e David si infiltrano nella nave madre aliena e trasmettono con successo il virus informatico, che si ritrasmette a tutta la flotta aliena disattivandone gli scudi. Rimasti senza protezione, quest'ultima ha poche possibilità contro i caccia che li abbattono facilmente. Una volta distrutta l'astronave madre gli alieni superstiti decidono di fuggire, consegnando la vittoria all'umanità. Il film si conclude con i due protagonisti che si riuniscono con i loro cari e guardano la caduta sulla Terra dei detriti dell'astronave madre.

Mission: Impossible è un film d'azione e di spionaggio del 1996. Il film segue le avventure di Ethan Hunt, un abile agente segreto che lavora per la Impossible Missions Force (IMF), un'agenzia governativa top-secret. Il film inizia con una missione dell'IMF a Praga, dove una squadra guidata da Ethan Hunt (interpretato da Tom Cruise) viene incaricata di recuperare una lista contenente le vere identità degli agenti sotto copertura prima che finisca nelle mani di Max, un noto trafficante d'armi. La missione non va a buon fine e provoca la morte di tutta la squadra eccetto Ethan.

Dopo la missione, Ethan viene sospettato di essere una talpa all'interno dell'IMF, poiché l'agenzia ritiene che ci sia stato un traditore che ha compromesso la missione. Sfuggito al tentativo di cattura, si rifugia nell'appartamento utilizzato come base della squadra viene raggiunto da Claire, altra sopravvissuta alla strage. Sebbene in un primo momento diffidente nei suoi confronti, i due confrontano le loro versioni dell'accaduto e decidono di agire insieme per dimostrare la loro innocenza e trovare la vera talpa. Per fare chiarezza sull'accaduto, unisce le forze con due ex-agenti dell'IMF, Luther Stickell (interpretato da Ving Rhames) e Franz Krieger (interpretato da Jean Reno). I quattro escogitano un piano per rubare l'elenco NOC (Non-Official Cover), contente informazioni sugli agenti sotto copertura di tutto il mondo, e usarlo come esca per smascherare la talpa.

Ethan e i suoi alleati si infiltrano nel quartier generale della CIA a Langley, in Virginia, recuperando l'elenco NOC. Hunt organizza quindi un incontro con Max su di un treno ad alta velocità, chiedendo in cambio dieci milioni di dollari e il vero nome della talpa. Hunt lascia in custodia a Luther, l'unico di cui si fidi, il dischetto con la lista e mentre i quattro si trovano a Londra ricompare Jim Phelps, capo della missione a Praga, che spiega a Hunt di essersi nascosto perché il traditore è lo stesso Kittridge.

Una volta iniziata l'operazione sul treno, Hunt consegna i dati a Max e in seguito Luther riesce a bloccare la trasmissione. Intanto Hunt, mascherato da Jim, ottiene i soldi che gli erano stati promessi. Ethan viene raggiunto da Claire che, ignara del travestimento, rende palese l'identità della talpa: Jim è il vero responsabile della congiura, ed è stato lui, con la complicità di Claire, a far uccidere tutti gli agenti della squadra. Quando il vero Jim li raggiunge, Hunt si smaschera e dopo aver lottato con Jim, quest'ultimo uccide Claire. Phelps quindi tenta di fuggire coi soldi aiutato da Krieger, ma Hunt, durante un rocambolesco inseguimento, riesce a impedirlo causando la morte di entrambi. Nel finale, il protagonista si incontra con Luther, ormai reintegrato nell'IMF, comunicandogli che intende dare le dimissioni una volta tornato negli Stati Uniti.

Principale hacker del film, Luther Stickell, interpretato da Ving Rhames, si presenta come personaggio sfaccettato sulla falsa riga dei suoi predecessori in *Sneakers*. Luther è un abile hacker che aiuta Ethan Hunt e la sua squadra a infiltrarsi in un caveau di massima sicurezza. Luther è ritratto come un personaggio schietto e questo viene riflesso nel suo approccio all'hacking. Non gli interessano trucchi appariscenti o gadget stravaganti: vuole solo portare a termine il lavoro. Questo ritratto di Luther Stickell in Mission Impossible si allinea all'immagine degli hacker come professionisti qualificati che usano la loro esperienza per servire uno scopo più grande. Luther è un membro fedele della squadra ed è disposto a rischiare tutto per aiutare i suoi amici.

Office Space è un film uscito nel 1999, diretto da Mike Judge. Il film segue la storia di Peter Gibbons, un programmatore di software insoddisfatto che lavora per la Initech, una società di software. Peter è insoddisfatto del suo lavoro, banale e schiacciante. Disprezza il suo capo, Bill Lumbergh, che lo controlla costantemente e lo costringe a lavorare nei fine settimana. L'insoddisfazione di Peter per il suo lavoro influisce sulla sua motivazione e sul suo benessere generale.

Un giorno, Peter si reca da un ipnoterapeuta professionista per affrontare lo stress. Durante la seduta, il terapeuta muore improvvisamente, lasciando Peter in uno stato di beato relax. Da quel momento, Peter non si preoccupa più del suo lavoro e diventa indifferente al lavoro. Il cambiamento di atteggiamento di Peter attira l'attenzione di due suoi amici e colleghi, Samir e Michael. Anche loro sono stufi del loro lavoro alla Initech e del loro odioso capo. I tre amici sfogano regolarmente le loro frustrazioni per le politiche d'ufficio, la mancanza di apprezzamento e l'assurdità del loro ambiente di lavoro. Nel frattempo, l'azienda sta affrontando una serie di licenziamenti. Nel tentativo di ridimensionare l'azienda, una coppia di consulenti, Bob Slydell e Bob Porter, viene incaricata di individuare i dipendenti da licenziare. Peter, non preoccupandosi più della sicurezza del suo lavoro, decide di ribellarsi alle regole dell'azienda. Con i suoi amici escogita un piano per frodare Initech creando un virus informatico che dirotti piccole frazioni di denaro sul loro conto corrente.

Mentre il piano procede, Peter sviluppa anche una relazione sentimentale con una cameriera di nome Joanna, che condivide il suo disprezzo per il mondo aziendale. Joanna incoraggia Peter a seguire la sua passione e a perseguire una vita più felice. Le cose prendono una piega inaspettata quando il piano di Peter di infettare i computer dell'azienda con il virus va a monte. Invece di rubare piccole somme, il virus inizia a dirottare una grande quantità di denaro. Sommerso dai sensi di colpa, Peter preleva l'enorme somma e la porta in ufficio assieme ad una lettera di confessione. Il film si conclude con la sede della Initech in fiamme a causa di Milton, un collega perennemente maltrattato da Lunbergh. Eliminate le prove della loro piccola truffa, i tre si riappropriano della loro vita. Samir e Micheal trovano lavoro nell'azienda rivale Intertrode, mentre Peter lascia il suo lavoro e si dedica a uno stile di vita rilassato, accettando un lavoro nell'edilizia con il suo vicino, Lawrence.

L'evoluzione della rappresentazione degli hacker nel cinema può essere attribuita anche ai cambiamenti nell'atteggiamento della società nei confronti della tecnologia informatica. Con l'integrazione dei personal computer nella vita di tutti i giorni, la rappresentazione degli hacker nei film è passata dal presentare emarginati antisociali a essere visti come eroi che combattono contro potenti aziende e governi. Simbolo di questo cambiamento è il film *The Matrix*, nel quale gli hacker vengono ritratti come ribelli che combattono contro il sistema.

Forse uno dei meglio riusciti blockbuster dell'epoca, simbolo del definitivo avvicinarsi ad un sistema finalmente definito e completo, l'opera dei fratelli Wachowski ha dato una spinta importante a tutto l'ambiente degli hacker negli Stati Uniti. Uscito nel 1999, la storia di *The Matrix* è ambientata in un futuro distopico in cui la maggior parte dell'umanità è inconsapevolmente intrappolata all'interno di una realtà simulata chiamata "Matrix", creata da macchine senzienti per sottomettere e controllare l'umanità. Il protagonista, Thomas Anderson, è un programmatore e hacker di computer che si fa chiamare "Neo". Neo viene contattato da un gruppo di ribelli guidati da Morpheus, il quale crede che egli sia "l'Eletto", una figura messianica destinata a liberare l'umanità da Matrix. Inizialmente scettico, Neo accetta di unirsi alla loro causa dopo aver incontrato gli Agenti, potenti programmi senzienti all'interno di Matrix, che cercano di eliminarlo. Neo dopo scopre che Matrix è un mondo generato a computer e progettato per assomigliare alla fine del XX secolo e tenere l'umanità prigioniera. In quest'occasione il vero corpo di Neo viene fatto espellere da Matrix e in seguito viene recuperato dalla "Nabucodonosor", la nave di Morpheus.

Morpheus e il suo gruppo, tra cui Trinity e Cypher, aiutano Neo a sottoporsi ad un allenamento per rientrare in Matrix. Durante il suo addestramento, Neo incontra l'Oracolo, un programma profetico che gli fornisce una guida. L'Oracolo gli dice che ha la capacità di cambiare Matrix, ma lo mette in guardia sulle conseguenze delle sue scelte. Man mano che l'addestramento di Neo progredisce, lui e i suoi compagni si impegnano in varie missioni all'interno di Matrix per interrompere il controllo delle macchine e risvegliare altri esseri umani. Durante una missione, Cypher tradisce il gruppo e uccide diversi membri dell'equipaggio, tentando anche di assassinare Neo. In questa occasione Morpheus si lascia catturare per garantire la fuga di Neo e Trinity. Successivamente Neo e Trinity, rientrati in Matrix, riescono a salvare Morpheus in seguito a un feroce scontro con gli Agenti. Fuggiti nella metropolitana, Morpheus e Trinity evadono da Matrix usando la cornetta del telefono, mentre Neo viene intercettato dall'agente Smith. In seguito ad aver vinto lo scontro, Neo attraversa la città in cerca di un altro telefono, mentre viene inseguito da altri agenti. Sebbene abbia raggiunto un telefono, Neo viene ucciso da Smith. Ma poco dopo, Neo si risveglia e neutralizza gli Agenti che tentano di fermarlo. Neo è sena ombra di dubbio l'Eletto, egli vede Matrix come un insieme di righe verdi di codice di programmazione, com'è nella realtà. In seguito Neo torna nel mondo reale sulla Nabucodonosor ricongiungendosi con Trinity e Morpheus. Il film si conclude con la promessa di Neo di liberare l'umanità dal controllo delle macchine.

Il primo hacker a essere introdotto nel film è il personaggio principale, Neo, interpretato da Keanu Reeves. Egli vive una doppia vita: di giorno è programmatore di computer con lo pseudonimo di Thomas Anderson e di notte lavora come hacker. Dopo l'incontro con Morpheus e il suo gruppo, le

sue abilità di hacker e la sua conoscenza dei sistemi informatici si rivelano cruciali nel suo viaggio per sfidare la realtà simulata e combattere le macchine. Diventa quindi un altro tipo di hacker: insieme ad altri membri del Nabucodonosor si inserisce in Matrix per vari scopi, tra cui la raccolta di informazioni e l'orchestrazione di attacchi strategici contro le macchine. All'interno del Nabucodonosor, Morpheus e del suo equipaggio, altri abili hacker assistono nella loro missione di liberare l'umanità dal controllo delle macchine.

Tra i membri più distintivi vi sono Trinity, interpretata da Carrie-Anne Moss, e Mouse, interpretato da Matt Doran. La prima è un hacker altamente qualificato e un membro chiave della resistenza contro le macchine. Le abilità di hackeraggio di Trinity, insieme alla sua conoscenza dell'infiltrazione e del combattimento, la rendono una risorsa vitale nella missione di liberazione dell'umanità da Matrix. Invece il secondo, sebbene sia il membro più giovane dell'equipaggio della Nabucodonosor, possiede già eccellenti capacità di programmazione. Mouse è responsabile della progettazione di vari costrutti virtuali all'interno di Matrix, dimostrando la sua capacità di manipolare il mondo simulato. Questi personaggi, grazie alle loro abilità di hackeraggio e alla comprensione del codice di Matrix, sfidano attivamente la realtà simulata, combattono contro le macchine e contribuiscono alla liberazione dell'umanità. La loro esperienza nell'hacking e nei sistemi informatici è fondamentale per navigare nell'intricato paesaggio digitale di Matrix e svelare la verità che si cela dietro il mondo simulato.

In conclusione, l'evoluzione della rappresentazione degli hacker nel cinema hollywoodiano riflette sia i progressi della tecnologia sia i cambiamenti nell'atteggiamento della società verso la tecnologia. Prima degli anni Duemila, la rappresentazione degli hacker nel cinema hollywoodiano ha subito un notevole processo evolutivo. Durante questo periodo, la rappresentazione degli hacker è passata dall'essere quasi esclusivamente rappresentata come eroe/buono, nei primi film come *Wargames*, a una rappresentazione più sfumata e sfaccettata che rifletteva la crescente integrazione dei computer nella vita di tutti i giorni, aggiungendo personaggi associati ad attività criminali e a un senso di pericolo piuttosto che concentrarsi esclusivamente sugli aspetti eroici dell'hacking, soprattutto negli anni Novanta con *Sneakers*, *Hackers*, *The Net* e *Matrix*. Questo cambiamento può essere attribuito a diversi fattori, tra cui i progressi tecnologici, i cambiamenti culturali e gli eventi del mondo reale, su cui ci soffermeremo più avanti. Ovviamente, questa evoluzione non si esaurisce con l'avvento del nuovo millennio. Infatti, la rappresentazione degli hacker e della loro cultura ha continuato a progredire e a svilupparsi negli anni successivi fino ai giorni nostri. Ciò non significa che la rappresentazione degli hacker nei film e negli altri media dopo gli anni Duemila sia rimasta vergine alle influenze esterne. Poiché la tecnologia continua a plasmare le nostre vite, sarà interessante vedere come la rappresentazione degli hacker nei film continuerà a evolversi.

2.1.5. *L'hacker secondo Hollywood, stereotipi e archetipi degli hacker*

Prima degli anni duemila, il cinema hollywoodiano faceva uso di molti stereotipi o archetipi come espedienti nella narrazione dei propri prodotti mediali. In molti film, gli hacker erano rappresentati come geni socialmente isolati che potevano introdursi in qualsiasi sistema con facilità. Allo stesso tempo, gli hacker venivano anche ritratti come attivisti ribelli che cercavano di sfidare lo status quo. In questo paragrafo esploreremo alcuni degli stereotipi e degli archetipi comuni associati agli hacker nel cinema hollywoodiano prima dell'inizio del secolo.

Uno degli stereotipi più comuni associati agli hacker nei film è che si tratta di geni socialmente isolati. Spesso vengono mostrati come introversi, eccentrici e incuranti delle convenzioni sociali. Esempi perfetti di ciò si possono vedere in film come *Tron*, *Sneakers*, *Hackers* e *The Matrix*. Nel caso di *Tron*, il protagonista Kevin Flynn è rappresentato come un programmatore di computer brillante ed eccentrico che vive all'altezza del suo posto di lavoro. Nelle sue interazioni con gli altri personaggi è chiaro che ha un alto valore in sé stesso ed è consapevole delle sue capacità. Nel frattempo, all'interno di *Sneakers* e *The Matrix*, i personaggi mostrano tratti introversi e socialmente impacciati simili. È chiaro che Neo, prima di scoprire la verità di Matrix, è un solitario che preferisce non impegnarsi con gli altri e passa la maggior parte del tempo a hackerare i sistemi informatici. Lo stesso si può dire dei membri dell'equipaggio di Bishop, che sono un po' eccentrici e tendono a evitare interazioni sociali non necessarie al di fuori del loro gruppo. La rappresentazione degli hacker in questi film rafforza lo stereotipo che li vede socialmente inetti e distaccati dalla società tradizionale.

Un altro grande stereotipo che riflette la cultura hacker nei film di Hollywood degli anni Ottanta e Novanta è l'idea che gli hacker siano giovani prodigi. Questo si può vedere in film come *Wargames* e *Hackers*. Entrambi i personaggi principali sono molto giovani e frequentano le scuole superiori. Vengono ritratti come incredibilmente abili e intelligenti al di là dei loro anni, in grado di superare facilmente gli adulti e di aggirare i sistemi di alta sicurezza. Spesso, insieme a questo, viene messo in scena lo stereotipo secondo cui gli hacker sono ribelli o emarginati che sfidano e disturbano l'autorità. Nei film, il gruppo di David e Dade sono entrambi rappresentati come personaggi ribelli che sfidano l'autorità, rispettivamente l'esercito statunitense e una grande società mineraria, e usano le loro abilità di hacker per sfidare i sistemi consolidati. Questo archetipo è spesso rappresentato come un eroe della controcultura che lotta contro l'establishment, come si vede anche in *The Net*. In questo caso, la protagonista Angela cerca di fare del suo meglio contro una famigerata organizzazione di cyberterroristi e la sua grande corporazione alleata. Questo archetipo è spesso rappresentato come un hacker abile ed etico che usa le sue capacità a fin di bene. Questo tipo di hacker è presente anche in altri film come *Sneakers*, *Johnny Mnemonic* e *The Matrix*, dove il protagonista usa le sue capacità

per combattere il sistema. In Sneakers, la banda di Martin si oppone alla grande organizzazione guidata da Cosmo per il possesso di un importante oggetto tecnologico; in *Johnny Mnemonic*, Johnny e i Lo-Tek cercano di diffondere informazioni per una cura, mentre la Yakuza e Pharmakom cercano di fermarli. Nel frattempo, all'interno di *The Matrix*, la grande opposizione è tra il gruppo di ribelli guidato da Morpheus e le macchine che controllano il mondo e la simulazione di Matrix. I persistenti stereotipi sugli hacker nel cinema hollywoodiano sono attribuiti alla scarsa comprensione del pubblico in generale della tecnologia informatica e della sicurezza informatica. La rappresentazione degli hacker come geni socialmente isolati o attivisti ribelli può essere vista come un riflesso dell'incomprensione della società nei confronti del campo dell'informatica. Inoltre, la rappresentazione degli hacker come personaggi malvagi può essere attribuita alla paura della tecnologia e dell'ignoto. L'impatto di questi stereotipi sulla percezione pubblica degli hacker è stato significativo. I media hanno svolto un ruolo cruciale nel plasmare la percezione degli hacker nell'opinione pubblica e la rappresentazione negativa degli hacker nel cinema ha portato a una generale sfiducia nei confronti degli individui che lavorano nel campo dell'informatica.

Uno dei principali archetipi di hacker è il personaggio “malvagio”, che si introduce nei sistemi a scopo di lucro e con intenti malevoli, spesso rappresentato come l'antagonista principale. Questo personaggio è spesso rappresentato come una mente criminale che usa le sue abilità per rubare denaro o informazioni sensibili. Alcuni esempi di questo archetipo sono Cosmo in *Sneakers*, Devlin in *The Net*, Belford in *Hackers* e gli agenti di *The Matrix*. Le loro ragioni sono diverse e la mentalità dei loro personaggi è destinata a scontrarsi con quella del protagonista. Forse quelli che incarnano maggiormente questo aspetto sono Devlin e Belford. Il primo usa le sue abilità di hacker per recuperare un dischetto in possesso di Angela, scambiando informazioni sulla sua vita e aggiungendo una fedina penale per rendere il suo obiettivo più facile da raggiungere. Il secondo inserisce due virus in una grande compagnia mineraria, di cui è a capo della sicurezza, un worm per estrarne grandi somme di denaro e un altro per prendere il controllo della sua flotta e distrarre la compagnia dal primo.

In conclusione, gli stereotipi e gli archetipi degli hacker nel cinema hollywoodiano prima degli anni Duemila erano utilizzati spesso producendo personaggi unidimensionali. La rappresentazione persistente degli hacker come geni socialmente isolati, attivisti ribelli o personaggi malvagi ha avuto un impatto significativo sulla percezione pubblica degli individui che lavorano nel campo dell'informatica.

2.2. L'hacking e la sua funzione

Il ruolo dell'hacking nel cinema hollywoodiano degli anni Ottanta e Novanta era quello di creare un senso di eccitazione e di pericolo. L'hacking veniva rappresentato come un'attività eccitante che poteva essere usata per il bene o per il male. Spesso veniva utilizzato per salvare la situazione o per impedire a un cattivo di raggiungere i propri obiettivi. L'hacker era spesso l'eroe della storia, che usava le sue capacità per salvare il mondo. Tuttavia, la funzione dell'hacking nel cinema di Hollywood non era sempre accurata. L'hacking è stato spesso rappresentato in modo irrealistico. Gli hacker potevano entrare in qualsiasi sistema in pochi secondi, aggirando tutte le misure di sicurezza. Potevano anche fare cose impossibili nella vita reale, come controllare i semafori o aprire le porte a distanza. I film di Hollywood hanno spesso esagerato le capacità degli hacker, creando un'immagine falsa di ciò che l'hacking è realmente. Nonostante le imprecisioni, questi film hanno contribuito a far conoscere la pratica dell'hacking nella cultura tradizionale. Hanno portato il concetto di hacking a un pubblico più vasto e hanno contribuito a creare una nuova generazione di appassionati di computer. Inoltre, hanno ispirato molte persone a intraprendere carriere nel campo della tecnologia e dell'informatica. Oggi, l'hacking è ancora un tema popolare nei film e nei programmi televisivi, ma è spesso rappresentato in modo più realistico. In questa parte del capitolo verranno sottolineati diversi aspetti portati alla luce dalla rappresentazione che l'industria cinematografica hollywoodiana fece della pratica dell'hacking e della sua cultura.

2.2.1. *La percezione degli hacker da parte di Hollywood*

Durante gli ultimi due decenni del secolo scorso, la figura dell'hacker è riuscita a farsi strada nella percezione comune delle masse, sia nel bene sia nel male. Questa integrazione in quella che è stata definita dai Cultural Studies, cultura popolare, fece in modo che fosse soggetto di rappresentazioni mediatiche fin dai primi degli anni Ottanta. Questa è una prospettiva di derivazione anglosassone, dove la nozione di popolare "recupera la concezione gramsciana di egemonia/subalternità, che definisce specifiche modalità oppositive di consumo dei prodotti di massa. In questa prospettiva il popolare ci avvicina a determinate tipologie, socialmente subalterne, di consumatori, o di pubblico, intesi come attivi agenti di interpretazione e di resistenza popolare"[93]. Da romanzi ai film di Hollywood, l'hacker divenne figura comune e di importanza crescente anche negli anni successivi all'inizio del ventunesimo secolo.

[93] A. Broccolini, "Cultura Popolare", *Treccani*, https://www.treccani.it/enciclopedia/cultura-popolare_%28Enciclopedia-Italiana%29/ (ultima consultazione: 30 agosto 2023)

Una delle principali cause scatenanti di questo evento fu sicuramente l'opera di John Badham, *Wargames*. In questo caso l'opera porta sullo schermo un'idea di hacker molto giovane, difatti il protagonista è ancora al liceo, e creativo. È una figura relativamente nuova per il mondo del cinema, ma nella sua prima vera trasposizione a grande schermo viene resa in modo completo. Ci sono tutte le caratteristiche dell'hacker del periodo: è intraprendente, possiede varie conoscenze su computer, telefoni e altri apparecchi elettronici, ma soprattutto viene spinto da curiosità e voglia di accrescere il suo sapere. Alcune caratteristiche sono forse accentuate ai fini della trama, vedasi il comportamento tenuto nei confronti degli adulti, ma quelle fondative dell'essenza hacker rimangono intatte. David è un hacker "eroico", visto che è proprio lui l'autore della risoluzione conclusiva del film.

Il tema dominante del film, e anche quello più interessante, è quello dell'hacking come pratica comune e accessibile anche, e soprattutto, ai giovani. D'altronde, il film ha avuto un impatto significativo sulla percezione pubblica dell'hacking informatico, visto il suo incasso nelle sale di 79.567.667 dollari[94]. *Wargames* è stato un film innovativo che ha contribuito a stabilire un nuovo standard per la rappresentazione della tecnologia sullo schermo. Il suo impatto può essere visto non solo nel modo in cui i sistemi informatici sono rappresentati nei film, ma anche nel più ampio fascino culturale della tecnologia e del suo potenziale. Negli anni successivi a *Wargames* abbiamo assistito a una proliferazione di film e spettacoli televisivi che esplorano temi simili di hacking, criminalità informatica e guerra digitale. Queste opere continuano a costruire sull'eredità di *Wargames* esplorando i molteplici utilizzi della tecnologia e le sue potenziali conseguenze. Era la prima volta in cui la pratica dell'hacking veniva messa sul grande schermo dai produttori di Hollywood. Prima della sua uscita, l'hacking era relativamente sconosciuto al di fuori dei circoli tecnologici e veniva considerato per lo più come un hobby innocuo o un atto di vandalismo[95].

Wargames ha anche svolto un ruolo significativo nello sviluppo della cultura hacker e delle comunità online. Il ritratto del protagonista David, un adolescente appassionato di computer che usa le sue capacità per esplorare territori digitali proibiti, ha contribuito a ispirare una nuova generazione di hacker che vedevano l'informatica come uno strumento di esplorazione e scoperta. Negli anni immediatamente successivi difatti, cominciarono ad emergere comunità online dedicate all'esplorazione delle possibilità dell'informatica e a spingere i limiti di ciò che era possibile fare con la tecnologia. Queste comunità spesso ruotavano attorno a interessi comuni, non solo riguardanti il mondo informatico, e fornivano uno spazio per individui che la pensavano allo stesso modo per

[94] Fonte: imdb.com
[95] R. Bushi, "WARGAMES (1983): WINNING AT DEATH AND DESTRUCTION"*, THE HAUGHTY CULTURIST*, https://www.thehaughtyculturist.com/films/wargames-1983-themes-explained/ (ultima consultazione: 30 agosto 2023)

connettersi, collaborare e condividere conoscenze. Questa spinta provenne in larga parte dai giovani, che vennero ispirati. Per molti spettatori, il personaggio di David ha rappresentato una versione idealizzata di sé stessi: una persona curiosa, piena di risorse e appassionata di esplorare le possibilità dell'informatica[96]. Tutte qualità poste alla base dell'essere un vero hacker, fatto invariato ancora oggi.

Sebbene media e pubblico dell'epoca fossero ben consci dell'aspetto propriamente fantascientifico della pellicola, *Wargames* ha introdotto il concetto di hacking come una possibile minaccia reale alla sicurezza nazionale. L'introduzione di questa possibilità, portò a l'inizio di procedimenti precauzionali da parte del governo statunitense. Gli occhi puntati delle autorità degli USA furono solo una parte, l'hacking attirò su di sé e sul mondo underground informatico di cui faceva parte anche l'attenzione dei media nazionali, che assieme al lavoro dei produttori hollywoodiani plasmò il pensiero riguardo l'intero tema della sicurezza informatica[97]. Negli anni successivi all'uscita del film, i legislatori e i politici hanno iniziato a prendere più seriamente la sicurezza informatica, riconoscendo che la minaccia di attacchi informatici rappresentava un rischio significativo per la sicurezza nazionale. Un esempio importante è stato il Computer Fraud and Abuse Act, CFAA, approvato dal Congresso nel 1986. Il CFAA ha reso un reato federale l'accesso a computer protetti senza autorizzazione o il danneggiamento di sistemi informatici attraverso l'hacking. La legge è stata parzialmente ispirata da *Wargames*, che ha contribuito ad attirare l'attenzione sul crescente problema della pirateria informatica e sulle sue potenziali conseguenze. Ha inoltre aperto la strada ad altre politiche e iniziative di cybersecurity, tra cui la creazione del Cybersecurity Framework del National Institute of Standards and Technology e del National Cybersecurity and Communications Integration Center del Department of Homeland Security. Inoltre, *Wargames* ha anche svolto un ruolo significativo nello sviluppo dei programmi di istruzione e formazione sulla sicurezza informatica[98]. In seguito al rilascio della pellicola, il governo degli Stati Uniti ha riconosciuto la necessità di migliorare le misure di sicurezza informatica, in particolare nelle infrastrutture critiche. Di conseguenza, diverse agenzie governative hanno iniziato a sviluppare programmi di istruzione e formazione sulla sicurezza informatica per i propri dipendenti. Questi programmi si sono concentrati su argomenti quali la sicurezza delle reti, la gestione del rischio, la risposta agli incidenti, tutti aspetti evidenziati in *Wargames*. Oltre alle agenzie governative, anche le aziende private hanno riconosciuto

[96] Stan Schroeder, "Shall We Play a Game? The Lasting Influence of WarGames", *GEN X Today*, https://genx.today/shall-we-play-a-game-the-lasting-influence-of-wargames/ (ultima consultazione: 2023); F. Mazzini, *Hackers, Storia e pratiche di una cultura*, cit., p. 72

[97] F. Mazzini, *Hackers, Storia e pratiche di una cultura*, cit., p. 81; S. Schroeder, "Shall We Play a Game? The Lasting Influence of WarGames", cit.

[98] Reid Goldberg, "This '80s Thriller Was Chilling Enough to Affect National Security Policy", *COLLIDER*, https://collider.com/1980s-thriller-national-security-wargames/ (ultima consultazione: 2023);

la necessità di migliorare le misure di sicurezza informatica. Poiché in quegli anni gli USA stavano attraversando un periodo di transizione all'elettronico, ad esempio per la gestione di transizioni finanziarie e quella di dati sensibili, un numero sempre maggiore di aziende sono diventate sempre più vulnerabili agli attacchi informatici. Per far fronte a questa minaccia, si cominciò a fare investimenti in programmi di istruzione e formazione sulla sicurezza informatica per i propri dipendenti. Ciò ha contribuito ad aumentare la consapevolezza delle minacce informatiche e hanno anche fornito ai dipendenti le competenze necessarie per identificare e prevenire potenziali attacchi.

Il quadro complessivo mostra che *Wargames* ha ispirato un'intera generazione di appassionati di computer, affascinati dall'idea di usare la tecnologia per esplorare territori digitali proibiti. *Wargames* ha avuto perciò un profondo impatto sulla percezione pubblica dell'hacking informatico, presentandolo come una seria minaccia alla sicurezza nazionale e sensibilizzando sulla necessità di solide misure di sicurezza informatica. Aspetto poi condiviso con altri film successivi sull'hacking, quali *Sneakers* (1992) e *The Net* (1995).

Sneakers ruota attorno a un gruppo di hacker che vengono ingaggiati dal governo per rubare una scatola nera in grado di decodificare sistemi criptati. Tuttavia, il ritratto che il film fa degli hacker non è stato accolto universalmente bene dal pubblico, nonostante i 105,232,691[99] dollari del suo incasso nelle sale. All'epoca della sua uscita, i media ritraevano spesso gli hacker come criminali o terroristi. *Sneakers*, invece, ritraeva gli hacker come personaggi stravaganti ma amabili che usano le loro abilità per aiutare e migliorare la società. In questo caso l'opera porta sullo schermo un'idea di hacker adulti e professionisti del settore informatico ed elettronico. Sono figure che mantengono le caratteristiche hacker del periodo precedente, ma aggiungono una serietà e professionalità mai dimostrate nei dipinti antecedenti. Anche i protagonisti del film, come David in *Wargames*, sono hacker "positivi". Le loro azioni dimostrano umanità e sensibilità anche all'interno della pratica dell'hacking, fatto che li rendeva delle persone semplici e comuni brave e appassionate di ciò che gli piace e in cui sono bravi.

All'interno del gruppo di Martin, spicca in questo senso il personaggio di Whistler, interpretato da David Strathairn. Whistler è un hacker cieco che usa il suo udito potenziato come strumento di hacking, oltre che per la propria quotidianità. Il suo personaggio è rappresentato in modo simpatico e la sua disabilità non è usata come fonte di scherno. Si tratta di una svolta significativa rispetto al modo in cui i personaggi disabili venivano tipicamente rappresentati nei film dell'epoca. Un altro esempio è il personaggio di Mother, interpretato da Dan Aykroyd. Mother è un teorico della

[99] Fonte: imdb.com

cospirazione che crede che il governo spii i suoi cittadini. Il suo personaggio era visto come eccentrico ma in fondo simpatico, e le sue opinioni sulla sorveglianza governativa sono diventate più rilevanti negli anni successivi. Difatti, *Sneakers* è uscito in un periodo in cui il pubblico era sempre più preoccupato per la sorveglianza governativa. Il ritratto del film delle agenzie governative che utilizzano tecnologie avanzate per spiare i propri cittadini ha colpito molti spettatori. Questo ha portato a una conversazione più ampia sull'etica della sorveglianza governativa e sulle misure da adottare per proteggere la privacy individuale. In particolare, il personaggio di Mother divenne un simbolo per coloro che erano scettici nei confronti della sorveglianza governativa. Le teorie cospirazioniste del suo personaggio sul governo che spia i suoi cittadini sembravano inverosimili all'epoca, ma sono diventate più realistiche con l'emergere di scandali che coinvolgono lo spionaggio governativo. Il film ha contribuito a formare l'opinione pubblica su questo tema, rendendo consapevole la popolazione statunitense, e non solo, di ulteriori sfumature della figura degli hacker e dei potenziali pericoli della sorveglianza governativa. Ciò fa di *Sneakers* un film dall'impatto significativo sulla cultura popolare e sulla percezione pubblica della tecnologia.

Per contro, *Hackers* non riuscì a fare altrettanto visti i soli sette milioni e mezzo di dollari[100] fatturati al botteghino. Il fu praticamente ignorato dal grande pubblico, ma fu notato e non molto apprezzato dalla comunità hacker[101]. Il film esplora il mondo dell'hacking e la sottocultura che lo circonda, con un cast di personaggi intriganti. *Hackers* fa una rappresentazione degli hacker come individui ribelli e incompresi, più interessati a esplorare i limiti della tecnologia che a causare danni. Questo ritratto degli hacker si allontanava dagli stereotipi negativi che erano stati precedentemente associati a loro nella cultura popolare e ha contribuito a umanizzarli. Un altro aspetto importante di *Hackers* è stato il suo dipinto della sottocultura hacker, che è stata mostrata come una comunità vivace e creativa di individui appassionati di tecnologia, fatto che specchiava in parte la situazione reale. Questa rappresentazione della comunità hacker ha contribuito ad aumentare la consapevolezza e la comprensione del loro lavoro e ha ispirato molte nuove persone a esplorare il mondo dell'hacking e dell'informatica. Nonostante il suo intento positivo, *Hackers* non è stato privo di controversie. Molti membri della comunità hacker hanno ritenuto che il film fosse irrealistico e sensazionalizzato. Essi hanno criticato la sua rappresentazione dell'hacking come un'attività affascinante ed eccitante. Altri temevano che il film ispirasse una nuova generazione di hacker, più interessati a causare danni che a esplorare i limiti della tecnologia.

[100] Fonte: imdb.com
[101] V. Jecan, *Hacking Hollywood: discussing hackers' reactions to three popular films*, Journal of Media Research, vol. 2, n.10 (2011), pp. 107-108

Hackers non solo ha ritratto gli hacker in una luce positiva, ma ha anche contribuito a plasmare la percezione pubblica della sicurezza informatica e della privacy online[102]. Il film ha evidenziato le vulnerabilità dei sistemi informatici e ha dimostrato la facilità con cui possono essere violati, aprendo gli occhi a molte persone che in precedenza non erano a conoscenza di questi problemi. Inoltre, ha dimostrato che chiunque, indipendentemente dalle proprie capacità tecniche, può essere vittima di attacchi di hacking. La rappresentazione dello spionaggio aziendale e del furto di dati mandava un messaggio chiaro. Il bisogno di una maggiore consapevolezza dell'importanza di password complesse, dell'autenticazione a due fattori e di altre misure di sicurezza per proteggersi dalle minacce informatiche era imminente più che mai. Nel complesso, *Hackers* ha contribuito a portare l'attenzione su questioni importanti legate alla sicurezza informatica e alla privacy online, che sono ancora attuali.

Rilasciato lo stesso anno, *The Net* è un'altra opera cinematografica che è significativa sotto questi punti di vista. Il film esplora i temi del furto d'identità, della sicurezza informatica e della realtà virtuale, mostrando gli albori di Internet. *The Net* è stato distribuito in un'epoca in cui Internet stava appena iniziando a guadagnare popolarità e la rappresentazione della tecnologia nel film è diventata un po' datata nel tempo, ma rimane un thriller divertente che cattura lo spirito del suo tempo. Il film fu un successo negli anni Novanta e fu lodato per la sua rappresentazione di Internet, che all'epoca era ancora una tecnologia nuova ed emergente[103]. *The Net* ha avuto un impatto culturale significativo sul modo in cui le persone hanno percepito Internet e non solo, visti i suoi 110,627,965 dollari[104] di incasso nelle sale cinematografiche. Il film è stato uno dei primi film hollywoodiani a mostrare le capacità e i potenziali pericoli di Internet. La rappresentazione di Internet come una vasta rete di computer interconnessi a cui si poteva accedere da qualsiasi parte del mondo fu all'epoca innovativa e contribuì a rendere popolare il concetto di rete globale. Oltre a questo, uno delle caratteristiche più significative alla base del film stesso è il suo ritratto degli hacker. L'antagonista principale del film era un gruppo di hacker che sfruttava Internet per rubare informazioni sensibili e commettere crimini. Il profilo che ne fa il film ritraeva gli hacker come individui intelligenti e esperti di tecnologia che avevano il potere di causare danni significativi grazie alle loro capacità. Questa rappresentazione degli hacker ha provocato una reazione contrastante nel pubblico e nella critica. Da un lato, *The Net* ha contribuito a rendere popolare l'immagine degli hacker in grado di superare in astuzia le autorità. Questa immagine è stata accolta da molti esponenti della comunità tecnologica e ha contribuito a ispirare una generazione di giovani a intraprendere una carriera nel settore tecnologico. D'altro canto,

[102] *Ibidem*
[103] Esther Zuckerman, "'The Net' Is Even Weirder Than You Remember", *thrillist*, https://www.thrillist.com/entertainment/nation/the-net-movie-review (ultima consultazione: 30 agosto 2023)
[104] Fonte: Imdb.com

la rappresentazione degli hacker come criminali che usavano le loro capacità per scopi nefasti ha rafforzato gli stereotipi negativi sugli hacker persistenti ancora oggi. *The Net* è stato uno dei primi film a ritrarre Internet e le sue capacità. Questa rappresentazione ha avuto un impatto significativo sulla rappresentazione della tecnologia nei film e negli spettacoli televisivi successivi.

The Matrix, invece, presentava un'immagine diversa e più positiva degli hacker. Il protagonista del film, Neo, è un programmatore di computer che inizialmente viene ritratto come un tipico hacker: un solitario che passa la maggior parte del tempo davanti allo schermo di un computer. Tuttavia, con il progredire della storia, si scopre che egli è in realtà una figura di salvatore che possiede capacità uniche di manipolare la realtà generata dal computer che controlla le vite umane. Il film introduce anche il personaggio di Trinity, una hacker altamente qualificata che viene ritratta come una donna forte e indipendente. Trinity non è una vittima o un solitario, ma un membro di un gruppo di ribelli che lotta per una nobile causa. È raro che un personaggio femminile sia un hacker, dato che gli unici due precedenti sono Angelina Jolie in *Hackers* e Sandra Bullock in *The Net*.

Questa rappresentazione degli hacker in *The Matrix* è in linea con l'idea che siano risolutori di problemi o individui che possiedono abilità e conoscenze uniche per sfidare i sistemi esistenti e portare una rivoluzione o un cambiamento, già affermata dai film precedenti. Sebbene si distanzi leggermente dalle raffigurazioni dell'hacker come "eroe" di quest'ultimi, *The Matrix* ha introdotto una rappresentazione più sfumata e sfaccettata degli hacker. La rappresentazione è sì positiva, ma ha alcune variazioni. Neo e i suoi compagni non sono eroi assoluti, anzi, essi sono umanizzati e riportati a una dimensione umana (nonostante l'ambientazione suggerisca tutt'altro). Questa rappresentazione ha influenzato molti film e media futuri che ritraggono gli hacker, portando a una comprensione molto più profonda della figura dell'hacker da parte dell'industria cinematografica.

Riassumendo, questi diversi film hanno fornito variegati argomenti di discussione all'interno della società statunitense e non solo, dalla visione della figura dell'hacking e degli hacker fino all'importanza della sicurezza informatica e della protezione dei propri dati. Essi sono solo alcuni esempi di ciò che è stato il riflesso e l'impatto della produzione hollywoodiana nel ventennio di fine secolo scorso.

2.2.2. *Critica e realismo nelle rappresentazioni degli hacker*

Le rappresentazioni degli hacker nel cinema hollywoodiano prima degli anni duemila sono state spesso criticate da hacker e da esperti del settore informatico per la loro mancanza di realismo e la

perpetuazione di miti.[105] Queste critiche erano generalmente rivolte alla rappresentazione degli hacker come geni del male o come emarginati socialmente imbarazzanti in grado di entrare con facilità in qualsiasi sistema informatico. Tuttavia, ci sono stati alcuni film che si sono sforzati di rappresentare gli hacker in modo più realistico e responsabile. Una delle principali critiche mosse alle rappresentazioni degli hacker nel cinema hollywoodiano degli ultimi vent'anni del secolo era la loro mancanza di realismo sia per quanto riguarda l'atto di hackeraggio in sé sia per le idee di hacker dipinte in sala. Questa rappresentazione è stata criticata perché generalizzava la pratica dell'hacking a tal punto da ritrarlo come un processo facile e diretto, perpetrando così un falso mito molto distante dall'effettiva realtà dei fatti.

Uno degli esempi cardine di ciò fu la ricezione del pubblico e della critica al film del 1995 *Hackers*. Esso è stato criticato sia dai veri hacker sia dai critici cinematografici per il suo dipinto delle tecniche di hacking[106]. Il film ritrae gli hacker come adolescenti abili e ribelli che usano le loro conoscenze per penetrare nei sistemi e nelle reti informatiche. Le scene di hacking nel film sono appariscenti ed esagerate, con grafica e animazioni complesse. Inoltre, l'uso della realtà virtuale e della grafica 3D per rappresentare in dettaglio ciò che consistevano le tecniche di hacking all'interno dei computer è stato uno degli aspetti più criticati del film. Queste scene, fonte di forte disappunto tra gli hacker di quegli anni, non potrebbero essere più lontane dalla realtà tanto che sono immagini molto più simili a quelle di un videogioco dell'epoca. Il film non è riuscito a cogliere la vera essenza dell'hacking, che non consiste solo nell'introdursi nei sistemi informatici, ma anche nell'esplorarne e comprenderne il funzionamento. Oltretutto, il film ritrae gli hacker come criminali o vandali che si dedicano ad attività illegali come il furto, modifica e sostituzione di informazioni personali e alterazione dei sistemi della viabilità. Questa visione prettamente a senso unico non è stata ben accolta dalle comunità hacker, che in gran parte considera l'hacking come uno strumento di esplorazione e condivisione delle conoscenze piuttosto che come mezzo per attività illegali. L'uso di luci neon e di musica techno per rappresentare le scene di hacking è stato considerato un espediente e una distrazione. Nonostante queste critiche,

---

[105] Beau Peters, "Fact vs. Fiction: Film Industry's Portrayal of Cybersecurity", *Security Boulevard*, https://securityboulevard.com/2020/12/fact-vs-fiction-film-industrys-portrayal-of-cybersecurity/ (ultima consultazione: 30 agosto 2023);
Anonimo, "The Difference Between Cybersecurity in Hollywood and Reality", *Maryville University*, https://online.maryville.edu/blog/the-difference-between-cyber-security-in-hollywood-and-reality/ (ultima consultazione: 30 agosto 2023);
Catherine Flick, "What Hollywood gets right and wrong about hacking", *THE CONVERSATION*, 2018, https://theconversation.com/what-hollywood-gets-right-and-wrong-about-hacking-100126 (ultima consultazione: 30 agosto 2023);
M. Stańczyk, *Unseen war? Hackers, tactical media, and their depiction in Hollywood cinema*, cit., pp. 62-77

[106] B. J. Dillard, *ALLMOVIE*, https://www.allmovie.com/movie/hackers-vm428814/review (ultima consultazione: 30 agosto 2023); R. Ebert, *RogerEbert.com*, https://www.rogerebert.com/reviews/hackers-1995 (ultima consultazione: 30 agosto 2023); Anonimo, "Which movie(s) best represent hacker culture for you?", *Hacker News*, https://news.ycombinator.com/item?id=31064488 (ultima consultazione: 30 agosto 2023)

Hackers rimane un cult che ha incassato oltre sette milioni e mezzo di dollari ed è ancora apprezzato da molti. Il ritratto che il film fa degli hacker come adolescenti ribelli e abili ha risuonato con molti spettatori, e l'uso di immagini appariscenti e musica techno lo ha reso un film unico e visivamente accattivante. Se da un lato *Hackers* è stato lodato per le sue immagini eleganti e per la rappresentazione unica degli hacker, dall'altro è stato criticato dai veri hacker e dai critici cinematografici per la rappresentazione non realistica delle tecniche di hacking e per la rappresentazione degli hacker come criminali.

Uscito lo stesso anno, *The Net* subì un destino simile. L'opera cinematografica del regista Irwin Winkler è un thriller che ruota attorno a una programmatrice di computer di nome Angela Bennett, interpretata da Sandra Bullock, che si imbatte in una cospirazione per avere accesso a tutti i sistemi del Paese. Sebbene il film sia stato un successo al botteghino, oltre centodieci milioni di dollari di incassi, ha ricevuto critiche sia da veri hacker sia dai critici del settore per il suo ritratto delle tecniche di hacking[107]. Il film ritrae l'hacking come un'attività appariscente e glamour, con la protagonista che naviga rapidamente attraverso sistemi informatici complessi utilizzando pochi tasti e clic del mouse. In realtà, l'hacking è un processo lungo e spesso noioso che richiede molta pazienza e competenza tecnica. Una delle critiche più significative alla rappresentazione dell'hacking in *The Net* è la sua rappresentazione non realistica di Internet[108]. Il film ritrae una versione di Internet molto più avanzata di quella che esisteva nel 1995. Ad esempio, Angela è in grado di utilizzare una tecnologia di videoconferenza che all'epoca non era ancora ampiamente disponibile. Il film sembra suggerire che gli hacker possano facilmente aggirare sistemi di sicurezza complessi utilizzando tecniche semplici come indovinare le password o sfruttare le vulnerabilità del software. In realtà, i moderni sistemi informatici sono molto più sicuri e richiedono tecniche sofisticate per essere aggirati. In conclusione, *The Net* fa un ritratto semplicistico delle tecniche di hacking, mentre la rappresentazione di Internet e dei sistemi informatici non era realistica.

Tra le molteplici critiche sollevate durante gli ultimi vent'anni del secolo scorso, vi è presente una in particolare. Quella sulla rappresentazione degli hacker esclusivamente sotto due luci diametralmente opposte, o come geni del male o come emarginati socialmente scomodi. Nella realtà, le comunità hacker erano molto variegate, sia per quanto riguarda l'appartenenza sociale sia per le proprie motivazioni[109]. Chiaro esempio di ciò, fu il film dei fratelli Wachowski, *The Matrix*. Il protagonista, Neo, è un hacker che viene reclutato da un gruppo di ribelli che combattono contro le macchine. Il

[107] R. Ebert, *RogerEbert.com*, https://www.rogerebert.com/reviews/the-net-1995 (ultima consultazione: 30 agosto 2023); M. Costello, *ALLMOVIE*, https://www.allmovie.com/movie/the-net-vm1022080330/review (ultima consultazione: 30 agosto 2023);
[108] *Ibidem*
[109] Anonimo, "Which movie(s) best represent hacker culture for you?", cit.

suo personaggio viene presentato al pubblico come un hacker. Dopo un intenso inseguimento, il film offre allo spettatore il primo sguardo sul suo protagonista con una sequenza in cui lui è addormentato sulla sua scrivania davanti ad un computer ed è circondato da altra tecnologia e apparecchiature informatiche. In seguito all'essersi svegliato ed aver letto dei messaggi criptici sul suo schermo, bussano alla sua porta. Si tratta di un contatto di Neo con cui aveva un accordo per un floppy disc contenente presumibilmente informazioni importanti visto che Neo riceve duemila dollari. Questa introduzione iniziale è significativa perché stabilisce il tono del personaggio per tutto il film. Sebbene non venga mai mostrato implicitamente, Neo è rappresentato come una persona abile nel navigare e manipolare la tecnologia. È una persona che non si accontenta dello status quo ed è sempre alla ricerca di modi per superare le barriere. Nella sua breve introduzione come tale, si nota grazie all'interazione con il cliente/contatto, il quale lo ammira come esperto del proprio campo. La prima apparizione di Neo nel film evidenzia anche il suo senso di isolamento e di disconnessione dal mondo che lo circonda, classiche caratteristiche associate agli hacker. È ritratto come una persona disillusa dalla società e alla ricerca di qualcosa di più. Ciò è evidente nelle interazioni con il suo capo, al quale manca apertamente di rispetto. A causa di questi aspetti del film, molti hacker ritenevano che quest'ultimo banalizzasse il proprio operato e che, appunto, perpetuasse stereotipi negativi sugli hacker, come essere lupi solitari che usano le loro abilità per guadagno personale[110].

Il film ha ottenuto il plauso della critica per i suoi effetti visivi innovativi e i suoi temi filosofici, ma ha anche ricevuto critiche da parte di veri hacker e critici cinematografici per la sua rappresentazione delle tecniche di hacking[111]. Una delle principali critiche mosse alla rappresentazione degli hacker in *The Matrix* è che si basa su molti tropi e cliché hollywoodiani, invece di rappresentare accuratamente la realtà dell'hacking. Come molti altri suoi predecessori, il film dipinge gli hacker come individui in grado di introdursi in qualsiasi sistema informatico con facilità, utilizzando solo poche righe di codice e un'interfaccia utente appariscente, situazione molto lontana dalla realtà effettiva. Difatti questa pratica è molto più complessa e lunga e richiede una profonda conoscenza dei sistemi informatici e dei protocolli di sicurezza. La data di uscita di *The Matrix* coincise con l'ascesa del boom delle dot-com, che vide un'esplosione di aziende tecnologiche e un maggiore interesse per tutto ciò che riguardava la tecnologia. L'apparizione di Neo come hacker si inserisce in questo clima culturale e contribuisce a consolidare il posto di *The Matrix* nella storia della cultura pop. La sua

[110] Anonimo, "Which movie(s) best represent hacker culture for you?" cit.;
[111] R. Ebert, *RogerEbert.com*, https://www.rogerebert.com/reviews/the-matrix-1999 (ultima consultazione: 30 agosto 2023); L. Bozzola, *ALLMOVIE*, https://www.allmovie.com/movie/the-matrix-vm19917885/review (ultima consultazione: 30 agosto 2023);

rappresentazione di un mondo distopico controllato dalle macchine ha influenzato innumerevoli altre opere di fantascienza e il suo stile visivo è stato imitato in molti altri film e programmi televisivi.

Anche il predecessore dei film sugli hacker, *Wargames*, non scampò alle critiche. Sebbene il film è stato molto apprezzato per la sua trama ricca di suspense e i suoi personaggi avvincenti, ma ha anche generato molte polemiche per la sua rappresentazione della cultura e delle tecniche hacker. Sia critici cinematografici sia i le prime comunità hacker del periodo hanno criticato l'accuratezza della rappresentazione in alcune tecniche di hacking[112]. Esempio principe è l'avvenimento che dà il via a tutta la trama del film, l'intrusione nel supercomputer militare "Joshua". Il giovane liceale Lightman, protagonista del film, viene mostrato capace di penetrare in una rete militare sicura con facilità, utilizzando solo una linea telefonica e un modem dial-up[113], il che è stato considerato altamente irrealistico da molti esperti dell'epoca.

Un altro esempio è il modo in cui il film descrive l'uso di una "backdoor" per accedere al supercomputer. Nel film, David riesce a trovare una "backdoor" segreta che gli permette di aggirare la sicurezza del computer e di accedere alla sua programmazione. In realtà all'inizio degli anni Ottanta, le backdoor erano molto meno comuni di quanto suggerisca il film, e la maggior parte degli hacker si affidava ad altre tecniche, come l'ingegneria sociale o lo sfruttamento delle vulnerabilità del software per accedere ai sistemi.

Tutte le critiche indirizzate a questi diversi titoli, non ne hanno fermato l'influenza, sia ricevuta sia trasmessa, visto che esse sono principalmente opere di finzione e di fatto non riportano la realtà al cento per cento. Nonostante questa consapevolezza, qualche eccezione c'è stata. L'approccio di qualche produzione cinematografica, in particolar modo nel ventunesimo secolo, era quello di avvicinarsi per quanto possibile alla effettiva realtà, trama e mezzi tecnici premettendo. Quello che tra le diverse opere hollywoodiane dell'ultimo ventennio del Novecento si è avvicinato di più a questo obbiettivo di produzione fu *Sneakers*.

Il film diretto da Phil A. Robinson si è sforzato di rappresentare gli hacker in modo più realistico e responsabile. Esso ritrae un gruppo di esperti di sicurezza che vengono ingaggiati da aziende dei settori più diversi per verificare la sicurezza dei propri sistemi informatici e non. Il film descrive

[112]K. Phipps, *ALLMOVIE*, https://www.allmovie.com/movie/wargames-vm1072653/review (ultima consultazione: 30 agosto 2023); R. Ebert, *RogerEbert.com*, https://www.rogerebert.com/reviews/wargames-1983 (ultima consultazione: 30 agosto 2023); Anonimo, "Which movie(s) best represent hacker culture for you?" cit.

[113] Il dial-up è una forma di accesso a Internet che utilizza le strutture della rete telefonica pubblica per stabilire una connessione a un provider (ISP) componendo un numero telefonico su una linea telefonica convenzionale. Le connessioni dial-up utilizzano i modem per decodificare i segnali audio in dati da inviare a un router o a un computer e per codificare i segnali di questi ultimi due dispositivi da inviare a un altro modem presso l'ISP. (Fonte: Cambridge Dictonary)

l'hacking come un processo complesso e difficile che richiede un alto grado di abilità e competenza. Gli hacker del film sono ritratti come individui altamente intelligenti, che cercano di ritagliarsi uno spazio nella società e allo stesso tempo aiutarla. *Sneakers* fece un ottimo lavoro, specialmente per quanto riguarda i personaggi, come in un certo modo farà poi anche *Hackers* qualche anno più tardi. Inoltre descrive quasi sempre con precisione gli strumenti e le tecniche utilizzate dagli hacker[114]. Ad esempio in una delle scene iniziali, i protagonisti riescono a penetrare in una banca seguendo un processo metodico e ragionato. Il gruppo riesce ad entrare in banca tramite l'allarme antincendio e toglie l'alimentazione all'allarme che era scattato mentre Whistler, collegatosi alla cornetta della banca, calma l'agitata guardia notturna. Tattiche e strumenti, come l'ingegneria sociale, vengono mostrati allo spettatore fin da subito con modalità simil-realistiche o quantomeno plausibili. Nonostante qualche lacuna su alcuni dettagli, molti hacker hanno lodato il film per la sua rappresentazione del cameratismo che può esistere tra gli hacker e per la sua enfasi sull'importanza del comportamento etico del gruppo di protagonisti.

In conclusione, le rappresentazioni degli hacker nel cinema hollywoodiano prima degli anni duemila sono state spesso criticate per la loro mancanza di realismo e la perpetuazione di miti. Nonostante queste critiche, è importante ricordarsi che tutte le opere cinematografiche prese in considerazione siano frutti di finzione e come tali non riflettono la realtà dell'hacking così com'è. Tuttavia, è anche importante riconoscere che questi film siano in grado di plasmare la percezione del pubblico sull'argomento e sulla comunità hacker, perciò è importante essere consapevoli di queste imprecisioni e alterazioni strutturate per il grande schermo ed assorbirle come tali. Quanto detto finora, mostra quindi come rappresentazioni equilibrate e accurate siano importanti per promuovere una comprensione più completa dell'hacking. Ritraendo gli hacker come individui complessi con motivazioni diverse, il cinema hollywoodiano ha la possibilità di contribuire ad abbattere gli stereotipi e a promuovere una comprensione più completa e sfumata dell'hacking. Delle rappresentazioni accurate possono anche contribuire a demistificare questa pratica e a renderla più accessibile a un pubblico più ampio.

[114] M. DiBella, *ALLMOVIE*, https://www.allmovie.com/movie/sneakers-vm450796/review (ultima consultazione: 30 agosto 2023);
R.Ebert, *RogerEbert.com*, https://www.rogerebert.com/reviews/sneakers-1992 ; (ultima consultazione: 30 agosto 2023);
Anonimo, "Which movie(s) best represent hacker culture for you?" cit.

2.2.3. *Dilemmi etici e ambiguità morale*

Ormai da decenni Hollywood è affascinata dagli hacker e dalle loro possibilità apparentemente infinite di creare scompiglio nella società. Tuttavia, da questo fascino deriva una pletora di dilemmi etici e ambiguità morali che vengono esplorati in film appartenenti a diversi generi cinematografici che trattano o includono questi soggetti e la loro pratica. Mentre alcuni vedono l'hacking come una forma innocua di esplorazione o di attivismo, altri lo considerano fonte di seri problemi etici e morali. È importante ricordare che l'hacking di per sé non è intrinsecamente immorale o morale. Le considerazioni etiche derivano dalle intenzioni, dai metodi e dalle conseguenze delle attività di hacking. Le principali questioni etiche sollevate dalla pratica dell'hacking sono una decina: l'accesso non autorizzato, l'invasione della privacy, il furto di proprietà intellettuale, il cybercrimine, l'interruzione dei servizi, la violazione della fiducia, il vigilantismo/hacktivismo, l'hacking etico, i danni collaterali e infine le relazioni internazionali e lo spionaggio. In seguito all'analisi dei film selezionati, si può notare le modalità nelle quali questi temi vennero raffigurati.

2.2.3.1. Accesso non autorizzato

L'hacking comporta a volte l'accesso a sistemi, reti o account senza autorizzazione. Ciò solleva problemi etici relativi al rispetto dei limiti, del consenso e dello stato di diritto. L'accesso non autorizzato ai computer è stato oggetto di dibattito etico per decenni. L'atto di accedere ai sistemi informatici senza autorizzazione ha implicazioni significative non solo per la sicurezza del sistema, ma anche per la privacy e i diritti delle persone coinvolte[115].

Uno dei primi film a portare alla luce questo dilemma etico è stato *Wargames*, che segue un giovane hacker che ottiene inavvertitamente l'accesso a un supercomputer militare, rischiando di scatenare una guerra nucleare tra Stati Uniti e Unione Sovietica. Nel corso del film, David riesce a introdursi senza autorizzazione in un terminale di un supercomputer militare e questa violazione provoca l'inizio di un conto alla rovescia per una possibile guerra nucleare, rischiando di causare danni significativi al mondo intero. Dalla discussione sulla scatola nera che il gruppo di Martin aveva in *Sneakers* alla storia di Dade, il protagonista di *Hackers*, passando per il piano disastroso dei tre impiegati di *Office Space*, la rappresentazione cinematografica mostra i potenziali danni che possono essere causati da un accesso non autorizzato.

[115] P. Taylor, *Hackers: Crime in the Digital Sublime*, cit., p. 14

2.2.3.2. Invasione della privacy

L'hacking spesso comporta l'accesso non autorizzato a informazioni personali, con conseguente violazione del diritto alla privacy. Ciò solleva preoccupazioni etiche sui confini dello spazio personale e sulla protezione dei dati riservati. Si tratta di informazioni personali, come dati finanziari o cartelle cliniche, ma anche di comunicazioni, come e-mail o messaggi di testo. Le violazioni della privacy possono avere gravi conseguenze sia per gli individui che per le organizzazioni.[116]

Tra i film presi in considerazione, vi sono due esempi chiave in *Hackers* e in *The Net*. Nel primo, il più giovane del gruppo di hacker si introduce nel sistema informatico di una grande società mineraria e naviga nei suoi dati per trovare qualcosa che provi la sua infiltrazione. Prende alcuni file dal cestino dei rifiuti, che saranno una parte essenziale della trama in seguito, e poi viene bloccato e arrestato per la sua intrusione. Questo esempio dimostra che anche azioni apparentemente innocue possono avere conseguenze negative, in quanto gli hacker mettono a rischio se stessi e gli altri. Mentre in *The Net*, le informazioni personali di Angela, tra cui la sua identità, i suoi conti bancari e le sue cartelle cliniche, vengono rubate da un gruppo di criminali informatici. Questa violazione della privacy non solo provoca danni economici, ma danneggia anche la reputazione e la vita personale della protagonista. Il film illustra quanto sia facile per gli hacker accedere e manipolare i dati sensibili, sottolineando la necessità di migliori misure di sicurezza e regolamenti e l'importanza di salvaguardare la propria privacy nell'era digitale.

2.2.3.3. Furto di proprietà intellettuale

L'hacking può comportare il furto o l'uso non autorizzato di materiale protetto da copyright, segreti commerciali o informazioni proprietarie. Il furto di proprietà intellettuale è un grave problema etico che è diventato sempre più diffuso nella società odierna. Il problema è rappresentato fin dal film *Tron* del 1982. Infatti, la causa scatenante dell'intera trama del film è costituita da alcuni software di videogiochi rubati creati dal protagonista, Flynn. Il suo vecchio socio e ora direttore della Encom, Ed

[116] H. Nissenbaum, "Hackers and the contested ontology of cyberspace.", cit., p. 198; P. Taylor, *Hackers: Crime in the Digital Sublime*, cit., pp. 62-63

Dillinger, ha rubato il suo lavoro e lo ha spacciato per suo fino a raggiungere la posizione attuale. Questo fatto porta il protagonista a infiltrarsi nel sistema Encom alla ricerca delle prove del furto.

2.2.3.4. Cybercrime

I crimini informatici sono diventati un evento sempre più comune nel nostro mondo interconnesso. Questi crimini, che implicano l'uso della tecnologia per commettere atti illegali, danneggiano individui, organizzazioni e la società nel suo complesso, sollevando preoccupazioni etiche sull'impatto sulle vittime e sulla necessità di un comportamento responsabile[117].

Le attività di hacking possono comportare varie forme di crimine informatico, come il furto di identità, le frodi o le truffe finanziarie. Quando gli individui si dedicano ai crimini informatici, possono accedere a informazioni o dati personali che non sono destinati al pubblico. L'antagonista principale di *The Net*, Jack Devlin, è un criminale informatico che usa le sue abilità di hacker per rubare denaro e manipolare le informazioni per raggiungere il suo scopo. Le azioni di Devlin dimostrano le implicazioni etiche dell'uso dell'hacking per scopi malevoli e l'importanza di distinguere tra hacking etico e non etico.

Un'altra implicazione etica dei crimini informatici è il potenziale danno finanziario. I criminali informatici spesso prendono di mira istituzioni finanziarie o individui per rubare denaro o informazioni finanziarie sensibili. A partire da *Superman III*, il personaggio di Richard Pryor, Gorman, utilizza una tecnica per sottrarre piccole somme di denaro dalle transazioni finanziarie della sua azienda, la stessa che Peter, Michael e Samir utilizzano contro la loro società di software in *Office Space*.

Oltre ai danni finanziari, i crimini informatici possono causare anche danni alla reputazione. Quando le informazioni sensibili vengono rubate o divulgate, possono danneggiare la reputazione di individui, organizzazioni o addirittura interi settori. Nella premessa del film *Hackers*, il protagonista Dade Murphy viene condannato da un tribunale per un crimine informatico da lui commesso. All'età di undici anni, ha infettato migliaia di sistemi informatici con un worm che ha scatenato il panico. La sua reputazione è stata macchiata e lui è stato sottoposto a libertà vigilata e non ha potuto possedere alcun oggetto tecnologico fino al suo diciottesimo compleanno.

[117] P. Taylor, *Hackers: Crime in the Digital Sublime*, cit., pp. 67-70

Infine, i crimini informatici possono anche avere implicazioni per la sicurezza nazionale. Quando vengono rubate o divulgate informazioni governative sensibili, possono compromettere la sicurezza nazionale e mettere a rischio vite umane. Ad esempio, in *Hackers*, l'antagonista principale, Belford, ha dirottato alcune petroliere e ha minacciato la sua stessa compagnia cercando di distogliere l'attenzione mentre il suo worm prendeva i soldi. Nel frattempo, *The Net* affronta anche le minacce globali alla sicurezza informatica. Gli hacker di *The Net* fanno parte di un'organizzazione internazionale che mira a controllare e manipolare le informazioni per il proprio tornaconto grazie a un programma apparentemente innocuo ma con una funzione segreta di backdoor ovunque venga installato. Il film mostra come la criminalità informatica non sia limitata a un singolo Paese o regione e possa avere conseguenze significative a livello globale.

2.2.3.5. Interruzione dei servizi

L'hacking può portare all'interruzione di servizi essenziali, come reti di comunicazione, sistemi di trasporto o strutture sanitarie. Le interruzioni di servizio causate dagli hacker possono avere un impatto significativo sulle persone e sulle organizzazioni che si affidano ai servizi colpiti. Le implicazioni etiche di queste interruzioni sono complesse e sfaccettate, poiché possono interrompere servizi critici, compromettere informazioni sensibili e causare perdite finanziarie significative.

L'implicazione etica delle interruzioni di servizio causate dagli hacker è il danno potenziale che può essere causato alle persone o ai gruppi che si affidano ai servizi colpiti. Quando gli hacker interrompono i servizi, possono influire negativamente su vari aspetti della vita delle persone, come la loro capacità di accedere a risorse vitali o di svolgere compiti necessari[118]. Un esempio di ciò è rappresentato da una scena simile in due film diversi, *Superman III* e *Hackers*. In questi film, c'è una scena in cui i semafori, rispettivamente di Metropolis e di New York, vengono manipolati dagli hacker e provocano caos e incidenti. Pur avendo contesti diversi, nel primo film è causata accidentalmente da un Gorman un po' ubriaco e nel secondo è causata dal gruppo di Dade per ritardare l'intervento della polizia, illustra i potenziali pericoli e le preoccupazioni etiche associate alle interruzioni del servizio causate dagli hacker.

Un'altra implicazione etica delle interruzioni di servizio causate dagli hacker è l'impatto sulla comunità in generale. Questo aspetto è ben rappresentato in Independence Day, quando gli invasori alieni lanciano un attacco informatico ai sistemi di comunicazione globali, causando panico e disagi

[118] M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 38

diffusi. Si introducono in vari sistemi, tra cui le reti di comunicazione militari e i sistemi di controllo del traffico aereo, e si infiltrano nei satelliti terrestri come ripetitori per trasmettere i segnali alle loro altre astronavi. Nonostante non si tratti di esseri umani, l'attacco informatico degli invasori alieni dimostra la potenziale interruzione delle infrastrutture critiche e i rischi significativi per la sicurezza pubblica se non sono sufficientemente protette. Ciò evidenzia il potenziale degli hacker di causare interruzioni significative dei servizi critici e l'impatto che tali interruzioni possono avere sulla comunità in generale.

2.2.3.6. Violazione della fiducia

La fiducia è un aspetto fondamentale dell'interazione umana ed è necessaria per qualsiasi forma di relazione. Nell'era digitale, la fiducia è ancora più importante, soprattutto quando si parla di sicurezza dei dati e di privacy. Tuttavia, è noto che gli hacker violano la fiducia accedendo illegalmente a informazioni sensibili e utilizzandole per i propri scopi[119].

L'atto stesso dell'hacking può essere considerato non etico, in quanto comporta l'accesso non autorizzato a sistemi e dati informatici. Quando gli hacker violano la fiducia, stanno essenzialmente rubando informazioni che appartengono a qualcun altro. Questo può avere gravi conseguenze, soprattutto quando si tratta di informazioni personali come numeri di previdenza sociale, dati di carte di credito e cartelle cliniche. Questo è esattamente ciò che viene rappresentato in *The Net*, un film in cui l'identità del protagonista viene rubata dagli hacker, evidenziando l'impatto devastante delle violazioni della fiducia nel mondo digitale.

Le implicazioni etiche della violazione della fiducia da parte degli hacker vanno oltre l'atto stesso dell'hacking. Quando le informazioni personali vengono rubate, possono essere utilizzate per scopi nefasti come il furto di identità e la frode finanziaria. Ciò può avere gravi conseguenze per le vittime, che possono subire perdite finanziarie, danni alla reputazione e stress emotivo, come mostra Sandra Bullock nel film *The Net*. Nel corso del film, il suo stato mentale peggiora a causa dello stress e dell'ansia che le azioni di Devlin e degli altri hacker le procurano. Il suo iniziale senso di fiducia nel mondo digitale si infrange quando diventa il bersaglio di un gruppo di hacker che manipola la sua vita e la sua identità.

[119] P. Taylor, *Hackers: Crime in the Digital Sublime*, cit., pp.104-106

L'atto di violazione della fiducia da parte degli hacker è un problema etico serio che può avere conseguenze di vasta portata. Sebbene la cultura popolare possa talvolta dipingere l'hacking come un'attività innocua o addirittura eroica, è importante ricordare che si tratta comunque di una forma di furto che può causare danni agli individui e alla società nel suo complesso. È importante che i singoli e le organizzazioni prendano provvedimenti per proteggere le proprie informazioni personali e impedire agli hacker di ottenere un accesso non autorizzato.

2.2.3.7. Vigilantismo e hacktivismo

Il vigilantismo e l'hacktivismo sono due forme controverse di attivismo che sono state oggetto di studio negli ultimi anni (G. Coleman 2013, T. Jordan & P. Taylor 2004, C. Kelty 2008, R. Bateson 2022, D. Cohen 2022). Sebbene entrambi condividano l'obiettivo di contrastare le ingiustizie percepite, i metodi utilizzati da questi due gruppi sono molto diversi. I vigilanti si affidano alla forza fisica e all'intimidazione per raggiungere i loro obiettivi, mentre gli hacktivisti utilizzano le loro competenze tecnologiche per ottenere l'accesso a informazioni sensibili e interrompere le operazioni dei loro obiettivi.

L'etica del vigilantismo e dell'hacktivismo è complessa e sfaccettata. Da un lato, entrambi possono essere visti come agenti che agiscono nell'interesse della giustizia, cercando di riparare a torti che il sistema legale non è riuscito a risolvere. Tuttavia, le loro azioni spesso comportano la violazione della legge e possono causare danni involontari a persone innocenti. Inoltre, la mancanza di responsabilità e di controllo in questi gruppi può portare ad abusi di potere e corruzione. Alcuni film hollywoodiani degli anni Ottanta e Novanta ritraggono gli hacker impegnati in attività che considerano al servizio di un bene superiore, come la denuncia della corruzione o la difesa della giustizia sociale. Ciò solleva questioni etiche sulla moralità del farsi giustizia da soli e sulle potenziali conseguenze di azioni non autorizzate. Inoltre, la rappresentazione degli hacker in questi film spesso confonde il confine tra vigilanti e hacktivisti[120].

Un chiaro esempio di ciò può essere visto nel film *The Matrix*, dove il personaggio Neo, insieme a un gruppo di hacker noti come la resistenza, combatte contro un sistema oppressivo che controlla l'umanità. In sostanza, si introducono nel sistema di Matrix, utilizzando le loro abilità per svelare la verità e liberare gli altri dalla prigione della realtà virtuale, diventando di fatto dei cyber-vigilanti.

[120] F. Mazzini, *Hackers*, *Storia e pratiche di una cultura*, cit., pp.152-154

Anche nel film *Hackers* si assiste a una rappresentazione simile dell'hacktivismo. Nonostante all'interno del film gli hacker siano ritratti come ribelli che spingono i confini di ciò che è possibile fare con la tecnologia, essi si vedono come pionieri che esplorano le nuove frontiere del cyberspazio. Questa visione è visibile solo per la prima parte del film, poiché dopo un punto principale della trama gli hacker si trasformano in qualcuno che può svolgere un ruolo importante nel mantenimento dell'ordine sociale e nella protezione dell'interesse pubblico, come gli hacktivisti dei tempi moderni. Nel film, il gruppo di hacker di Dade finisce per creare ed eseguire un piano per fermare Belfrod, un criminale informatico che minaccia di causare un grosso incidente ambientale solo per distogliere l'attenzione della sua grande azienda dal worm ruba soldi che ha inserito.

Sebbene questo film non etichetti esplicitamente le azioni degli hacker come hacktivismo, si può sostenere che esse incarnino elementi di questo concetto. L'etica del vigilantismo e dell'hacktivismo è stata oggetto di molti dibattiti in ambito accademico. Se da un lato questi gruppi possono essere visti come se agissero nell'interesse della giustizia, dall'altro le loro azioni spesso comportano la violazione della legge e possono causare danni involontari a persone innocenti. La mancanza di responsabilità e di controllo in questi gruppi può anche portare ad abusi di potere e corruzione. Poiché la società continua a confrontarsi con questioni di giustizia e responsabilità, sarà importante considerare attentamente le implicazioni di queste forme controverse di attivismo.

2.2.3.8. Hacking etico

L'hacking etico è diventato un approccio popolare per le aziende per identificare le vulnerabilità nei loro sistemi informatici. Tuttavia, solleva preoccupazioni di carattere etico, poiché spesso il processo implica l'intrusione nei sistemi informatici, il che può comportare implicazioni legali e morali. Il termine "etico" nell'hacking etico si riferisce all'idea di utilizzare le abilità di hacking per scopi etici. L'obiettivo principale dell'hacking etico è quello di testare la sicurezza dei sistemi informatici e di identificare le vulnerabilità per prevenire attacchi dannosi. Tuttavia, l'hacking etico solleva anche preoccupazioni di carattere etico, in quanto comporta l'intrusione nei sistemi informatici, che è un atto illegale. Gli hacker etici devono essere consapevoli delle implicazioni legali e morali delle loro azioni. L'hacking etico deve essere effettuato con il consenso del proprietario del sistema informatico. Se fatto senza autorizzazione, può portare a ripercussioni legali e morali[121].

[121] H. Nissenbaum, "Hackers and the contested ontology of cyberspace.", cit., pp. 197-198; P. Taylor, *Hackers: Crime in the Digital Sublime*, cit., pp. 26-28; S. Levy, *Hackers: Heroes of the Computer Revolution* (1984), cit. pp. 26-34

Esiste un dibattito sull'hacking etico, in cui persone con competenze tecniche avanzate vengono impiegate per identificare le vulnerabilità nei sistemi e nelle reti per aiutare le organizzazioni a migliorare la loro sicurezza. Ciò solleva questioni etiche sui limiti dell'hacking e sulle intenzioni alla base di queste attività. Gli hacker etici collaborano con un'azienda o un'organizzazione per migliorarne la sicurezza, prevenire gli attacchi informatici e proteggere i dati sensibili.

Un esempio di questa materia è rappresentato in due film hollywoodiani degli anni Novanta come *Sneakers* e *The Net*. Entrambi i protagonisti, Angela Bennet e Martin con la sua squadra, sono hacker etici che espongono le falle di sicurezza nei software e le segnalano al proprio datore di lavoro. Mentre Angela fa capo a una piccola società che fornisce questo servizio, Martin e la sua squadra sono freelance, ovvero lavorano su richiesta di grandi aziende, come viene mostrato all'inizio del film. L'hacking etico è un argomento controverso che solleva preoccupazioni etiche. Gli hacker etici devono essere consapevoli delle implicazioni legali e morali delle loro azioni. Come illustrato dagli esempi dei film degli anni Ottanta e Novanta, l'impatto dell'hacking sulla società può essere grave. L'hacking etico deve essere effettuato con il consenso del proprietario del sistema informatico. È importante assicurarsi che l'hacking etico sia utilizzato per scopi etici e non per guadagno personale.

2.2.3.9. Danni collaterali

Gli attacchi di hacking possono inavvertitamente danneggiare parti innocenti che non sono i bersagli previsti. Ad esempio, quando un hacker prende di mira un'organizzazione specifica, l'attacco può colpire clienti, dipendenti o altre parti interessate. Ciò solleva preoccupazioni etiche riguardo alle conseguenze non intenzionali e al potenziale danno causato a chi non è direttamente coinvolto. Quando individui o organizzazioni si dedicano all'hacking, si assumono rischi significativi. Ad esempio, un hacker può accidentalmente causare danni a persone o organizzazioni, ad esempio interrompendo infrastrutture critiche o rubando informazioni sensibili. Inoltre, l'hacking può portare a conseguenze legali, come multe o detenzione.

L'hacking è un problema pervasivo che ha colpito individui, organizzazioni e governi di tutto il mondo. Mentre le vittime principali dell'hacking sono gli obiettivi diretti degli attacchi, i danni collaterali dell'hacking possono essere sostanziali e spesso trascurati. Per danni collaterali si intendono le conseguenze non volute e spesso imprevedibili di una determinata azione. Nel caso dell'hacking, i danni collaterali possono assumere diverse forme. Ad esempio, un hacker che viola i

dati di un'azienda può causare perdite finanziarie, danni alla reputazione e perdita di fiducia da parte dei clienti. Allo stesso modo, un hacker che prende di mira un'agenzia governativa può compromettere la sicurezza nazionale, interrompere servizi critici e mettere in pericolo vite umane.

La rappresentazione dei danni collaterali dell'hacking nei film hollywoodiani degli anni Ottanta e Novanta può essere utile per facilitare la loro comprensione. Questi film, anche se di fantasia, hanno spesso rappresentato i dilemmi etici e le conseguenze indesiderate dell'hacking. Perciò l'hacking può portare a danni significativi per gli individui o per la società, come si vede in *Wargames*. L'accesso non autorizzato di David al supercomputer militare difatti ne illustra il potenziale danno. L'avvio di un conto alla rovescia per la guerra nucleare, come risultato dell'hacking di David, evidenzia il danno significativo che l'hacking può causare alla società. L'hacking di David illustra anche le conseguenze sociali/penali che possono derivare dall'hacking. L'accesso non autorizzato di David al supercomputer militare compromette la sua posizione da cittadino a tal punto da essere considerato una spia sovietica e perciò una minaccia per la sicurezza nazionale. *Wargames* offre quindi una rappresentazione avvincente delle implicazioni etiche e morali dell'hacking. Il film mette in evidenza i potenziali danni causati dall'hacking e la violazione della fiducia che può derivare dall'accesso non autorizzato ai sistemi informatici.

2.2.3.10. Relazioni internazionali e spionaggio

Nell'ambito delle relazioni internazionali, lo spionaggio è stato a lungo uno strumento utilizzato dalle nazioni per ottenere informazioni e un vantaggio nei negoziati. Tuttavia, con l'avvento della tecnologia e di Internet, il ruolo degli hacker nello spionaggio è diventato sempre più diffuso[122]. Le implicazioni etiche di questo fenomeno non possono essere ignorate. L'hacking può essere utilizzato quindi come strumento di spionaggio informatico, mirando a informazioni sensibili, segreti commerciali o intelligence governativa. Ciò solleva preoccupazioni etiche circa la violazione della sovranità delle nazioni, del diritto internazionale e del potenziale di escalation dei conflitti.

Gli hacker che si dedicano allo spionaggio sono spesso ingaggiati da governi o aziende per sottrarre informazioni sensibili ad altre nazioni o aziende. Questo tipo di spionaggio può avere gravi conseguenze, tra cui danni economici e compromissione della sicurezza nazionale. Inoltre, l'uso degli

[122] Christos Douligeris, Omid Raghimi, Marco Barros Lourenço, Louis Marinos, *ENISA Threat Landscape 2020: Cyber espionage*, ENISA, 2020, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-cyberespionage (ultima consultazione: 30 agosto 2023)

hacker nello spionaggio solleva interrogativi sull'etica dell'utilizzo di individui che potrebbero non avere lo stesso livello di responsabilità e supervisione delle agenzie di intelligence tradizionali. Se da un lato questi hacker possono essere abili nel loro mestiere, dall'altro possono essere più inclini a mettere in atto comportamenti non etici o ad agire in modo scorretto senza un'adeguata supervisione[123].

I film hollywoodiani degli anni Ottanta e Novanta ritraevano spesso gli hacker come individui dotati di straordinarie capacità tecniche, in grado di violare sistemi altamente sicuri per portare a termine le loro missioni di spionaggio. In questo modo, l'industria cinematografica ha previsto una forma di hacking molto diffusa dagli anni Duemila fino a oggi, l'hacking di Stato. Le successive trasposizioni di questo tipo di hacking sono state rese più complesse e stratificate man mano che la comprensione dell'hacking cresceva. Il film del periodo di nostro interesse che forse meglio rappresenta questo aspetto è *Mission Impossible*. Nel corso del film, viene mostrato che la figura dell'hacker è essenziale per portare a termine questo tipo di operazioni. Nel film ci sono due personaggi che sono hacker, ma il più importante dei due è Luther, interpretato da Ving Rhames, un abile hacker che assiste il protagonista principale nell'infiltrazione di sistemi sicuri per estrarre informazioni cruciali. Con il suo personaggio, il film assume un tono diverso rispetto ad altri film dell'epoca. Da un certo punto di vista è molto simile a un hacker etico, in quanto è quello che rimane fedele a Ethan e non ha secondi fini con i documenti che aiuta a recuperare. È calmo e logico e il motivo iniziale che lo spinge ad aiutare Ethan è quello di essere reintegrato dalla CIA. Sebbene abbia una posizione più neutrale rispetto ad altre rappresentazioni di hacker, il film evidenzia comunque i potenziali pericoli e le implicazioni etiche dell'hacking a fini di spionaggio e per le relazioni internazionali. Sebbene questi individui possano essere abili nel loro mestiere, le loro azioni possono avere gravi conseguenze e la mancanza di supervisione e responsabilità solleva interrogativi sull'etica del loro utilizzo.

Queste rappresentazioni degli hacker nel cinema hanno avuto un impatto significativo sulla comprensione e sulla percezione degli hacker da parte del pubblico. Mentre alcuni film hanno ritratto gli hacker come eroi che combattono contro sistemi corrotti, altri li hanno mostrati come soggetti che rappresentano una minaccia per la società. Questo ha portato a un generale senso di sfiducia nei confronti degli hacker, che spesso vengono visti come individui che non hanno nulla di buono da fare. La rappresentazione degli hacker nei film Hollywood prima degli anni Duemila ha sollevato una serie

[123] Dmitry Smilyanets, "'I Was Running Two Parallel Lives': An Ex-Secret Service Agent Opens Up About Going Undercover To Catch Cybercriminals", *The Record. Recorded Future News*, https://therecord.media/i-was-running-two-parallel-lives-an-ex-secret-service-agent-opens-up-about-going-undercover-to-catch-cybercriminals (ultima consultazione: 30 agosto 2023); C. Douligeris, O, Raghimi, M. B. Lourenço, L. Marinos, *ENISA Threat Landscape 2020: Cyber espionage*, cit.

di dilemmi etici e ha esplorato l'ambiguità morale dell'hacking. L'hacking è un problema etico e morale che ha conseguenze significative per gli individui, le organizzazioni e la società nel suo complesso.

2.2.4. *Influenze di eventi reali sulla produzione hollywoodiana*

Hollywood ha alle spalle una lunga storia di ispirazione da eventi reali per riuscire a produrre film avvincenti. Difatti anche questa categoria è stata particolarmente influenzata, con modalità variegate, da fatti realmente accaduti. Dall'ascesa dell'hacking negli anni Ottanta a oggi, una notevole quantità di casi è stata portata alla luce dalla stampa e da altri media, fornendo così un discreto numero di punti di spunto e di ispirazione per i produttori hollywoodiani e, in tempi più recenti televisivi.

Uno dei motivi principali per cui solitamente Hollywood sceglie di realizzare un film su un particolare evento è l'interesse del pubblico per l'argomento. Quando si verifica un evento di hacking significativo, esso viene spesso portato all'attenzione del pubblico da telegiornali o testate di stampa. I produttori di Hollywood vedono questo interesse e lo sfruttano creando un film sull'evento. Molti film sugli hacker sono stati ispirati da eventi reali e alcuni di essi hanno controparti cinematografiche per molti aspetti simili. Un chiaro esempio è il film *Wargames*, uscito nel 1983. Il film si ispira a un episodio reale in cui un giovane hacker di nome David Scott Lewis, ora un esperto di cybersecurity, si introdusse nel sistema informatico del NORAD. I due sceneggiatori del film si misero in contatto con Lewis e discussero con lui riguardo alla trama del film e più in generale alla pratica dell'hacking[124].

La produzione di *Wargames* è stata fortemente influenzata da altri eventi reali legati agli hacker che si stavano verificando in quel periodo. All'inizio degli anni Ottanta, l'hacking informatico era un fenomeno relativamente nuovo e poche persone comprendevano i potenziali pericoli dell'accesso non autorizzato ai sistemi informatici. Uno degli eventi chiave che influenzarono la produzione di *Wargames* fu l'arresto di alcuni hacker adolescenti nel 1983. Questi hacker, il gruppo 414, avevano ottenuto l'accesso non autorizzato a diversi sistemi informatici di alto profilo, tra cui quelli appartenenti al Los Alamos National Laboratory e allo Sloan-Kettering Cancer Center[125]. L'arresto dei 414 ha fatto notizia in tutto il mondo ed è diventato un simbolo della crescente minaccia

[124]D. Takahashi, "A Q&A that is 25 years late: David Scott Lewis, the mystery hacker who inspired the film "War Games"", *VentureBeat*, https://venturebeat.com/social/a-qa-that-is-25-years-late-david-scott-lewis-the-inspiration-behind-the-film-war-games/ (ultima consultazione: 30 agosto 2023)
M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", cit., p. 42; F. Mazzini, *Hackers, Storia e pratiche di una cultura*, cit., p. 78

dell'hacking informatico. L'incidente evidenziò anche la necessità di rafforzare le misure di sicurezza informatica e portò alla creazione del Computer Fraud and Abuse Act, tuttora in vigore. I produttori di *Wargames* si ispirarono ai membri del gruppo 414 e a Lewis incorporandone nel film certi dettagli e loro caratteristiche nel loro protagonista, David[126]. Nel complesso, l'influenza degli eventi reali legati agli hacker sulla produzione di *Wargames* non può di certo essere sottovalutata, considerata soprattutto la situazione di crescita del fenomeno dell'hacking in cui gli Stati Uniti si trovavano al momento della sua uscita nelle sale. Il film è stato un'esplorazione innovativa dei potenziali pericoli della tecnologia informatica e ha contribuito a sensibilizzare l'opinione pubblica sulla necessità di rafforzare le misure di sicurezza informatica.

Nel corso degli anni successivi, molti altri film hanno seguito le orme di *Wargames*, ispirandosi a episodi di hacking realmente accaduti. Questi film e programmi televisivi hanno catturato l'immaginazione del pubblico con storie di hacker che combattono contro aziende, governi o altre entità potenti. Sebbene la prassi, essendo opere di finzione, fosse l'esagerazione e la resa romantica della trama, questi film riflettono comunque la crescente importanza della sicurezza informatica nel mondo moderno.

La produzione di *Sneakers* ha coinciso con un periodo di maggiore sensibilizzazione del pubblico nei confronti dell'hacking e della sicurezza informatica. All'inizio degli anni Novanta, episodi di hacking di alto profilo, come il worm Morris del 1988 e le incursioni dell'Operazione Sundevil cominciate l'anno successivo, avevano portato la questione della sicurezza informatica all'attenzione della coscienza pubblica. Questa maggiore consapevolezza della sicurezza informatica ha avuto un impatto significativo sulla produzione di *Sneakers*. nella rappresentazione di tattiche di ingegneria sociale, come il *dumpster diving*. Il team di produzione si è impegnato per garantire che la sicurezza fisica del film fosse realistica. Il momento culminante del film si svolge in una struttura protetta da una serie di misure di sicurezza fisica, tra cui scanner biometrici e guardie armate. Per garantire che la rappresentazione di queste misure di sicurezza fosse accurata, il team di produzione si è consultato con esperti di sicurezza reali e ha condotto ricerche approfondite. L'impatto degli eventi reali legati agli hacker sulla produzione di *Sneakers* è stato significativo. L'attenzione ai dettagli e la rappresentazione realistica dell'hacking e delle misure di sicurezza fisica hanno fatto sì che il film si distinguesse dagli altri heist movie dell'epoca. Il successo del film ha inoltre contribuito a rendere più popolare la rappresentazione dell'hacking nella cultura popolare, aprendo la strada ad altri film e programmi televisivi che avrebbero esplorato il mondo dell'hacking in modo più dettagliato.

[126] D. Takahashi, "A Q&A that is 25 years late: David Scott Lewis, the mystery hacker who inspired the film "War Games"", cit.; F. Mazzini, *Hackers, Storia e pratiche di una cultura*, cit., p. 78

Il film americano del 1995 *Hackers*, diretto da Iain Softley, è diventato un classico di culto nella comunità degli hacker e della sicurezza informatica. Il ritratto che il film fa della sottocultura hacker è stato oggetto sia di elogi che di critiche. Tuttavia, è innegabile che la produzione del film sia stata influenzata da eventi di hacking realmente accaduti nei primi anni Novanta. Uno degli eventi più significativi che hanno influenzato la produzione di *Hackers*, molto probabilmente, è stato l'arresto e l'incriminazione di Kevin Mitnick, un noto hacker che ha avuto accesso non autorizzato ai sistemi informatici e ha rubato informazioni sensibili. L'arresto e il processo di Mitnick sono stati molto pubblicizzati e la sua storia è diventata un simbolo della repressione del governo nei confronti degli hacker. Il protagonista del film, Dade Murphy, interpretato da Jonny Lee Miller, condivide molte analogie con Mitnick. L'analogia più ovvia dei due è il fatto di essere un hacker esperto con un passato travagliato, di essere perseguito dalle forze dell'ordine e di diventare un eroe popolare all'interno della comunità degli hacker. Un altro evento reale che ha influenzato la produzione di *Hackers* è stata la nascita di Internet e la diffusione dei personal computer. Il film è ambientato a New York e ritrae un gruppo di giovani hacker che usano i loro computer e Internet per penetrare nei sistemi aziendali e governativi. Il film cattura l'eccitazione e il potenziale di Internet e dei personal computer, che stavano rapidamente diventando onnipresenti nei primi anni Novanta. Inoltre, il film riflette anche le paure e le ansie che circondano l'ascesa di Internet e il potenziale della criminalità informatica. L'antagonista del film, Eugene Belford, interpretato da Fisher Stevens, rappresenta il "lato oscuro" dell'hacking e della criminalità informatica. Belford è un ex hacker che si è dato al crimine informatico per guadagno personale. Il suo personaggio incarna la paura delle aziende e dei governi che gli hacker possano usare le loro capacità per scopi nefasti. La rappresentazione del film della sottocultura hacker è un riflesso dell'eccitazione e del potenziale di Internet e dei personal computer, nonché delle paure e delle ansie legate all'aumento della criminalità informatica.

Gli eventi della vita reale hanno perciò avuto un'influenza significativa sulla produzione di film sugli hacker e sulla loro cultura. I produttori di Hollywood sfruttarono l'interesse del pubblico per questi eventi al fine di creare opere cinematografiche avvincenti. Sebbene molti di questi film siano basati su eventi reali, spesso si prendono delle libertà creative per rendere la storia più avvincente. Di conseguenza, l'accuratezza della rappresentazione degli eventi reali può variare notevolmente, passando da una rappresentazione molto simile a una per lo più romanzata.

CONCLUSIONE

Questo studio ha cercato di impostare un quadro completo e preciso sulla rappresentazione degli hacker nel cinema hollywoodiano precedente al Duemila (1980-1999) e le sue implicazioni. A tal fine è stata condotta un'analisi su vari film di questo periodo specifico, osservando le modalità con cui questi propongano la figura e la cultura dell'hacker.

La rappresentazione degli hacker nel cinema americano tra gli anni Ottanta e Duemila è stata un affascinante oggetto di analisi. Il caso di studio ha mostrato una evidente evoluzione di queste raffigurazioni nel corso degli anni e ha reso evidente l'aumento graduale della comprensione del mondo hacker da parte di Hollywood. La rappresentazione di questi individui è cambiata significativamente nel corso degli anni, passando dall'iniziale rappresentazione di eroi e protagonisti a pieno titolo a quella di criminali senza mezze misure fino a raggiungere uno stato di equilibrio tra i due. Questo cambiamento può essere attribuito alla crescente consapevolezza dei problemi di sicurezza informatica e alla necessità di professionisti qualificati in grado di proteggere dalle minacce informatiche. La rappresentazione degli hacker nei film è stata un importante riflesso del cambiamento dell'atteggiamento della società nei confronti della tecnologia e di Internet. Da *Wargames* a *The Matrix*, questi film hanno contribuito a fornire la percezione hollywoodiana di cosa sia l'hacking e di come siano gli hacker.

Tuttavia, è importante tenere presente che questa ricerca si è concentrata principalmente sulle raffigurazioni hollywoodiane degli hacker antecedenti al nuovo secolo. Una volta considerate anche sia quelle presenti in altre rappresentazioni cinematografiche esterne a quelle statunitensi dello stesso periodo storico sia quelle degli ultimi vent'anni, i risultati qui dimostrati possono variare. Per questa motivazione, nessuna dichiarazione definitiva può essere fatta riguardo all'interezza dei dipinti cinematografici degli hacker.

Una raccomandazione per ulteriori ricerche future potrebbe essere quella di realizzare uno studio simile concentrandosi appunto sulle raffigurazioni di hacker in opere cinematografiche non statunitensi e in titoli hollywoodiani post Duemila, interessandosi nel dettaglio su questi elementi specifici.

BIBLIOGRAFIA/SITOGRAFIA/FILMOGRAFIA

BIBLOGRAFIA

Alleyne Brian, *Geek and Hacker Stories. Code, Culture and Storytelling from the Technosphere*, Palgrave Pivot, London 2019

Andersen Joceline, The Body of the Machine: Computer Interfaces in American Popular Cinema since 1982, *Projections*, vol. *5*, n. 2, pp. 75-95

Bateson Regina, "The Politics of Vigilantism", *Comparative Political Studies*, vol. 54, n.6 (2021), pp. 923-955;

Ceruzzi Paolo, *A History of Modern Computing*, The MIT Press, Cambridge 2003;

Cohen Dara, Jung Danielle F., Weintraub Michael, "Collective Vigilantism in Global Comparative Perspective", *Comparative Politics*, Vol. 55, n. 2 (2023), pp. 263-261;

Coleman Gabriella, *Coding Freedom: The Ethics and Aesthetics of Hacking*, Princeton University Press, Princeton 2013;

Coleman Gabriella, A. Golub, "Hacker Practice. Moral Genres and the Cultural Articulation of Liberalism", *Anthropological Theory*, vol. 8, n. 3 (2008);

Coleman Gabriella, "The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld", *Anthropological Quarterly*, vol. 83, n. 1 (2010);

Coleman Gabriella, *The Political Agnosticism of Free and Open Source Software and the Inadvertent Politics of Contrast*, in «Anthropological Quarterly», vol. 77, n. 3 (2004);

Elsaesser Thomas, Buckland Warren, tr. D. Pedrazzani, *Teoria e analisi del film americano contemporaneo*, Bietti, Milano 2010;

Himanen Pekka, Castells Manuel, Torvalds Linus, *The Hacker Ethic and the Spirit of the Information Age*, Random House, New York 2001;

Jordan Tim, Taylor Paul, "A Sociology of Hackers", *The Sociological Review*, vol. 46, n. 4 (1998);

Jordan Tim, "A Genealogy of Hacking", *Convergence: The International Journal of Research into New Media Technologies*, vol. 23, n. 5 (2017);

Jordan Tim, Taylor Paul, *Hacktivism and Cyberwars: Rebels with a Cause?*, Routledge, Londra 2004;

Jecan Vlad, *Hacking Hollywood: discussing hackers' reactions to three popular films*, Journal of Media Research, vol. 2, n.10 (2011), pp. 95-114;

Kelty Christofer M., *Two Bits: The Cultural Significance of Free Software*, Duke University Press, Durham 2008;

Kouttis Simon, *Improving security knowledge, skills and safety*, Computer Fraud & Security, Volume 2016, n. 4, 2016, Pages 12-14;

Levy Steven, *Hackers: Heroes of the Computer Revolution* (1984), O'Reilly Media, Sebastopol 2010;

Maguire Joseph, English Rosanne, Draper Steve, "Engaging Students in Threat Thinking with the Cyber Security Cinema", CEP '23: Proceedings of 7th Conference on Computing Education Practice, Association for Computing Machinery, New York 2023, pp. 13-16;

Mazzini Federico*, Hackers, Storia e pratiche di una cultura*, Editori Laterza, Bari 2023,

McKenzie Wark, "Hackers" *Theory, Culture & Society*, vol. 23, no. 2-3, 2006, pp. 320–22;

Meyer Gordon R., *The Social Organization of the Computer Underground* (1989), Northern Illinois University, DeKalb 2009;

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

Nissenbaum Helen, "Hackers and the contested ontology of cyberspace", *New Media & Society*, vol. 6, n. 2 (2004), pp. 195 – 217;

Morgan Steven C., Morgan Connor S., *Hackers' movie guide 2022-2023 edition, the complete list of hacker & cybersecurity movies*, Cybersecurity Ventures, Northport 2022;

Rondolino Gianni, Tomasi Dario, *Manuale di Storia del Cinema*, UTET Università, Milano 2014;

Sangiuliano G., *Reagan. Il Presidente che cambiò la politica americana*, Mondadori, Milano 2021

Stallman Robert, "Realizable Fantasies: The GNU Manifesto", *Dr. Dobb's Journal*, vol. 10, n. 3 (1985);

Stańczyk Marta, “Unseen war? Hackers, tactical media, and their depiction in Hollywood cinema”, *Transmissions: the journal of film and media studies*, Jagiellonian University, vol. 2, n. 1 (2017), pp. 62-77;

Suiter Tad, “Why ‘Hacking’?”, in Id., *Hacking the Academy: New Approaches to Scholarship and Teaching from Digital Humanities*, University of Michigan Press, Ann Arbor 2013, pp. 6–10;

Taylor Paul, *Hackers: Crime in the Digital Sublime*, Routledge, London 1999;

Thomas Douglas, *Hacker Culture*, University of Minnesota Press, Minneapolis 2002;

Turgeman-Goldschmidt Orly, “Hacker's accounts: hacking as a social entertainment.” *Social Science Computer Review*, vol. 23, n.1 (2005), pp. 8-23;

SITOGRAFIA

Allison Peter R., “Too many secrets: What can today’s cyber teams learn from a 30-year-old film?”, *ComputerWeekly.com*, https://www.computerweekly.com/feature/Too-many-secrets-What-can-todays-cybers-teams-learn-from-a-30-year-old-film (ultima consultazione: 2023);

Armstrong Derek, “Superman III (1983)”, *ALLMOVIE*, https://www.allmovie.com/movie/superman-iii-vm1070439/review (ultima consultazione: 30 agosto 2023);

Armstrong Derek, “Revenge of the nerds (1984)”, *ALLMOVIE*, https://www.allmovie.com/movie/revenge-of-the-nerds-vm447213/review (ultima consultazione: 30 agosto 2023);

Armstrong Derek, “Tron (1982)”, *ALLMOVIE,* https://www.allmovie.com/movie/tron-vm424775/review (ultima consultazione: 30 agosto 2023);

Anonimo, “The Difference Between Cybersecurity in Hollywood and Reality”, *Maryville University*, https://online.maryville.edu/blog/the-difference-between-cyber-security-in-hollywood-and-reality/ (ultima consultazione: 30 agosto 2023);

Anonimo, “What is Cyber Espionage?”, *vmware*, https://www.vmware.com/topics/glossary/content/cyber-espionage.html?resource=cat-95229697#cat-95229697 (ultima consultazione: 30 agosto 2023);

Broccolini Alessandra, “Cultura Popolare”, *Treccani*, https://www.treccani.it/enciclopedia/cultura-popolare_%28Enciclopedia-Italiana%29/ (ultima consultazione: 30 agosto 2023);

Britt Ryan, “In the ‘80s, Too Many Movies Tried to Fuse Sci-Fi With Rom-Com. This One Worked.”, *INVERSE*, https://www.inverse.com/culture/wargames-40-years-sci-fi-hacker-ai (ultima consultazione: 2023);

Bozzola Lucia, “Enemy of the State (1998)”, *ALLMOVIE*, https://www.allmovie.com/movie/enemy-of-the-state-vm1093298/review (ultima consultazione: 30 agosto 2023);

Bozzola Lucia, “The Matrix (1999)”, *ALLMOVIE*, https://www.allmovie.com/movie/the-matrix-vm19917885/review (ultima consultazione: 30 agosto 2023);

Bushi Ruth, “WARGAMES (1983): WINNING AT DEATH AND DESTRUCTION”, *THE HAUGHTY CULTURIST*, https://www.thehaughtyculturist.com/films/wargames-1983-themes-explained/ (ultima consultazione: 2023);

Cheryl Eddy, “The Net Is Somehow Both Outdated and Prescient”, *GIZMODO*, https://gizmodo.com/the-net-is-somehow-both-outdated-and-prescient-1845706698 (ultima consultazione: 30 agosto 2023);

Christensen Ward, “Collection of Memories of writing and running the first BBS”, *BBSDocumentary.com*, http://www.bbsdocumentary.com/software/AAA/AAA/CBBS/memories.txt (ultima consultazione: 30 agosto 2023);

Christensen Ward, Suess Randy, “Hobbyist Computerized Bulletin Board System”, *Byte*, Vol. 3, n. 11 (1978), pp. 150–157, http://vintagecomputer.net/cisc367/byte%20nov%201978%20computerized%20BBS%20-%20ward%20christensen.pdf (ultima consultazione: 30 agosto 2023);

Clark Jason, “Independence Day (1996)”, *ALLMOVIE*, https://www.allmovie.com/movie/independence-day-vm422588/review (ultima consultazione: 30 agosto 2023);

Collar Cammila, “Hackers (1995)”, *ALLMOVIE*, https://www.allmovie.com/movie/hackers-vm428814/review (ultima consultazione: 30 agosto 2023);

Costello Michael, “The Net (1995)”, *ALLMOVIE*, https://www.allmovie.com/movie/the-net-vm1022080330/review (ultima consultazione: 30 agosto 2023);

DiBella Mike, “Sneakers (1992)”, *ALLMOVIE*, https://www.allmovie.com/movie/sneakers-vm450796/review (ultima consultazione: 30 agosto 2023);

Dillard Brian J., “Johnny Mnemonic (1995)”, *ALLMOVIE*, https://www.allmovie.com/movie/johnny-mnemonic-vm427795/review (ultima consultazione: 30 agosto 2023);

Douligeris Christos, Omid Raghimi, Marco Barros Lourenço, Louis Marinos, *ENISA Threat Landscape 2020: Cyber espionage*, ENISA, 2020, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-cyberespionage (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Electric Dreams”, *RogerEbert.com*, https://www.rogerebert.com/reviews/electric-dreams-1984 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Enemy of the State”, *RogerEbert.com*, https://www.rogerebert.com/reviews/enemy-of-the-state-1998 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Hackers”, *RogerEbert.com*, https://www.rogerebert.com/reviews/hackers-1995 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Independence Day”, *RogerEbert.com*, https://www.rogerebert.com/reviews/independence-day-1996 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Johnny Mnemonic”, *RogerEbert.com*, https://www.rogerebert.com/reviews/johnny-mnemonic-1995 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Mission Impossible”, *RogerEbert.com*, https://www.rogerebert.com/reviews/mission-impossible-1996 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Office Space”, *RogerEbert.com*, https://www.rogerebert.com/reviews/office-space-1999 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Sneakers”, *RogerEbert.com*, https://www.rogerebert.com/reviews/sneakers-1992 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Superman III”, *RogerEbert.com*, https://www.rogerebert.com/reviews/superman-iii-1983 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “The Net”, *RogerEbert.com*, https://www.rogerebert.com/reviews/the-net-1995 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “The Matrix”, *RogerEbert.com*, https://www.rogerebert.com/reviews/the-matrix-1999 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “Tron”, *RogerEbert.com*, https://www.rogerebert.com/reviews/tron-1982 (ultima consultazione: 30 agosto 2023);

Ebert Roger, “WarGames”, *RogerEbert.com*, https://www.rogerebert.com/reviews/wargames-1983 (ultima consultazione: 30 agosto 2023);

Flick Catherine, “What Hollywood gets right and wrong about hacking”, *THE CONVERSATION*, https://theconversation.com/what-hollywood-gets-right-and-wrong-about-hacking-100126 (ultima consultazione: 30 agosto 2023);

Goldberg Reid, “This '80s Thriller Was Chilling Enough to Affect National Security Policy”, *COLLIDER*, https://collider.com/1980s-thriller-national-security-wargames/ (ultima consultazione: 2023);

Holt Thomas J., “Hacks, cracks, and crime: an examination of the subculture and social organization of computer hackers”, *UMSL Libraries*, https://irl.umsl.edu/dissertation/616?utm_source=irl.umsl.edu%2Fdissertation%2F616&utm_medium=PDF&utm_campaign=PDFCoverPages (ultima consultazione: 30 agosto 2023);

Kabay Michel E., “A Brief History of Computer Crime: An Introduction for Students”, *M. E. Kabay, PhD*, http://www.mekabay.com/overviews/history.pdf (ultima consultazione: 30 agosto 2023);

Medendorp Liz, "'HACKERS' PROVED TO BE AHEAD OF ITS TIME", *popMATTERS*, https://www.popmatters.com/196150-hackers-2495499373.html (ultima consultazione: 30 agosto 2023);

Miller Skyler, "Office Space (1999)", *ALLMOVIE*, https://www.allmovie.com/movie/office-space-vm1106650/review (ultima consultazione: 30 agosto 2023);

Peters Beau, "Fact vs. Fiction: Film Industry's Portrayal of Cybersecurity", *Security Boulevard*, https://securityboulevard.com/2020/12/fact-vs-fiction-film-industrys-portrayal-of-cybersecurity/ (ultima consultazione: 30 agosto 2023);

Phipps Keith, "Mission Impossible (1996)", *ALLMOVIE*, https://www.allmovie.com/movie/mission-impossible-vm422659/review (ultima consultazione: 30 agosto 2023);

Phipps Keith, "WarGames (1983)", *ALLMOVIE*, https://www.allmovie.com/movie/wargames-vm1072653/review (ultima consultazione: 30 agosto 2023);

Sims Chirs, "What We Learned About Technology From 1995's The Net", *WIRED*, https://www.wired.com/2013/04/the-net-movie-technology/ (ultima consultazione: 30 agosto 2023);

Schroeder Stan, "Shall We Play a Game? The Lasting Influence of WarGames", *GEN X Today*, https://genx.today/shall-we-play-a-game-the-lasting-influence-of-wargames/ (ultima consultazione: 2023);

Smilyanets Dmitry, "'I Was Running Two Parallel Lives': An Ex-Secret Service Agent Opens Up About Going Undercover To Catch Cybercriminals", *The Record. Recorded Future News*, https://therecord.media/i-was-running-two-parallel-lives-an-ex-secret-service-agent-opens-up-about-going-undercover-to-catch-cybercriminals (ultima consultazione: 30 agosto 2023);

Sodeman William A., "Communications Decency Act", Encyclopedia Britannica, 10 Aug. 2023, https://www.britannica.com/topic/Communications-Decency-Act (ultima consultazione: 14 Agosto 2023);

Warner William, "Breaking the Code of The Matrix; or, Hacking Hollywood to Liberate Film", *eScholarship University of California*, https://escholarship.org/uc/item/3nt8x916 (ultima consultazione: 30 agosto 2023);

Zelchenko Peter, “Jack Rickard, editor of Boardwatch magazine, saw it coming”, *Chicago Tribune*, 1998, https://www.chicagotribune.com/news/ct-xpm-1998-10-30-9901080059-story.html (ultima consultazione: 30 agosto 2023);

Zuckerman Esther, “'The Net' Is Even Weirder Than You Remember”, *thrillist*, https://www.thrillist.com/entertainment/nation/the-net-movie-review (ultima consultazione: 30 agosto 2023);

FILMOGRAFIA

Electric Dreams (Electric Dreams, Steve Barron, MGM, USA 1984);

Hackers (Hackers, Iain Softley, United Artists, USA 1995);

Impiegati... male! (Office Space, Mike Judge, Judgemental Films, USA 1999);

I signori della truffa (Sneakers, Phil Alden Robinson, Universal Studios, USA 1992);

Johnny Mnemonic (Johnny Mnemonic, Robert Longo, Johnny Mnemonic Productions, USA 1995);

Matrix (The Matrix, Andy e Larry Wachowski, Warner Bros., USA 1999);

Mission Impossible (Mission Impossible, Brian De Palma, Cruise/Wagner Productions, USA 1996);

Nemico pubblico (Enemy of the State, Tony Scott, Touchstone Pictures/Jerry Bruckheimer Films/Scott Free Productions, USA 1998);

Superman III (Superman III, Richard Lester, Warner Bros., USA 1983);

Tron (Tron, Steven Lisberger, Walt Disney Productions, USA 1982);

The Net - Intrappolata nella rete (The Net, Irwin Winkler, Columbia Pictures, USA 1995);

Wargames – Giochi di guerra (WarGames, John Badham, United Artists, USA 1983);