Hacking Hollywood: discussing hackers' reactions to three popular films

Vlad JECAN
Universitatea Babeş-Bolyai
E-mail: vjecan@gmail.com

Abstract: *In this paper I analyze the main characteristics of hacker culture as presented in three popular hacker films,* WarGames, Hackers *and* Takedown *with the intention of identifying the key elements against which the hacker community reacted. We shall find that hackers reacted favorably in the case of* WarGames *because the film offered an accurate portrayal of hacker activity and their culture while* Hackers *and, especially,* Takeover, *did not. I conclude in the case of* Hackers *that hackers reacted negatively probably because they felt that their culture was reduced to mere fashion while inaccurately portraying their activities and against Takeover because the film's intention was to criminalize the very idea of hacking.*

Keywords: *hacker culture,* Hackers, *Hollywood,* Takeover, WarGames, *popular films*

Hollywood has generally had an ambivalent approach towards hackers by portraying them in the 1980s and early 1990s as unintentional criminals who later emerge as necessary heroes while also depicting them as criminals hunted by the law enforcement in narratives of good versus evil. However, various films borrow certain elements of the hacker culture and display them as tools (or weapons) that will ultimately save the day. For example, in the 1996 film *Independence Day*, directed by Roland Emmerich, the alien invasion which threatened to annihilate mankind was successfully repelled not by advanced military technology but by intrusion and infection of the alien command ship. Intrusion occurred when the two main characters, played by Will Smith and David Levinson, used a captured alien ship to successfully sneak inside the command

ship and by infection when they ultimately succeeded in planting a computer virus that would immediately disrupt its impenetrable energy shield. By all definitions, this was an act of hacking. Furthermore, hacking is also positively portrayed in popular films like *Matrix*, when the main character, Neo, becomes himself a system anomaly, a virus by all means, and fights "the machines". There are numerous similar examples, however, this study focuses on three popular films that had their narratives focusing directly on hackers and hacking entirely and seeks to analyze the elements of the hacker culture as portrayed in these films in order to understand hacker reactions. In order to do so it is imperative to investigate the hacker culture and underline its main characteristics. Further, these characteristics will be identified in the three films which will enable us to understand hacker reactions. Consequently, we will be able to see why the hacker community was positively impressed by *WarGames* and responded negatively in other two cases, *Hackers* and *Takedown*, respectively.

Hacker culture

The hacker culture developed since the 1960s with the emergence of networked computing and finally the Internet itself. It is in this matter safe to suggest that hacker culture emerged in tandem with the development of the Internet and, as of today, their separation is inconceivable. Indeed, as Taylor observes, "the main and most obvious point to be made about hacker culture is its dependence upon technology" (Taylor 1999, 28). The first Trojan horses, the first viruses and computer worms, and everything related have been coded in the laboratories of various universities in the United States. At that time hacking did not have a negative connotation. In fact, the activity was seen as beneficial, as constant improvements to programs were made. Furthermore, computing at that time came with certain principles. Thomas observes that "the old-school hacker was frequently motivated by the motto "Information wants to be free", a credo that attributed both a will and an awareness to the information itself" (Thomas 2002, 11). In this matter, and with a mind on the socio-political context of the Cold War, we could argue that the hacker culture was part of the counterculture movement. However, in this article I will trace the main characteristics of the hacker culture and do not intend to discuss the culture in the wider context of the Cold War.

Jordan and Taylor (2004) distinguish three main types of the initial hackers: *the original hackers*, or the pioneering computer scientists who were coding at large universities in the United States like MIT during the 1950s and the 1960s, *hardware hackers* or innovators who, starting with the 1970s, contributed to the development of the personal computing revolution, and, finally, *software hackers* who focused mainly on building programs that would run on different hardware. However, these three originating communities are not completely distinct from one another; they "intersected and overlapped, such as it would not be surprising if some people fitted all three definitions" (Jordan and Taylor, 2004, 10. Chiesa et al. 2009, 41). By the

1980s hacker activity received criminal connotations. Initially, however, computer worms were seen as programs that would look for programming errors and fix them. After the Morris worm, the computing community sought a different term for harmful programs; the term computer virus was acknowledged (Zeltser, 2000). Furthermore, throughout the 1980s and the 1990s, and perhaps even today, the media was interested in the criminal aspect of hacking. Thomas observes that "the current image of the hacker blends high-tech wizardry and criminality". Indeed, "portrayals in the media have done little to contradict that image, often reducing hackers to lonely, malicious criminals who delight in destroying sensitive computer data or causing nationwide system crashes" (Thomas, 2002, 5), much to the protest of hackers. Even inside the hacker community there is a division between *white hat* and *black hat* hackers. The former usually conduct hacking in the name of improvement or for better security. Their hacks are usually sent to system administrators and later made public. After 911 a new category of hackers have emerged, the *patriot* hackers who broke into the Pentagon and NASA only to report their findings. *Black hat* hackers (or crackers) as the name suggests, are seen as "malicious" hackers. In any case, the media has ambiguously presented the hackers that "society's representation of hackers and definition describing them either demonize them or turn them into legends, depending on the source" (Chiesa et al. 2009, 33). For the purpose of this study we will first try to define what the hack and the hacker are, we will discuss their motivations, their ambivalent approach to secrecy and anonymity, and their relationship with technology. We can then proceed to analyzing the three films.

Hackers and the hack

There are various definitions of what "hacker" represents. Even among hacker groups the definition is continuously debated. Bruce Sterling notes that "'hacker' is what computer-intruders choose to call themselves. Nobody who 'hacks' into systems willingly describes himself (rarely, herself) as a 'computer intruder', 'computer trespasser', 'cracker', 'wormer', 'darkside hacker' or 'high tech street gangster'" (Sterling 1994, 66). A hacker who goes by the handle *Mofo the Clown* revealed his opinion on the term hacker in an interview with Paul Tyler. "'Hacker' to me – says Mofo – is a term which defines an individual who succumbs to his/her thirst for knowledge (and the computing power that accompanies that knowledge)" (Taylor 1999, 48). The term hacker is perhaps best defined by the activity it presumes. "The hack" is at the center of the hacker culture. Taylor observes that "despite its connotation of illicit computer break-ins, within hacking circles the hack is more widely defined as an attempt to make use of technology in an original, unorthodox and inventive way" (*Ibidem*, 15). Indeed, at the beginning of networked computing "the hack" itself meant improvement and progress. In the 1960s there were virtually no concerns about computer security, as Bruce Sterling wrote that back then "definitions of 'property' and 'privacy' have not yet

been extended to cyberspace[1]. Computers were not yet indispensable to society. There were no vast databanks of vulnerable, proprietary information stored in computers, which might be accessed, copied, without permission, erased, altered, or sabotaged" (Sterling 1994, 67). It was an age when software was not separated from hardware, when a computer was indeed a personal computer and for it to work, it had to be assembled by an individual who also had to write its entire software. "The way in which an operator programmed a computer, or accessed the information kept in it, depended upon the manufacturer and varied with each maker and each model" (Green 2010, 21). In consequence, knowledge of computing was reserved to a select few who ought to improve their programs by distributing them among themselves. A hack, in this matter, was considered an improvement, a smart and simple solution for a complex problem. One of the most famous hacks in history was performed by John Draper, better known as Captain Crunch. In early 1970s, Crunch discovered a whistle that came with Cap'n Cruch cereal (hence the handle) which sounded exactly the tone (2600Hz) that allowed to control the phone line and make phone calls for free (Thomas, 2002, 18). Turkle notes that the hack was impressive because Draper acquired a high level of expertise about the telephone system. "Mastery is of the essence everywhere within the hacker culture", but most notably, "the expertise was acquired unofficially and at the expense of a big system" (Turkle 2005, 208). Indeed, there are three main elements of a successful hack: (1) *simplicity*, a simple solution should meet a complex problem, (2) *mastery*, the hacker has to acquire extensive knowledge on the subject and (3) *illicitness*, "the act is 'against the rules'" (Taylor 1999, 16). Furthermore, a hack has to be original, "though it can be copied, it loses its status as a hack the more it is copied", (Jordan and Taylor 1998, 760) meaning that each hacker has to come up with innovative means of breaking into systems. *R,* a Dutch hacker interviewed by Tim Jordan and Paul Taylor said that the hack "pertains to any field of technology" as long as "you're using the technology in a way that it's not supposed to be used" (Jordan and Taylor 2004, 7-8). Thomas observes the distinction between a 'true hack' and a 'derivative hack.' "The first, according to Thomas, consists of using original methods to complete the hack. "True hacks" are the result of understanding how things work (or, sometimes, don't work) and taking advantage of those flaws, oversights, or errors in an original way" (Thomas 2002, 43). A 'derivative hack' on the other hand is frequently pursued by those who in the

1 The term "cyberspace" was coined by William Gibson in his 1984 book *Neuromancer*. Gibson defines cyberspace as "a consensual hallucination… A graphic representation of data abstracted from banks of every computer in the human system". Today the term is defined by the U.S. Department of Defense as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

hacking community are known as 'script-kiddies', individuals who use tools (programs) provided by others. Their hacking activity does not require in-depth knowledge of target systems. But why hack in the first place?

Motivations

Hackers themselves continuously mention a 'need for knowledge' and 'curiosity' as their main motivations to hack. However, Jordan and Taylor have identified no less than six motivations for hacking (Jordan and Taylor 1998, 768). First, according to the two authors, many hackers have "an addiction to computer and/or to computer networks, a feeling that they are compelled to hack". This view that hackers have an addiction to computing has frequently been employed in court. Bruce Sterling notes that "perhaps a metaphor was better – hackers should be defined as 'sick', as 'computer addicts' unable to control their irresponsible, compulsive behavior" (Sterling 1994, 68). Nevertheless, hackers constantly seek security loopholes in systems and prepare innovative programs in order to exploit them. Hackers find it difficult to describe this "addiction", but most often they discuss "the kick" behind hacking, a certain feeling that comes with the activity. Maelstrom, a hacker interviewed by Paul Taylor said that "I just do it because it makes me feel good, as in better than anything else that I've ever experienced" (Taylor 1999, 50). Indeed, it may be true that "the hack may provide a kick that is comparable to other forms of addiction but the imaginative and ingenious elements of hacking perhaps make it somewhat more important: few conventional drug addicts, for example, are perceived as posing a potential threat to national security as a direct result of their activity" (*Ibidem* 48).

The second motivation hackers frequently mention is curiosity. This curiosity probably emphasizes hacker distinct relationship to information. A hack is not necessarily performed to acquire secret information, rather "the desire to create the means to access that information". Indeed, this relationship to information may differ on a case by case basis. However, Douglas Thomas writes that "to the hacker, pure information is usually boring. The excitement lies in knowing how to get the information, regardless of its content" (Thomas 2002, 67).

Third, according to Jordan and Taylor, hackers feel that life outside the safety of the computer is boring. The element of technology is further emphasized here, as Turkle observes that "hackers don't live only with computers; they live in a culture that grows up around computers", (Turkle 2005, 196) contrary to the popular belief that hackers become fully immersed in a personal constructed world and prefer machines over people. The outside view is that hackers communicate with their computers while, in fact, they engage in long discussion with fellow peers on various topics. Turkle explains that "the hacker culture is a culture of loners who are never alone" (*Ibidem* 196).

The fourth motivation of hacking is the perceived power over important computer networks. Gaining control over systems like the NASA, ESA, military computers and

so on, is to gain power. Bruce Sterling notes that "'Power and knowledge' may seem odd motivations. 'Money' is a lot easier to understand. There are growing armies of professional thieves who rip-off phone services for money. Hackers, though, are into, well, power and knowledge. This has made them easier to catch than the street-hustlers who steal access codes at airports. It also makes them a lot scarier" (Sterling 1996). Additionally, Zoetermeer, a Dutch hacker interviewed by Paul Taylor, comments on the issue of 'feeling in power' as following: "Breaking into a bigger or more important system, or acquiring root-status can give you a real feeling of power and you seem to have proved yourself better than the system administrator" (Taylor 1999, 58).

A successful hack on an important system does not offer just a sense of being in power; it also offers peer recognition from other hackers and the acceptance into a community of elites, which is the fifth motivation for hacking according to Jordan and Taylor. Hacking into a perceived unbreakable system is also a form of winning and "in the hacker aesthetic, "winning" requires making the system and the challenge ever more complex" (Turkle 2005, 207). For hackers, peer recognition is essential to become 'elite,' or, put differently, to gain the respect within the hacker community. As we shall see further, the idea of peer recognition is constantly in conflict with hacker relationship to secrecy.

Finally, some hackers have taken on a computing crusade to make networks safe. This is mostly the case of *white hat* and *patriot* hackers who believe that their mission is to protect the Internet from whomever they perceive as being evil.

Secrecy and anonimity

Hackers usually have an ambivalent attitude towards secrecy. On one hand they support secrecy and operate inside its protective borders while on the other hand they expose their activities for peer recognition, mainly. As we have already seen the very intent of the hack is to be secret, it is to gain as much knowledge of a system as possible using illicit methods. "A hack demands secrecy, because it is illicit, but the need to share information and gain recognition demands publicity. Sharing information is key in the development of hackers, through it makes keeping illicit acts hidden law enforcement difficult" (Jordan and Taylor 1998, 764).

Anonymity, however, has nothing to do with secrecy; it concerns the offline identity of the hack which must always remain unknown. Hackers usually create handles, assume an online identity under which operate in cyberspace. The way in which hackers choose their handles reflects their attitude towards technology. In most cases, the identity given by a random word is immersed in programming language by transforming letters into numbers. For example, one will rarely see a hacker describe a hack using the word elite, instead he or she will most probably use 'l33t,' 'l337,' or '7337.' Bruce Sterling observes that "the digital underground, which specializes in information, relies very heavily on language to distinguish itself" (Sterling 1994, 84). Hackers also employ "specialized orthography", and frequently change the letter "f"

with "ph" (as philes instead of files), "z" instead of the plural "s", and the numeral "0" is preferred to the letter "O" (*Ibid.* 85). Thomas notes that these substitutions are in fact "translations of language into technology, translations that are the direct heritage of the keyboard" (Thomas 2002, 57). Group names do not differ essentially, but sometimes they are employed to mock corporations and established government institutions. Names such as "NASA Elite", or "NATO Associations", "IBM Syndicate" or "Feds R Us" are frequently used. Also, hackers tend to be "using stigmatizing pejoratives as a perverse badge of honor is a time-honored tactic for subcultures: punks, gangs, delinquents, mafias, pirates, bandits, racketeers" (Sterling 1994, 85). Other well-known groups have adopted colorful names such as "The Legion of Doom" or "The Cult of the Dead Cow".

Male dominance

We have underlined the hacker relationship to technology, secrecy and anonymity and what it is to hack. Another important aspect of the hacker culture must be analyzed before we can dwell further into our study. There are few female hackers, not because hacker culture is hostile towards women, but one reason may be that hacking is generally unappealing to women. Paul Taylor has interviewed *Mercury*, a male hacker, who underlines this very point: "My wife programs and she has the skills of a hacker. She has had to crack security in order to do her job. But she does it AS HER JOB, not for the abstract thrill of discovering the unknown… Females who compute would rather spend their time BUILDING a GOOD system, than breaking into some else's system" (Taylor 1999, 37). However, another important factor is that computing is generally perceived as a male activity, as Jordan and Taylor remind of "childhood socialization, where boys are taught to relate to technology more easily than girls" (Jordan and Taylor 1998, 767). While the hacker culture is not hostile towards women[2] it may be nonetheless an issue from the inside. Turkle suggests that the hacker culture resembles in many cases elements of a macho culture. "The preoccupation with winning and of subjecting oneself to increasingly violent tests makes their world peculiarly male in spirit, peculiarly unfriendly to women" (Turkle 2005, 194). Indeed, hackers "win" over systems and are keen for peer recognition. Male hackers are constantly looking for 'the kick' and for 'being in power,' while women, as Mercury explained, see hacking sometimes as a necessity, but they are generally interested in building and perfecting a system. As we shall see further, the contest

2 A hack is successful and well received by the hacker community if it has the mentioned characteristics of simplicity, mastery and illicitness, it is not a question of gender. Moreover, Steven Levy identified certain principles of the hacker 'moral code' according to which "hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position". Levy, Steven, *Hackers. Heroes of the computer revolution*, O'Reilly Media, 2010, p. 29.

between Dade (aka Zero Cool, aka Crash Override) and Kate (aka Acid Burn) from the movie *hackers* is actually a boy war during which they express affection for each other and acknowledge each other hacking skills.

Summary: main aspects of hacker culture

In previous pages we have discussed the main aspects of the hacker culture. It is a culture of the 'elite', of computer wizards who constantly seek new cyber-realms to explore. One important aspect of the hacker culture is its relationship with technology. As we have seen, everything related to the culture is primarily related to technology. The hacker culture was built upon technology and remains completely immersed in technology. Hackers frequently mention "an addiction to computer and/or to computer networks" and a desire for the ultimate experience found in 'the hack'. This 'addiction' persists due to unbound curiosity which reveals the hacker relationship to information. While discovering new information and continuously gaining knowledge, the information itself is not important. What matters is to discover the means on how to access that information. The experience of the hack also offers a feeling of being in power over systems and 'winning' over system administrators. Important systems are targeted not because they want to wreak havoc or for financial gains, but because an important hack offers peer recognition. A hacker builds a name for him or herself by the importance of the hack. This leads to the ambivalent relationship towards secrecy and anonymity. Secrecy is required during hacking but the result needs to be 'publicized' because only in this way a hacker can gain recognition and status within the hacker community. Anonymity on the other hand is distinct from secrecy and it practically refers to the offline identity of the hacker which must always remain unknown. In all cases they create handles, virtual identities, and perform their activities under their chosen pseudonyms. These handles reflect the strong relationship between hackers and technology. The words used are "translations of language into technology". Learning about technology is usually a male activity; this may be a factor that explains the absence of women hackers.

While the discussion about hacker motivations and the overall hacker culture continue, these are the prime characteristics of the hacker culture, and for our purpose it is sufficient to understand them. By identifying these characteristics in Hollywood films we can discover hacker's different reactions towards *WarGames*, *Hackers*, and *Takedown*.

WarGames (1983)

WarGames was one of the first Hollywood forays into a still young hacker culture. The film opens with a military simulation at a secret nuclear missile control center. The commanding officer hesitates to launch the missiles and breaks procedure "before we kill 20 million people". Following the simulation's failure, the U.S. Air Force Command decides to replace the human element with remotely controlled electronic

systems. Decisions about nuclear warfare are to be made by a state-of-the-art computer named WOPR – War Operations Plan Response – which "plays a series of war games. It already played World War 3 over and over again". The computer's sole purpose is to investigate all nuclear war scenarios and discover the best strategy for the U.S. in order to achieve victory with minimum damages and human casualties. It is with the opening scene that we are introduced to the context of the Cold War and, indeed, to the main anxieties of the time: nuclear warfare and technophobia. The later was expressed by the commanding general Beringer, played by Barry Corbin, who will constantly express his doubts about WOPR's capabilities. According to Douglas Thomas, "the film demonstrates a tremendous anxiety about technology, represented both by the missiles that threaten to destroy the United States and the Soviet Union and by the machines that control those missiles" (Thomas 2002, 25). We can perhaps suggest that the computing revolution was initiated and developed in a context of conflict. After all, the Internet is a military invention.[3] Indeed, as Keohane and Nye Jr. argue that "the information revolution occurred not merely within a preexisting political context, but within one characterized by continuing military tensions and conflicts" (Keohane and Nye 2006, 208). In a New York Times review of the film published the day after the film's premiere, Vincent Canby observes that "because it immediately

3 The Internet as a military innovation is highly debated among historians. Bruce Sterling argued that the Internet was developed out of a military communication necessity, "the RAND Corporation, America's foremost Cold War think-tank, faced a strange strategic problem. How could the US authorities successfully communicate after a nuclear war?" see http://w2.eff.org/Net_culture/internet_sterling.history.txt. Harper and Lyon de-emphasized the political context in which the Internet was developed and instead narrated, as Rosenweig put it, "a story that most engineers would like – a tale of adventurous young men motivated by technical curiosity and largely unaffected by larger ideological currents or ever narrower motives of self-advancement or economic enrichment" see Hafner, Katie, Lyon, Matthew, *Where Wizards Stay Up Late: The Origins of the Internet,*Simon & Schuster,1998, and *Rosensweig*, Roy, *Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet,* in The American Historical Review, vol. 103, no.5 (Dec., 1998), p. 1534. The role of the ARPA (Advanced Research Projects Agency) in creating the Internet is celebrated by Arthur Norberg and Judy E. O'Neill in their version of the history of the Internet, see Norberg, Arthur L., O'Neill, Judy, E., *Transforming Computer Technology: Information Processing for the Pentagon 1962-1986*, The Johns Hopkins University Press, 2000. However, a different approach is offered by Michael and Ronda Hauben who argue that the story is actually about the "netizens" who discovered the true functions of the Internet and popularized it. Their narrative moves away from the military and the engineers and focus on the Internet users, see Hauben, Michael, Hauben, Ronda, *Netizens: On the History and Impact of Usenet and the Internet*, Wiley-IEEE Computer Society Pr, 1997. Online version available here: http://www.columbia.edu/~rh120/ This author agrees that the Internet was a project initiated by the U.S. military due to military concerns in a context of political and military tensions.

connects our nightmares about thermonuclear war and a world ordered by unreliable computers, it grabs us where we're most vulnerable" (Canby 1983).

With this introduction the focus is shifted towards David Lightman, a high-school student with "an attitude problem" who successfully breaks into the school's computer and changes his grades to avoid summer school. Lightman reads in a magazine about an upcoming game which will be released by a company called Protovision and sets up his computer to repeatedly dial numbers in an attempt to identify the company online, hack into its system and play the game before everyone else. This practice was common among hackers, "I called it scanning", said John Draper, famous by his handle Captain Crunch, "the use of a dialer scanner program came from me repeatedly dialing up numbers until I found a computer modem" (Brown 2008). In his search for Protovision, Lightman stumbles upon a different computer, one that presents a diverse assortment of games from chess and checkers to thermonuclear war. Failing to access the computer, Lightman's curiosity enables him to seek information about the system developer which he hopes will offer him hints on how to hack the computer, "as the name suggests, Lightman wants to see something before anyone (or, more to the point, everyone) else does" (Thomas 2002, 30). Our main character learns everything there is to know about the system's developer professor Falken and understands his creation, which will enable him to find a simple solution to a complex problem. The password to the computer is Joshua, the name of Falken's defunct son. In this matter, Lightman's actions appealed to the hacker community, he illicitly obtained in-depth knowledge of the system which revealed a simple solution – these are, as we have seen, the requirements for an appreciated hack. However, once the hack was performed, Lightman unknowingly initiated a computer simulated nuclear conflict between the Soviet Union and the United States. However, at the NORAD military base, the threat is perceived as real and General Beringer prepares for a nuclear counter attack. "David is alarmed and genuinely frightened by the forces he sets in motion, but he is also a bit pleased. He's pleased, that is, until he realizes that the world will probably end about two hours before he has a chance to see his girlfriend, Jennifer (Ally Sheedy), in a brief television appearance" (Canby 1983).

WarGames reveals an ambivalent approach towards hackers. First, Lightman is portrayed as a harmless high-school student who only seeks an unreleased game, while also his in-depth knowledge of computers will ultimately save the day. However, "the hacker is positioned as dangerous because he is exploring things about which he has little or no understanding. It is easy in a world of such great technical sophistication, the film argues, to set unintended and potentially disastrous effects into motion even accidentally" (Thomas 2002, 25). One important characterization of the hacker that we find in this film is that of a hero. It is not WOPR's creator who will save the day, but David's knowledge on WOPR and his understanding of "playing a game".

The film was tremendously successful. Roger Ebert, one of Hollywood's most influential film critic, wrote immediately after the film's release that "the movie,

however, could easily go wrong by bogging us down in impenetrable *computerese*, or by ignoring the technical details altogether and giving us a "Fail Safe" retreat. "WarGames" makes neither mistake. It convinces us that it knows computers, and makes its knowledge into an amazingly entertaining thriller" (Ebert 1983). With a mind on the hacker community, Bruce Sterling observes that "it seemed that every kid in America had demanded and gotten a modem for Christmas. Most of these dabbler wannabes put their modems in the attic after a few weeks, and most of the remainder minded their Ps and Qs and stayed well out of hot water. But some stubborn and talented diehards had this hacker kid in *WarGames* figured for a happening dude. They simply could not rest until they had contacted the underground – or, failing that, created their own" (Sterling 1994, 84-85).

WarGames appealed to the hacker community mostly because it portrayed their activity not with hyperbole, but with fair accuracy. First, Lightman has performed a by the book hack consisting of simplicity, in-depth knowledge (mastery) and illicitness. Second, hackers could relate to the main character. In the film, Lightman was not portrayed as a dangerous individual, but as a harmless and well-intentioned high-school kid who only sought knowledge and was motivated by curiosity. Finally, the hacker was also portrayed as a hero. The '7337' skills of David prevailed over those of the WOPR's developer and managed to save the day.

Hollywood's ambivalent approach towards hackers continues in the 1995 movie *Hackers*. However, at that time the Cold War was over and a new wave of hackers emerged. While general reactions among hackers towards *WarGames* were positive, we shall further examine the negative appreciation of the film *Hackers*.

Hackers (1995)

Much has changed in the hacker community in the twelve years between the release of *WarGames* and *Hackers*. First and most important, within the hacker community emerged an evident divide between traditional hackers following their old-school creed and a new type of hackers with 'malicious' activities. Consequently, media attention was almost completely focused on how computers were hacked and sought to emphasize the new threat that hackers posed. Secondly the advent of the Internet had a tremendous impact on the hacking community and "the result has been an explosion of "hackers" of every type, from the preteen kids to old-school hackers in their forties and fifties" (*Ibid.* 81). In this matter, Douglas Thomas observes that "*Hackers* attracted the attention of a new generation of technologically literate hackers, who saw the Internet as the new frontier for exploration" (*Ibid.* 156).

The separation of the old-school and malicious hackers became evident with the launch of the Morris Worm, also known as the "Internet worm". It was developed in 1988 by Robert Morris, the son of one of the builders of the Internet. "The worm exploited a non-standard command available in a particular version of sendmail to propagate from one machine to another. As the worm installed itself on the newly

compromised host, the new instance of the program began self-replicating further in a recursive manner" (Zeltser 2000, 3-4). It would also send user information along with passwords and other data back to Morris. This incident ignited a serious debate inside the computer community on the intent of the worm and a new name was needed for this now perceived malicious program. Previously, the computer worm was first developed by Xerox and was designed to be beneficial. Certainly, there was nothing beneficial about the Morris worm and a new term was generally accepted, the computer virus. "The connotations of viruses as sickness, illness, and even death (particularly in the age of AIDS and Ebola) provide an interesting counterpoint to the discussion of the "Internet worm" (Thomas 2002, 29). *Mofo the Clown* in an interview with Paul Taylor explained that: "I and many others have used the UNIX sendmail bug to access many, many systems throughout the world (without damaging data in any way) until that stupendous asshole, Robert Morris, royally phucked everything up for us. I've known about the print f() sendmail bug ever since I got access to source. Only a dummy would publicize something as good as that by doing something completely phucking stoopid like what Morris did. His idiocy cost hackers/phreakers more than anyone can imagine" (Taylor 1999, 31). *Hackers* opening scenes portray the arrest and trial of eleven year old Dade Murphy, aka Zero Cool (played by Johnny Lee Miller) who is accused of "criminal acts of a malicious nature". The Prosecutor continues: "his computer virus crashed one thousand five hundred and seven computer systems, including Wall Street trading system, single handedly causing a seven point drop in the New York Stock Market". Dade is completely different from Lightman, he is not presented as a harmless and curious hacker who only seeks to play games, but instead it is revealed from the very beginning that he is a malicious hacker (he caused damage).

Years later, at the age of 18, Dade is once again legally permitted to use a computer. He is now in New York and his first hack is a local TV station. During the hack and while making use of social engineering (probably much to the appreciation of hackers) he successfully gains access to the TV station. However, he apparently entered the 'realm' of a hacker called Acid Burn and a battle begins for the control of the station, a battle that Dade, now going by the handle Crash Override, loses. Later he joins a socially active hacker group and discovers that Acid Burn is actually the attractive Kate Libby (played by Angelina Jolie). "These hackers are not isolated loners or misunderstood teens; they are cutting-edge techno-fetishists who live in a culture of "eliteness" defined by one's abilities to hack, phreak, and otherwise engage technological aspects of the world (including pirate TV and video games) (Thomas 2002, 161). In order to prove himself the better hacker, he challenges Acid Burn to a hacker contest. However this is not entirely a battle of skills, the contest is actually a way in which Kate and Dade express affection for each other while also acknowledging their hacker skills. Furthermore, "while Kate's *character* is female, the *role* she plays is masculine, a hacker superior to everyone in her circle of friends, until she is challenged by the newcomer, Dade" (*Ibid.* 161). Thomas further observes that

this is an instance of boy culture and "affection between Dade and Kate is displayed in a series of contests – first video games and later a series of hacks against Secret Service agent Richard Gill" (*Ibid.* 159). Meanwhile Joey, a yet untried hacker, in an attempt to prove himself 'elite' hacks into a corporation's super-computer, the Gibson computer. In order to prove his hack, Joey copies a series of files. Little does he know that the files contained the code of a worm that threatens to cause an ecological disaster if the corporation does not send a huge amount of money to a bank account. The Plague, the corporation's computer security wizard, finds this hack to be an excellent opportunity to blame hackers. A series of arrests follow in a man hunt conducted by Secret Service agent, Richard Gill. A few elements are quite obvious in this film. All hackers go by their handles while their real names are rarely used and the film portrays a different relationship to technology "manifested in their clothing, their appearance, and, ultimately, their bodies. Accordingly, *Hackers* reduces hacker styles to a techno-fetishism" (*Ibid.* 159). A San Francisco Gate reviewer wrote that "for reasons that don't always compute, they skate and wear punk clothes and exude a leather-centric counterculture attitude" (Stack 1995). This special relationship with technology is further emphasized in the film when The Plague finds the need to send a message to Dade. He does so by sending a laptop and after Dade opens it, The Plague appears and issues a warning. "As fantastic as such an interaction may be, it illustrates precisely the way the film views hackers' interactions. Hackers are seen as figures who are only able to communicate about and through technology" (Thomas 2002, 160). In the final scene, Dade is completely immersed in technology. In fact, he "has become the machine that he seeks to invade" (*Ibid.* 162). The way technology itself is presented in the film has attracted the attention of various reviewers. A StarPulse review notes that "depictions of actual computer interfaces all, of course, resemble cryptic and ornate screen-savers" (StarPulse 1996).

An important characterizing element of hackers in the film is the presence of National Security agent Richard Gill. The character is a general symbol standing for how hackers are usually misunderstood. Gill constantly repeats an exaggerated and sensationalistic description of hackers making absolutely clear that he, and generally the law enforcement, has virtually no knowledge of hackers: "Hackers penetrate and ravage delicate public and privately owned computer systems, infecting them with viruses, and stealing materials for their own ends. These people, they are terrorists". Thomas notes that "the highly sexualized metaphors of penetration and ravaging set against the delicacy of sensitive computer data suggest that the hackers are rapists and the computers are feminine" (Thomas 2002, 177). But this not the sole time that computers are depicted as feminine. Joey usually refers to his computer as "Lucy" when hacking the Gibson computer.

Hackers was neither a critical nor a commercial success, it was largely ignored. However, it was viewed by hackers who felt that their culture was being bombarded by inaccuracies and wild exaggerations. Consequently, they hacked the film's website

and created their own version in protest. Thomas suggests that "they argue that the film threatens to undermine an entire system of representations that describe hacker culture and which hackers themselves identify" (*Ibid.* 167). It should be quite obvious why the hackers reacted in protest. First, the main character was presented as a malicious character from the very first scenes. Second, and most important, their relationship with technology was completely misrepresented. Hackers apparently did not agree with *Hackers* fashion. Third, hackers reacted against the mantra of the film, "Hack the planet", believing that the new generation of hackers "will see the globalization of technology and capital as the "liberation" of knowledge" (*Ibid.* 170).

However, *Hackers* did an accurate depiction of the low level of understanding of hacker culture by law enforcement. Their highly hyperbolic discourse on hackers, comparing them to criminals and terrorists, and the media's interest in such stories will influence real-life convictions of hackers. Kevin Mitnick, on whose story was depicted in the film *Takedown*, spent about seven months in solitary confinement because of a fear that he would be able to damage phone lines by simply touching a phone.

Takedown (1999)

The film's narrative follows facts as presented by Tsutomu Shimomura and John Markoff in their book *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Outlaw*. Both have been deeply involved in the Kevin Mitnick story, Shimomura was the one who actually provided the FBI with necessary information in order to locate Mitnick while Markoff was a New York Times writer covering the story of whom he called the 'darkside hacker.' The book presents an epic battle between good and evil. Good represented by Shimomura and evil by Kevin Mitnick. Douglas Thomas observes that "in Shimomura and Markoff's telling of the incident, the contest between the two men was a "battle of values", where Shimomura represented the "honorable samurai" and Mitnick the "evil genius" (Thomas 1998, 3). This becomes quite evident in the film when Shimomura, played by Russell Wong, tells the FBI agent that "I'm a hacker, he's a cracker". In this film, the hacker is no longer presented as a harmless individual who seeks to uncover the unknown in cyberspace. Instead, the introductory scenes gather a series of images and statements that fully characterize hacking as a criminal activity and, consequently, the hacker as a dangerous individual. Most importantly in the general narrative of the film, curiosity is criminalized. In the case of the SAS (Switch Access Services) system hack which will eventually start the two year manhunt by the FBI, Mitnick replies "just have to know", when asked why does he need information on the system. However, much importance is conferred to social engineering, as Mitnick, played by Skeet Ulrich, frequently manages to talk his way to acquiring confidential information and gain access to research laboratories where he (mis)uses their state-of-the-art, government funded computers. Thomas notes that "Mitnick's social-engineering and phreaking abilities were always the bedrock of his hacks" (Thomas 2002, 198). The hacker himself would later writer that "the human factor is truly security's weakest link" (Mitnick 2002, 3). As in the case of *Hackers*,

law enforcement is unable to understand how hackers operate and ultimately accept the help of civilians in order to track down Mitnick. However, *Takeover's* real story begins when Mitnick hacks Shimomura's computer and downloads information on a phone system. At this point, tracking down Mitnick becomes Shimomura's personal mission and will ultimately prevail.

Hacker relationship with technology is not presented as in the case of *Hackers*, except in one instance at the end of the film when Tsutomu becomes the computer on which Mitnick uploads files. Overall, the film does not emphasis hacker relationship to technology, instead technology is depicted as a tool which can be used in malicious ways if it falls in the wrong hands, or, as the film suggests, if it is used by hackers.

In consequence, we can clearly see why hackers might have disapproved with the message of the film. The hacker is portrayed as a criminal and a dangerous individual to society who, if successful in acquiring the necessary technology, will use it to cause harm. Furthermore, the 'need to know' is criminalized and Mitnick is presented as an addict who eludes the FBI for two years only to satisfy his addiction. Nevertheless we should point out that the film was released four years after Mitnick's capture and imprisonment. During these years, the New York Times continued to follow his story and other publications began to emphasize the lack of understanding showed by law practitioners in Mitnick's case. For example, the judge responsible with his legal case "had prohibited Mitnick from unsupervised access to telephones while awaiting trial. The Office of Prisons found that the only way it could comply with the judge's order was to keep Mitnick separated from the general population. As a result, Mitnick spent eight months awaiting trial in solitary confinement" (Thomas 2002, 205). Furthermore, the judge denied him the right to a bail hearing. In response to what people believed to be illegal treatment of Mitnick, the "Free Kevin" movement emerged. It was at this time that hackers would organize and campaign for a cause, which it may be one of the first instances of hacktivism. In any case, the individuals involved in the movement created a website, freekevin.com, distributed flyers and sought to receive as much media attention as possible. In one instance, the website of the New York Times was hacked on the weekend the Starr report was released. Mitnick's lawyer presented the official statement: "Kevin Mitnick appreciates the support and good wishes of those who speak out against his continued state of incarceration for years without bail. However, he does not encourage any individuals to engage in hacking pranks on his behalf. Kevin believes other avenues exist that can be more beneficial to his circumstances" (Thomas 2002, 206).[4] The incident shows that hackers believed that the NY Times misrepresented their culture and their activities.

4 In a 1999 Forbes interview, Mitnick commented on the incident: "I don't condone anyone causing damage in my name, or doing anything malicious in support of my plight. There are more productive ways to help me. As a hacker myself, I never intentionally damaged anything". See http://www.forbes.com/1999/04/05/feat.html

Indeed, the difference between *Takedown*, *WarGames* and *Hackers* is that the later were fiction while the first was based on a real story, where "real" was defined by the highly criticized book written by Shimomura and Markoff. In the same time, hacker reactions to *WarGames* and *Hackers* were directed exactly towards how the films presented characteristics of their culture while reactions towards *Takedown* were generally influenced by Mitnick's story itself as presented by the media. Littman noted that "the front-page placement [in the New York Times] was proof of the enduring power of Kevin Mitnick's legend" (Littman 1998, 33). Years later, in 2005, Kevin Mitnick wrote about hacking that it "is a creative art-figuring out ways to circumvent security in clever ways, just like lock-picking enthusiasts try to circumvent locking mechanisms for pure entertainment value. Individuals could hack without breaking the law" (Mitnic and Simon 2005, 91).

Conclusions

We have seen the main characteristics of the hacker culture and analyzed the three Hollywood films. This will enable us to see exactly why hackers reacted.

Hacker and the hack

With the release of *WarGames* in 1983, the hacker was portrayed as a harmless individual who only sought to "play games". Indeed, Lightman is not portrayed as a dangerous individual and hacking is not meant to be a criminal activity. However, hacking itself is presented as potentially dangerous because the hacker may gain access to things which he does not understand and his actions can lead to serious consequences. The film presents a 'by the book' hack: Lightman secretly acquired in-depth knowledge of the system and discovered a simple solution to gain access. The process of hacking, as in scanning, can be easily identified and approved by hackers. Additionally, Lightman is also portrayed as a hero because the day was saved only due to his in-depth knowledge of WOPR and "7337" skills. Indeed, *WarGames* portrayed the hacker culture not with hyperbole but with fair accuracy.

Hackers on the other hand would respond to the changes that occurred within the hacker community itself and tried to depict hackers in terms of fashion rather than in terms of 'skills.' Although an emphasis is added to how hackers perceive themselves as 'elite,' with additional underlying of their relationship to secrecy and anonymity, it failed to vividly and accurately portray 'the hack.' Instead, the film suggests that hackers are able to communicate only through technology. Consequently, hackers felt that they are inaccurately presented and their culture is under threat.

Takedown is a special case. Hackers are depicted from the early scenes as malicious, as individuals will use their special skills and understanding of technology to do great harm to others. Although, the film provides as special emphasize of 'the hack' and 'the kick' while focusing on the social engineering part of hacking, its entire narrative was based on just one side of the story, that of Shimomura and Markoff. As

noted earlier, *Takedown* is a story of good versus evil where hackers are presented *in extenso* as evil, while the computer security specialist working for government and corporations was shown as a hero.

Motivations

Lightman does not intent to cause harm to anyone and most certainly doesn't want to start World War 3. His main motivation for hacking is the need for knowledge, to find out what is behind the mysterious computer he discovered while scanning for Protovision. But first he is interested to know how he can gain access to the computer. Indeed, the film points out that Lightman is motivated by curiosity.

In the film *Hackers* motivations are not presented as in the case of *WarGames*. We do not find curious hackers who seek knowledge; instead the film may show the need for peer recognition. Joey hacks the Gibson computer in order to show that he is worthy to be considered 'elite' while Kate and Dade engage in a battle of skills during which they express affection for each other and acknowledge their hacking skills. In *Hackers'* introductory scenes, Dade is shown as a hacker who caused damage and later The Plague is clearly depicted as a malicious hacker who sought financial profit. In this case, then, Dade and The Plague share the label of *black-hat* hackers at different degrees. The former has caused damage while the later seeks to cause damage if he does not get what he wants.

Takedown in terms of motivations is an entire different story. The film clearly underlines Mitnick's obsession with computers and defines the addictive nature of hacking. In the context of the film, curiosity while seen as the main reason for Mitnick's activity is also criminalized.

Secrecy and anonymity

Hacker culture usually offers an ambivalent approach to secrecy. Hackers operate in secrecy and one requirement for a successful hack is 'illicitness,' however they also seek to gain peer recognition by publishing their activity and discoveries. Anonymity on the other hand concerns the off-line identity of the hacker. As showed in previous pages, hackers usually operate online under the cover of pseudonyms that suggest their special relationship with technology. In the case of *WarGames*, Lightman did mostly operate in secrecy and there was no need for peer recognition. Anonymity in the film is not underlined as David did not operate under a handle.

Hackers clearly emphasizes anonymity. Characters usually go by their handles while their real names are only sporadically mentioned. However, the film shows that in order to become 'elite' a hacker has to make known his or her activity. This is the case of Joey, who, as previously mentioned, hacked the Gibson computer in order to gain peer recognition and become an 'elite' hacker.

Kevin Mitnick's hackings were usually performed under the handle 'Condor.' However, this is not mentioned in the film. The film, and Shimomura and Markoff's story, tried to show that there is no real difference between hacking and criminal

activities. Secrecy is further shown as employed by criminals. Mitnick did indeed operate in secrecy but he had no real other choice. Finally, the media attention Mitnick received was unintentional as he never went out after fame. However, as Littman wrote the media's interest in Mitnick's story built and strengthened his image as a hacker legend.

Male dominance of the hacker culture is clearly depicted the the three films, excepting maybe *Hackers*. However, in that film, as Thomas suggested, the character played by Angelina Jolie may be female but her activities are essencially male. The fact that the three films presented a male dominance of the hacker culture was not a cause for reaction. Hackers should be judged by their skills, as Levy showed, not by "bogus criteria such as degrees, age, race or position".

We can now conclude that hackers reacted to Hollywood depiction of their culture favorably in the case of *WarGames* because it was an accurate representation of their activity and did not try to criminalize it. While the film also suggests that hacking may be dangerous, it is with a special emphasis on *may* and it also suggests that hackers should be careful. However, hackers felt that they are misrepresented in the film *Hackers*, mostly because their culture was reduced to fashion and musical preferences combined with depiction of their activities and technology that undoubtedly was considered pure fantasy. While the film does indeed its best to portray other characteristics of the hacker culture, hackers reacted to the abovementioned misrepresentations of their culture. In the case of *Takedown*, hackers reacted because Mitnick was portrayed as a criminal and in consequence they were portrayed as criminals. However, as previously pointed out, the film was released about four years after Mitnick's arrest. During these years people who were or were not hackers have organized the "Free Kevin" movement because of Mitnick's inappropriate detention conditions and violation of his rights. Additionally, they reacted against the New York Times because of what they felt was its hyperbolic, incriminatory and inaccurate discourse.

References

Chiesa, Raoul, Ducci, Stefania, Ciappi, Silvio, (2009), *Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking*, CRC Press

Green, Leila, (2010) *The Internet: An Introduction to New Media*, Berg

Hafner, Katie, Lyon, Matthew, (1998) *Where Wizards Stay Up Late: The Origins of the Internet,* Simon & Schuster

Jordan, Tim, Taylor, Paul, A., (2004) *Hacktivism and Cyberwars. Rebels with a cause*, Routledge

Keohane, Robert, O., Nye, Joseph S., Jr. (2006), *Power and interdependence and the information age,* in Richard Little and Michael Smith (eds.), *Perspectives on World Politics,* Routledge, pp. 207-217

Levy, Steven, (2010), *Hackers. Heroes of the computer revolution*, O'Reilly Media

Littman, Jonathan, (1997), *The Fugitive Game*, Brown and Company Ltd.

Mitnick, Kevin, D., Simon, William, L., (2005), *The Art of Intrusion*, Wiley Publishing,
Mitnick, Kevin, (2002), *The Art of Deception. Controlling the Human Element of Security*, Wiley Publishing
Hauben, Michael, Hauben, Ronda, (1997), *Netizens: On the History and Impact of Usenet and the Internet*, Wiley-IEEE Computer Society Pr.
Norberg, Arthur L., O'Neill, Judy, E., (2000), *Transforming Computer Technology: Information Processing for the Pentagon 1962-1986*, The Johns Hopkins University Press
Sterling, Bruce, (1994), *The Hacker Crackdown*, Literary Freeware
Taylor, Paul, A., (1999), *Hackers. Crime in the digital sublime*, Routledge
Thomas, Douglas, (2002), *Hacker Culture*, University of Minnesota Press
Turkle, Sherry, (2005), *The Second Self: Computers and the Human Spirit*, The MIT Press

Webliography

Brown, Scott, (2008), *WarGames: A Look Back at the Film That Turned Geeks and Phreaks Into Stars*, Wired, Available here: http://www.wired.com/entertainment/hollywood/magazine/16-08/ff_wargames?currentPage=all
Canby, Vincent, (1983), *'WarGames,' a Computer Fantasy*, New York Times, Available: http://movies.nytimes.com/movie/review?res=9F0DE6D9103BF930A35755C0A965948260
Ebert, Roger, (1983), *WarGames*, Chicago Sun Times, Available: http://rogerebert.suntimes.com/apps/pbcs.dll/article?AID=/19830603/REVIEWS/306030301/1023
Jordan, Tim, Taylor, Paul, (1998), *A sociology of hackers*, p. 760. Available here: http://www.dvara.net/hk/1244356.pdf
Penenberg, Adam, L., (1999) *Mitnick speaks!*, May 4 1999, Available here: http://www.forbes.com/1999/04/05/feat.html
Stack, Peter, (1995) *'Hackers' Computer Visually*,. Available here: http://articles.sfgate.com/1995-09-15/entertainment/17814990_1_computer-hackers-director-iain-softley-angelina-jolie
StarPulse, (1996) *Hackers Review*, Available here: http://www.starpulse.com/Movies/Hackers/Review/
Sterling, Bruce, (1993) *A Short History of the Internet*, , Available: http://w2.eff.org/Net_culture/internet_sterling.history.txt
Sterling, Bruce, (1996) *CyberView `91*, available: http://w2.eff.org/Misc/Publications/Bruce_Sterling/cyberview_91.report
Thomas, Douglas, (1998) *Hacking L.A.: Exploring Los Angeles' Digital Underground*, Annenberg School for Communication, University of Southern California, Available here: http://www.usc.edu/dept/LAS/SC2/pdf/thomas.pdf
Zeltser, Lenny, (2000) *The Evolution of Malicious Agents*, http://zeltser.com/malicious-agents/