TRANSMISSIONS: THE JOURNAL OF FILM AND MEDIA STUDIES 2017, VOL.2, NO. 1, PP. 62-77.

Marta Stańczyk
Jagiellonian University

Unseen war? Hackers, tactical media, and their depiction in Hollywood cinema

The geeks have emerged in politics.
(Tim Jordan, *Activism! Direct Action, Hacktivism and the Future of Society*)

The feelings of vulnerability, fear of the unknown, and embarrassment that feed the hysterical reaction to hackers also lead to the fetishizing of hackers in popular culture.
(Tor Ekeland, *Hacker Madness*)

Abstract

Emerging controversies about WikiLeaks' contribution to Donald Trump's electoral triumph and the ongoing persona-non-grata status of Edward Snowden highlight the notion of hacking in the modern world. Hackers used to be dualistically stereotyped on one hand as black hats, criminals and cyberpunk/cypherpunk hidden figures, and on the other as whistle-blowers, open access activists and hacktivists whose actions are potentially subversive. Film coverage of hackers and their tactics shows a paranoid and militarized vision of the world, with grey eminence often depicted either as a threat, or as survivors. Hence, from *WarGames* (1983, John Bedham), *TRON* (1982, Steven Lisberger) and *Hackers* (1995, Iain Softley) to *The Fifth Estate* (2013, Bill Condon), *Live Free or Die Hard* (2007, Len Wiseman) to *Jason Bourne* (2016, Paul Greengrass), hacking seems to have emerged as the avant-garde of militarized social space—as its main weapon and fundamental defence. Pop culture feeds itself with this ambiguity as long as it accommodates the dualistic needs of its receivers: a countercultural anti-hero becomes a scapegoat while a general sense of insecurity predominates. Distrust in technology and underground experts is simultaneous with redemption narratives about disclosing corporate/state/elite conspiracies and is heavily influenced by current non-cinematic events. This paper is an examination of hackers' cultural impact and their connection with tactical media through subversive

actions. It becomes essential to decode their manipulated or simplified public image, especially with ongoing progressive politicization of hacking and its significance.

Key words: electronic civil disobedience, hack, hacker, hacktivism, tactical media

Introduction

Surfacing controversies about WikiLeaks' contribution to Donald Trump's electoral triumph, the commuting of Chelsea Manning's sentence, or the ongoing Edward Snowden's persona-non-grata status highlight the notion of hacking in the modern world. Hackers were stereotyped as black hats, criminals, and cyberpunk hidden figures for a long time, until the media and popular culture emphasized the potential subversiveness in their actions as whistle-blowers and free software and open source (FOSS) activists. Nowadays, on the one hand, they more often tend to be depicted as the last men standing; maybe antisocial, but driven by the virtuous ideological motives of a desire for justice, patriotism, anti-globalist protests, a sense of freedom, etc. On the other hand, with their excellent coding abilities, they are a part of information warfare (IW), threatening the inner harmony of social life and protecting citizens' privacy. Film coverage of hackers and their tactics redistributes a paranoid and militarized vision of the world, with hidden figures often depicted either as a potential threat, or as survivors; either as a weapon in the fight against plutocracy, or as a technocratic nightmare.

"Hackers induce hysteria. They are the unknown, the terrifying, the enigma. The enigma that can breach and leak the deepest secrets (…). You feel vulnerable and it feels as though what happened is black magic"[1]; this quotation shows that the elaborate nature of hacking practice can cause its pathologization and even demonization. Rejecting such a perspective, this paper tries to locate hackers in a more neutral, objective discourse and to decode the biased opinions which fuel cinematic depictions of programmers pushing back the frontiers of technology. My case studies of movies together with real events and their media coverage are influenced especially by Tim Jordan's research on hacker culture, community, ethics, and political agenda. He describes hacking as the act of computer intrusion, but he simultaneously accentuates that this intrusion does not have criminal motivations—its core is a tech-savviness. A good hack is original and autonomous; an activity is more important than the results, it extends the regular computer usage and is made in a joyful atmosphere, but "[h]acking has become associated in the mass media with illicit computer intrusion rather than with innovative uses of technology. This has led to the definition of cracking, a term many hackers use to refer to unwanted entry

[1] Tor Ekeland, "Hacker Madness", *Limn* 8 (2017), https://limn.it/hacker-madness/, date accessed: 22 July 2017.

into computer systems by explorers or criminals".[2] This differentiation has led Jordan to distinguish three fundamental notions about hacking: "there is the hacker who breaks into computer systems; the hackers who write software; and hacking as the essence of twenty-first century creativity".[3]

Today hacking is often more of a cultural than a technological asset; it "is the way of understanding what is possible, sensible, and ethical in the twenty-first century"[4], therefore it becomes essential to decode its manipulated or simplified public image, especially with the ongoing progressive politicization of hackers and their significance. First of all, they are treated as a threat to social and private security due to the state engagement of hackers in cyberwar, IW and the sabotaging of other countries. Secondly, their actions are legally prohibited. Thirdly, hacking is by nature political due to its subversive use of media and reversing of power relations. And finally, hackers increasingly frequent collaboration with social activism has initiated hacktivism; hacking "turns into a form of 'warfare' (…) hackers engage in to advance their political agendas".[5] Jordan describes hacktivists as "political activists, most often associated with the alter-globalisation movement, who utilize hacking techniques to create grassroots activist political campaigns. Hacktivists produce both ephemeral electronic civil disobedience actions (…) and try to create infrastructures of secure anonymous communication often to support human rights workers".[6] So, hackers can be both agents of difference and change, and criminally-inclined "black hats" or crackers. Moreover, Hollywood cinema accentuates the tension between cyberterrorism and hacktivism; narratives fluctuate from these taking advantage of the militarization of cyberspace and paranoiac spirits (especially since 9/11) to redemptive ones that disclose corporate/state/elite conspiracies. Hence (cinematic) hacking seems to emerge as the avant-garde of militarized social space, its main weapon, and a fundamental defence. Pop culture feeds itself with this ambiguity as long as it accommodates the dualistic needs of its audience—a countercultural anti-hero becomes a scapegoat while a general sense of insecurity predominates.[7]

---

[2] Tim Jordan, *Activism! Direct Action, Hacktivism and the Future of Society*, (London: Reaktion Books) (2002), p. 120.

[3] Tim Jordan, "Hacking and power: Social and technological determinism in the digital age", *First Monday*, 14:7 (2009), http://firstmonday.org/article/viewArticle/2417/2240, date accessed: 22 July 2017.

[4] Tim Jordan, *Hacking: Digital Media and Technological Determinism*, (Cambridge–Malden: Polity Press) (2008), p. 1.

[5] Annika Richterich, Karin Wenz, "Introduction: Making and Hacking", *Digital Culture & Society* 3:1 (2017), p. 8.

[6] Tim Jordan (2009).

[7] This article describes Hollywood cinema and American cases of hacking due to the range of the phenomenon, but other countries with notorious hackers recreate their stories in pop culture, e.g. *23* (1998, Hans-Christian Schmid) and *Who Am I. No System Is Safe* (2014, Baran bo Odar) succeeded in German box office and *Deutschland 83* (2015–) is a national TV hit due to the fame of Chaos Computer Club and Klaus Koch.

They're stealing the Internet![8]

Hacking culture emerged in the 60s within American universities, but only two decades later did cinema find a formula for depicting computer geeks. In the 80s—with its hi-tech excitement, youth culture, and popularity of the IBM PC and other technological gadgets (e.g. the fetishized Power Glove[9])—the faith in information technology's limitless potential and the sense of overriding fun were all-pervading. Although in *Superman 3* (1983, Richard Lester), a hacker constructed a supercomputer in order to defeat the protagonist, coding had previously been used primarily as a tool of entertainment for movie characters (*Revenge of the Nerds* [1984, Jeff Kanew]; *Weird Science* [1985, John Hughes]). In *TRON* (1982, Steven Lisberger) Master Control's predatory needs were justified by the real-life villain's greed and in *Electric Dreams* (1984, Steve Barron) the PC and the protagonist were rivals over a woman. Even in *WarGames* (1983, John Badham) a military central computer appeared to be not maleficent but wrongly programmed. However, these optimistic narratives simplified hacking itself, presenting it as a movie gimmick rather than a process requiring professional skills. Depictions of hacking in 80s Hollywood cinema were often misunderstood and misleading. Repeating a random command such as "Access database" seemed to be sufficient for breaking into any system, thus making coding skills redundant.[10]

In the 90s modern angst emerged. There were still some gimmick hacks (as in *Jurassic Park* [1993, Steven Spielberg] or *Universal Soldier: The Return* [1999, Mic Rodgers][11]), sci-hack flicks (the absurd *The Lawnmower Man* [1992, Brett Leonard]) and genre recreation of hacking motives (for example, the corporate thriller *The Net* [1995, Irwin Winkler], comedy *Office Space* [1999, Mike Judge], and heist movie *Sneakers* [1992, Phil Alden Robinson]), but some Baudrillardist movies were

---

[8] Jerry Holkins, Mike Krahulik, "Penny Arcade", http://pennyarcade.wikia.com/wiki/July_16,_2007, date accessed: 1 April 2017.

[9] *Kung Fury* (2015, David Sandberg), an homage to the 80s poetics, had a wide web advertising, for example video *Kung Fury: Hackerman – How to Hack Time* in which we can find grid, computer disk ("First off you need a lot of ram... at least 256 kb" which is commented: "But remember – with great processing power came great responsibility") and even the Power Glove, a pre-haptic accessory for the Nintendo Entertainment System (https://www.youtube.com/watch?v=KEkrWRHCDQU, date accessed: 1 April 2017).

[10] One of the YouTube users commented accurately the compilation of the 80s hack flicks: "The fast track method to become an 80's computer hacker. You'll need... 1) - A can of Pepsi 2) - A poster of Michelle Pfeiffer on the wall 3) - A pair of Walkman headphones around your neck 4) - A nervous friend looking over your right shoulder 5) - A desk lamp ...Now type the words 'Access database'. Wait for the response 'Access denied', and simply reply with 'Override'. Congratulations, the world is now your oyster." 97channel, https://www.youtube.com/watch?v=rUGQHdYUIEo, date accessed: 1 April 2017.

[11] In *Universal Soldier: The Return* alleged supercomputer creating its army has a rather primitive way of communicate his rebellious nature: "Hello Dr. Cortner. I'm ready when you are. But, on the other hand… fuck you!"

indicative of the sense of paranoia: *Johnny Mnemonic* (1995, Robert Longo), *The Thirteenth Floor* (1999, Josef Rusnak) and especially *The Matrix* trilogy (1999, 2003 and 2003, The Wachowskis). Hackers began to be perceived as a threat for common citizens whose lives were affected by information technology to the point where it became an immanent element of their day-to-day reality. The Ashley Madison data breach,[12] the Sony Pictures Entertainment hack,[13] Silk Road's embezzlement,[14] or Celebgate[15] all are scandals which undermined cybersecurity and net neutrality.

Hackers—although they should be called crackers for their criminal inclinations— occurred as hidden figures thinking only about their profits and capitalizing on their digital supremacy by preying on the malfunctions of omnipresent technology. Moreover, cybercrime gangs and state-backed hackers[16] joined the information warfare (which is defined as a "conflict or struggle between two or more groups in the information environment"[17]). In the case of cyberwarfare particularly, computers and networks are main targets and are struck by cyberattacks, espionage (depicted and revealed in *Snowden* [2016, Oliver Stone] or *Jason Bourne* [2016, Paul Greengrass]), sabotage (the disruption of equipment which is shown in *Live Free or Die Hard* [2007, Len Wiseman] among others), or DDoS attacks (the Distributed Denial-of-Service attacks that finds their most iconic representation in *Hackers* [1995, Iain Softley]). In 2009, President Barack Obama declared America's digital infrastructure to be a "strategic national asset".[18] On the one hand, cyberwar is often safer and reduces losses in people and infrastructure, as was the case of the American attacks on Iraqi communications networks in the Gulf War. On the other hand, it encourages illegal actions. During the aforementioned war, Dutch hackers

[12] S. Kumar, "How Ashley Madison hack hurt everyone, not only cheaters", *Fortune*, http://fortune.com/2015/08/20/ashley-madison-hacks-cybersecurity/, date accessed: 1 April 2017. The case was mentioned in *Mr. Robot* by Michael whose wife asked for divorce after his romances had been disclosed.

[13] Andrea Peterson, "The Sony Pictures Entertainment hack, explained", *The Washington Post*, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.b7f9226e319d, date accessed: 1 April 2017.

[14] Nicole Hong, "Silk Road Creator Found Guilty of Cybercrimes", *The Wall Street Journal*, https://www.wsj.com/articles/silk-road-creator-found-guilty-of-cybercrimes-1423083107?mod=WSJ_hp_RightTopStories, date accessed: 1 April 2017. The scandal and other abuses connected with Dark Web were depicted in documentary *Deep Web* (2015, Alex Winter).

[15] Jason Meisner, "Chicago man plead guilty to 'Celebgate' photo hacking", *Chicago Tribune*, http://www.chicagotribune.com/news/local/breaking/ct-celebrity-photos-hacking-plea-met-20160927-story.html, date accessed: 1 April 2017.

[16] Danny Palmer, "What's the difference between state-backed hackers and cybercrime gangs? Nothing at all", *ZDNet*, http://www.zdnet.com/article/whats-the-difference-between-state-backed-hackers-and-cybercrime-gangs-nothing-at-all/, date accessed: 1 April 2017.

[17] Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, (Santa Monica–Arlington–Pittsburgh: RAND Corporation) (2013), p. XV.

[18] The White House, Office of the State Secretary, *Executive Order on Improving Critical Infrastructure Cybersecurity*, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0, date accessed: 1 April 2017.

stole information about U.S. troop movements from U.S. Defense Department computers and tried to sell it to the Iraqis, who thought it was a hoax and turned it down. Nowadays such an offer would be taken more seriously. Other threats are for example viruses and worms such as the infamous Stuxnet, "the world's first digital weapon",[19] which installed a rootkit on Windows OS. This was later believed to be an effect of American-Israeli cooperation against Iran's nuclear facilities.[20] As Eugene Kaspersky, founder of Kaspersky Lab, said, "[t]he term 'cyber-war' is used by many to describe the situation, but that term—which implies that there are two equal, known enemies duking it out—is outmoded. With today's attacks, you are clueless about who did it or when they will strike again. It's not cyber-war, but cyberterrorism".[21]

The threat seems ominous; therefore, in this situation hackers have commonly been criminalized, especially after the September 11 attacks, when the sense of paranoia became predominant. "Since 9/11, however, many liberal democratic states around the world have adopted legislation that '…paves the way for a far more permissive environment for electronic surveillance…', and the online surveillance of activist communities as a way of policing social movements and stifling political protest is a growing concern for activists under traditionally repressive regimes and in Western democracies alike."[22] The persecution of hackers, for example Fidel Salinas[23] and Jeremy Hammond[24], or Barack Obama's attitude towards Edward Snowden show a state-based hysteria about any hack regardless of its motivations.[25]

---

[19] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", *Wired*, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, date accessed: 8 April 2017. The cyberattack was depicted in documentary *Zero Days* (2016, Alex Gibney).

[20] Ellen Nakashima, Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say", *The Washington Post*, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.920c5dae260b, date accessed: 1 April 2017.

[21] David Shamah, "Latest viruses could mean 'end of world as we know it,' says man who discovered Flame", *Start-up Israel*, http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/, date accessed: 1 April 2017.

[22] Sonja Hohenbild, Shahriar Khonsari, Heather McMullen, and Kalea Turner-Beckman, "The Internet protection movement", *New Media Activism*, http://wpmu.mah.se/nmict11group4/the-internet-protection-movement/, date accessed: 8 April 2017.

[23] Andy Greenberg, "Hacker claims feds hit him with 44 felonies when he refused to be an FBI spy", *Wired*, https://www.wired.com/2015/02/hacker-claims-feds-hit-44-felonies-refused-fbi-spy/, date accessed: 8 April 2017.

[24] Jeremy Hammond, "Jeremy Hammond's Sentencing Statement", *Indymedia UK*, http://www.indymedia.org.uk/en/2013/11/513761.html, date accessed: 8 April 2015. His case and political agenda were shown in *The Hacker Wars* (2014, Vivien Lesnik Weisman).

[25] Jeff Mason, Mark Felsenthal, "Obama Disses Snowden, Says No 'Wheeling and Dealing' Or 'Scrambling Jets To Get A 29-year Old Hacker", *Business Insider*, http://www.businessinsider.com/obama-not-scrambling-jets-to-get-29-year-old-hacker-2013-6?IR=T, date accessed: 1 April 2017. China, not especially legitimate for respecting human rights itself, called hypocritical – Joe Mullin, "Obama says he can't pardon Snowden", *ArsTechnica*,

But whistle-blowers and hacktivists undermine the social trust in law and order, exposing state and media misuses: infiltration, invigilation, gatekeeping and hacking itself.[26] Moreover, as is written on the "Exposing the Invisible" webpage, "[p]eople are newly empowered to uncover hidden information, expose corruption and bring the truth to light",[27] taking advantage of their anonymity and subverting power relations.

Hack the planet!

Hackers are often more socially accepted, as represented by the popularization of hacking conferences (H.O.P.E., DefCon), makerspaces, Hackathons and the Internet Protection Movement. There are even training courses for hackers that end with the certificate of Ethical Hackers.[28] FOSS' flagship products—Firefox and GNU/Linux—"have both significant symbolic effects (in providing the ability of FOSS methods to create complex, stable programs) and market effects (providing significant alternatives of quality and freedom to commercial dominance)".[29] Hackers engage themselves in fighting for social change not only through free software and open source principles The threat posed on the digital freedom was an inspiration for acts of electronic civil disobedience (ECD).[30] More and more social activists appropriate the tactical media manifesto written by Geert Lovink: "Tactical media are media of crisis, criticism and opposition. This is both the source [of] their power, ('anger is an energy': John Lydon), and their limitation. Their typical heroes are the activist, nomadic media warriors, the prankster, the hacker, the street rapper, the camcorder kamikaze; they are the happy negatives, always in search of an enemy. (…) [C]onsumers use the texts and artefacts that surround us (…) 'tactically'. That is, in far more creative and rebellious ways than had previously been imagined."[31]

---

https://arstechnica.com/tech-policy/2016/11/obama-says-he-cant-pardon-snowden/, date accessed: 1 April 2017.

[26] One of the latest leaks applied to revealing CIA hacking tools: "VAULT 7: CIA Hacking Tools Revealed", *WikiLeaks*, https://wikileaks.org/ciav7p1/, date accessed: 1 April 2017.

[27] *Exposing the Invisible*, https://exposingtheinvisible.org/, date accessed: 1 April 2017.

[28] Rebecca Slayton, "The Paradoxical Authority of the Certified Ethical Hacker", *Limn* 8 (2017), http://limn.it/preface-hacks-leaks-and-breaches/, date accessed 22 July 2017. Slayton writes that CEH "sought to appropriate the technical savvy associated with hackers and the U.S. military and intelligence agencies while distancing itself from the untrustworthy and morally suspect image of hacking" but she also quotes Swartz's statement about CEH "alumns": "Some 'IT pros' may find a few techniques to secure against well-known attacks, but the underground is always 10 steps ahead."

[29] Tim Jordan (2009).

[30] Critical Art Ensemble, *Electronic Civil Disobedience & Other Unpopular Ideas*, www.critical-art.net/books/ecd, date accessed: 1 April 2017.

[31] Geert Lovink, "The ABC of Tactical Media", *nettime* (1997), http://www.nettime.org/Lists-Archives/nettime-l-9705/msg00096.html, date accessed: 1 April 2017.

Hacktivism can be understood as "activism! running free in the electronic veins that enliven our 21st-century, global socio-economies".[32] Digitally-founded social actions are "a qualified form of humanism"[33] and they aim to create the space for "netizens",[34] nevertheless hacking is conducted mainly by people with excellent coding skills who try to inspire social change by translating political thought into code. The most notorious groups in the United States are Anonymous and LulzSec. Julian Assange has been posting classified documents on WikiLeaks to call for "privacy of the weak, transparency for the powerful".[35] In 1996, the Critical Art Ensemble recognized the politicization of cybersphere. In 1998, the Electronic Disturbance Theatre shared FloodNet, which was a tool enabling acts of (electronic) civil disobedience. And in 1999, the CULT OF THE DEAD COW (cDc) launched the Hacktivismo group, whose main goal was fighting for access to information as an expression of human rights. The group explained their mission in "The Hacktivismo Declaration" and "The Hacktivismo FAQ". A few paragraphs from the latter should be evoked here as a representative of hactivists' goals and hacker culture:

> Q: What do you mean by the word "hacktivism", then?
>
> A: The provenance of hacktivism winds back to Omega – a longstanding member of the cDc – who started using it as a joke to describe on-line protest actions. Oxblood appropriated the word and began using it with a straight face; then many journalists, fading stars of the Left, and eventually script kiddies picked up on it, all claiming to know what hacktivism meant. It has been a noun in search of a verb for some time now. Oxblood once defined hacktivism as "an open-source implosion", and now he's added "disruptive compliance" to its range of description.
>
> Q: What the hell are you talking about? I'm just looking for a simple answer here.
>
> A: Hold your kimono, cupcake. O.K., hacktivism is the use of technology to advance human rights through electronic media.[36]

This short excerpt from cDc's FAQ emphasizes not only the mission and motivations of Hacktivismo and similar groups, but also their slightly anarchistic, ironic style, anonymity linked with peer recognition and alternate, partly hidden communicating platforms such as IRC. It is the "performance of technology"[37] that

[32] Tim Jordan (2002), p. 119.
[33] Geert Lovink (1997).
[34] The paradigm of DIY is substituted with DIWO – Do It with Others – which emphasizes common goals and inclusive operations.
[35] Julian Assange, *Cypherpunks: Freedom and the Future of the Internet*, (New York–London: OR Books) (2012), p. 7.
[36] CULT OF THE DEAD COW, *The Hacktivismo FAQ*, http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html, date accessed: 22 July 2017.
[37] Douglas Thomas, *Hacker Culture*, (Minneapolis–London: University of Minnesota Press) (2002), p. xx.

interested the movie industry. Hacking has an allure which spread not only among whitehats involved in cybersecurity or computer geeks, but also film producers. However, hackers are still stereotyped and treated as public enemies because of their abilities, common illicitness and anonymity symbolized by Guy Fawkes' mask.

Hollywood OS: bio-digital jazz[38]

"Most hackers do it for the challenge, thrill, and social fun. (…) [I]t [hacker culture] reconfigures technology and social relations by subverting the rules, laws, and social norms regarding the use of technology. It works in opposition to monopolistic, capitalist, statist regulation and perception of the new technologies."[39] Hacker culture, while maybe not as cyberpunk or cypherpunk as in *Hackers*, has risen from a vivacious cleverness and striving for intellectual challenges amongst students, especially from MIT. *The Social Network* (2010, David Fincher) is a contemporary movie that redistributes that sense of adventurous experiments with emerging technology. Hackers have their ethics inspired by the notions of information sharing, freedom of inquiry, unlimited availability of (digital) tools and democratic ideals, in sheer opposition to cybercrimes, cracking, and all black hat activities.[40] Simultaneously, media depictions of hacking are frequently unjust, although not always deliberately.

As Cory Doctorow from MIT Media Lab points out: "[t]he persistence until now [until the premiere of *Mr. Robot*, 2015–, series – M.S.] of what the geeks call 'Hollywood OS,' in which computers do impossible things just to drive the plot, hasn't just resulted in bad movies. It's confused people about what computers can and can't do. (…) The worst thing about *WarGames* [in which a teenager broke into NORAD's mainframe, nearly causing a nuclear escalation – M.S.] – and its most profound legacy – was the reaction of panicked lawmakers. (…) The CFAA took an exceptionally broad view of what constitutes criminal 'hacking,' making a potential felon out of anyone who acquires unauthorized access to a computer system".[41] Stephanie Schulte says that "the release of the film 'WarGames' helped merge Cold War anxieties with those involving teenage rebellion".[42] Relatively soon after its premiere, public opinion, IT specialists and lawyers were surprised by the so-called

[38] "It's a bio-digital jazz, man" is a quote from *TRON: Legacy*.

[39] Pramod K. Nayar, *An Introduction to New Media and Cybercultures*, (Malden–Oxford Chichester: Wiley-Blackwell) (2010), p. 100.

[40] At least in their literal, official meaning because hacktivists describe legal system as biased, corrupted, and serving elites.

[41] Cory Doctorow, "Mr. Robot Killed the Hollywood Hacker", *Technology Review*, https://www.technologyreview.com/s/603045/mr-robot-killed-the-hollywood-hacker/, date accessed: 1 April 2017.

[42] Stephanie Ricker Schulte, *Cached: Decoding the Internet in Global Popular Culture*, (New York–London: New York University Press) (2013), p. 28.

Morris worm (1988), but this was cinema itself that strengthened law related to cybercrimes, causing penalisation (and even criminalisation) of young programmers—as was evident during the Obama administration—and had its peak in Aaron Swartz's suicide after he was charged with thirteen felonies, the result of using his own script to download files from the JSTOR repository.[43]

Swartz's story was depicted emphatically in *The Internet's Own Boy* (2014, Brian Knappenberger). Modern documentaries are actually very committed to legitimatising hackers' actions, but mainstream Hollywood cinema is still abundant in iniquitous representations. Hack flicks distort the image of hackers, their personality and hacking itself, which is reduced to fast typing and simply playing a game (*Hackers*, *TRON,* or *Masterminds* [1997, Roger Christian]). Hackers use multiple windows whose abundance is representative of the hacker's skills; they talk with personified viruses,[44] they give nonsense explanations in which they merge random parts of IT vernacular[45] when locked in their mother's basement with a myriad of screens, wires and bobbleheads (provoking wisecrack comments from the old guard, like John McClane in *Live Free or Die Hard*). The sole process of hacking is compressed and reduced to erratic typing from which multidimensional visual data or Nmap graphics emerge in order to cover the boring truth about the nature of coding. Hollywood representations eliminate not only the wearisome writing of lines of illegible code, but also software and hardware parameters or social engineering that are necessary to gain access to most accounts. Hackers are not modern sorcerers, although their depictions show the contrary. One of the most frequent and absurd sentences in hack flicks is "Hack the mainframe!"[46], hackers have supernatural computer intuition (as Stanley in *Swordfish* [2001, Dominic Sena]) and they are often vindictive masterminds (which is the case of *Skyfall* [2012, Sam Mendes], *Untraceable* [2008, Gregory Hoblit], *GoldenEye* [1995, Martin Campbell], *Mission: Impossible – Ghost Protocol* [2011, Brad Bird] and so on). And even if they are shown in a more psychologically-motivated way, filmmakers annihilate realism with a high level of aestheticization. For example, in *Takedown* (2000, Joe Chappelle) the process of hacking is shown through multiple exposures in which the protagonist is merely

[43] Declan McCullagh, "From 'WarGames' to Aaron Swartz: How U.S. anti-hacking law went astray", *C-Net*, https://www.cnet.com/news/from-wargames-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray/, date accessed: 8 April 2017.

[44] In the 4th episode of *Mr. Robot's* season 1, few members of society watch *Hackers* which is criticised by Romero: "Hollywood hacker bullshit. I've been in this game 27 years. Not once have I come across an animated singing virus."

[45] For example, in *CSI: Cyber* (2015-2016) there is a very absurd dialogue: "I'll create a GUI interface using Visual Basic. See if I can track an IP address." "I'll distract her. You ping her IP." See also: Nick Cannata-Bowman, "Why 'CSI: Cyber' Fails in Terms of Accuracy", *The Cheat Sheet*, http://www.cheatsheet.com/entertainment/why-csi-cyber-fails-in-terms-of-accuracy.html/?a=viewall, date accessed: 1 April 2017.

[46] "You won't find the nuclear launch codes hidden in anything attached to Defense.gov" (Robert Evans, Caleb Eldon Brinkman, "5 Hacking Myths You Probably Believe (Thanks to Movies)", *Cracked*, http://www.cracked.com/personal-experiences-1262-5-hacking-myths-you-probably-believe-thanks-to-movies.html, date accessed: 1 April 2017.

engulfed by code. Similar poetics are used in *Hackers*, in which film characters' faces are changed into screens with mathematical equations on them. The film adds to that the transformation of New York into optical fibres and an embodied virus that is a half-naked man with long hair. And while *Blackhat* (2015, Michael Mann) tries to show code's architecture through a simple figuration of links, wires, optical fibres and electrical impulses, *TRON* and *TRON: Legacy* (2010, Joseph Kosinsky) create autonomous worlds on the grid where duels, races and power games take place. No wonder *Mr. Robot*, with its social engineering, legitimate use of IT tools and jargon (ShellShock bug, onion routing, tor networking, rootkit, etc.), or accurate representations of hacker culture (more realistic and down-to-earth than the cyberpunk universe developed in *Hackers*) has gained words of approval not merely from critics, but also from programmers, cybersecurity professionals, and even Anonymous.[47]

The image of computers as black boxes or magical crates is dangerous [48] and leaves viewers awed when confronted with someone who recognizes deep technological structures, especially in the age of total digitalization and web 2.0. Hackers could be depicted in an even more "analogue" way—as they are in heist movies (*Sneakers*, *The Italian Job* [2003, F. Gary Gray], *Swordfish*, or *Coin Heist* [2017, Emily Hagins]), where they are often only a small part of crooks' operations—but the black hat image remains. Hackers as antisocial, alienated, predominantly male[49] hidden figures seem to threaten society with their menacing invisibility and immanence (related to technological immanence itself). People's privacy is identified as being most vulnerable to cyber activity; hence the popularity of ghost hacking's motive has risen, resulting in such movies as *Ghost in the Shell* (1995, Mamoru Oshii, and 2017, Rupert Sanders), *Inception* (2011, Christopher Nolan), *Source Code* (2011, Duncan Jones) or even *The Lawnmower Man* and *Johnny Mnemonic*. The whistle-blowers' activities which exposed many state or corporate abuses of privacy were a turning point in the social image of hackers, or rather hacktivists. Their pursuit of

[47] Chancellor Agard, "Why USA Network's 'Mr. Robot' Is The Most Realistic Depiction Of Hacking On Television," *International Business Times*, http://www.ibtimes.com/why-usa-networks-mr-robot-most-realistic-depiction-hacking-television-2020213, date accessed: 9 April 2017. Sam Esmail hired many consultants (for example Michael Bazzell and Kor Adana) to help screenwriters with technological details. It can be seen in television that showrunners give much more attention to programming "anthropology." There are still TV series as *CSI: Cyber* or *Scorpion* (2014–), but next to them we can observe shows that depict computer environment with reverence – *Halt and Catch Fire* (2014–), *Sense8* (2015-2018), *Person of Interest* (2011-2016), and so on.

[48] The sense of insecurity is fuelled by narratives about the machines' rebellion – as in *The Matrix Trilogy*, *TRON* and *TRON: Legacy*, *WarGames: The Dead Code* (2008, Stuart Gillard) or *Storm Watch* (2002, Terry Cunningham) – and almost omnipotent antagonists who use advanced technological devices in simplified way - for example in *Live Free or Die Hard* the villain left all country in despair with two clicks, in *Eagle Eye* (2008, D.J. Caruso) the offender used an everyday technology to trace and monitor her victims, and even in *Sneakers* characters had an ultimate weapon for hackers – a universal key which can break into all software.

[49] *The Girl with the Dragon Tattoo*, based on first part of Stieg Larsson's trilogy, can initiate a new trend.

their own vision of justice, patriotism (as shown by Oliver Stone in *Snowden*) and freedom has gained them support as watchmen and as the last men standing.

Hackers with their subversive potential have become pop cultural icons, as is apparent in their biopics and cameos. Steve Jobs and Silicon Valley's moguls are not the only epitome of information technology because filmmakers depict net activists juxtaposing the open source movement[50] with the corporate establishment. *Takedown* tells the story of Kevin Mitnick. Although based on a book by Tsutomu Shimomura, Mitnick's main antagonist in real life, the hacker is shown ambiguously. This more understanding perspective was inspired by another book, *The Fugitive Game* by Jonathan Littman. Shimomura and Mitnick are shown as equal in skills and means, but with different goals. The first works for big corporations as a cybersecurity specialist, while the latter, although intrusive and invasive to the privacy of others, fights for freedom of information. The real Mitnick refused to acknowledge his crime as cracking and rather think of it as the effect of social engineering. He is now a white hat, a security consultant and pop cultural icon (appearing in Emmanuel Goldstein's documentary *Freedom Downtime* (2004) and Werner Herzog's documentary *Lo and Behold, Reveries of the Connected World* (2016) or as the inspiration for the main protagonist of the comic book *Wizzywig*). Edward Snowden (*Snowden*, *Citizenfour* [2014, Laura Poitras]) or Julian Assange (Australian *Underground: The Julian Assange Story* [2012, Robert Connolly], *The Fifth Estate* [2013, Bill Condon]) are other heroes of public interest who are followed by (for the time being, only in documentaries) stories about such hacktivists as Jeremy Hammond, Aaron Swartz and so on. Even without any real characters, movies recreate *Zeitgeist*, conspiracy theories, the sense of living in a tech-illusion, or just a deep contempt for the unseen mechanisms elaborated by corporations or states. It remains valid regardless of narrative structure. Popular types of characters include programmers and hackers working in big, exploiatative companies (e.g. *Antitrust* [2001, Peter Howitt]),[51] disadvantaged rebels using computer skills as their only weapon against elites (e.g. *The Girl with the Dragon Tattoo* [2011, David Fincher]), people treated as a tool in cybermanipulations and living in dystopias blurring the line between reality and VR (e.g. *The Matrix* trilogy but also the less obvious *One Point O* [2004, Jeff Renfroe, Marteinn Thorsson] and the already mentioned TV series *Mr. Robot*[52]).

Another popular narrative arc is old versus new, in which the old guard that can be called 'a Timex watch in a digital age', is confronted with digital era challenges. But this conflict is artificial and maybe even vaguely compensating. Popular culture

[51] Geert Lovink called them "the Army of Software" and appealed to them for rejecting Finazism (see: Franco Berardi, Geert Lovink, "A call to the Army of Love and to the Army of Software", *Net Critique*, http://networkcultures.org/geert/2011/10/12/franco-berardi-geert-lovink-a-call-to-the-army-of-love-and-to-the-army-of-software/, date accessed: 8 April 2017).

[52] Elliot's mental illness emphasises the schizoid character of modernity which is best depicted in the last episode of the first season – Elliott is standing in front of neon American flag in Times Square full of society supporters after talking with projections of his mind.

has begun to acknowledge the omnipresence of hacking and put it in the context of warfare. Unseen war is not only the set of tactics related to IW: nowadays hackers are a synecdoche of socio-political conflicts and predominant power dynamics.

References

Agard Chancellor, "Why USA Network's 'Mr. Robot' Is the Most Realistic Depiction of Hacking On Television", *International Business Times*, http://www.ibtimes.com/why-usa-networks-mr-robot-most-realistic-depiction-hacking-television-2020213, date accessed: 9 April 2017.

Assange Julian et al., *Cypherpunks: Freedom and the Future of the Internet*, (New York–London: OR Books) (2012).

Berardi Franco, Lovink Geert, "A call to the Army of Love and to the Army of Software", *Net Critique*, http://networkcultures.org/geert/2011/10/12/franco-berardi-geert-lovink-a-call-to-the-army-of-love-and-to-the-army-of-software/, date accessed: 8 April 2017.

Cannata-Bowman Nick, "Why 'CSI: Cyber' Fails in Terms of Accuracy", *The Cheat Sheet*, http://www.cheatsheet.com/entertainment/why-csi-cyber-fails-in-terms-of-accuracy.html/?a=viewall, date accessed: 1 April 2017.

Clarke Richard A., *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: HarperCollins) (2010).

Critical Art Ensemble, *Electronic Civil Disobedience & Other Unpopular Ideas*, www.critical-art.net/books/ecd, date accessed: 1 April 2017.

CULT OF THE DEAD COW, *The Hacktivismo FAQ*, http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html, date accessed: 22 July 2017.

Doctorow Cory, "Mr. Robot Killed the Hollywood Hacker", *Technology Review*, https://www.technologyreview.com/s/603045/mr-robot-killed-the-hollywood-hacker/, date accessed: 1 April 2017.

Tor Ekeland, "Hacker Madness", *Limn* 8 (2017), https://limn.it/hacker-madness/, date accessed: 22 July 2017.

Exposing the Invisible, https://exposingtheinvisible.org/, date accessed: 1 April 2017.

Evans Robert, Brinkman Caleb Eldon, "5 Hacking Myths You Probably Believe (Thanks to Movies)", *Cracked*, http://www.cracked.com/personal-experiences-1262-5-hacking-myths-you-probably-believe-thanks-to-movies.html, date accessed: 1 April 2017.

Ashley Gorham, "The Political Meaning of Hacktivism", *Limn* 8 (2017), https://limn.it/the-political-meaning-of-hacktivism/, date accessed: 22 July 2017.

Greenberg Andy, "Hacker claims feds hit him with 44 felonies when he refused to be an FBI spy", *Wired*, https://www.wired.com/2015/02/hacker-claims-feds-hit-44-felonies-refused-fbi-spy/, date accessed: 8 April 2017.

Hammond Jeremy, "Jeremy Hammond's Sentencing Statement", *Indymedia UK*, http://www.indymedia.org.uk/en/2013/11/513761.html, date accessed: 8 April 2015.

Hohenbild Sonja, Khonsari Shahriar, McMullen Heather, Turner-Beckman Kalea, "The Internet protection movement", *New Media Activism*, http://wpmu.mah.se/nmict11group4/the-internet-protection-movement/, date accessed: 8 April 2017.

Holkins Jerry, Krahulik Mike, "Penny Arcade", http://pennyarcade.wikia.com/wiki/July_16,_2007, date accessed: 1 April 2017.

Hong Nicole, "Silk Road Creator Found Guilty of Cybercrimes", *The Wall Street Journal*, https://www.wsj.com/articles/silk-road-creator-found-guilty-of-cybercrimes-1423083107?mod=WSJ_hp_RightTopStories, date accessed: 1 April 2017.

Tim Jordan, *Activism! Direct Action, Hacktivism and the Future of Society*, (London: Reaktion Books) (2002).

Tim Jordan, *Hacking: Digital Media and Technological Determinism*, (Cambridge–Malden: Polity Press) (2008).

Tim Jordan, "Hacking and power: Social and technological determinism in the digital age", *First Monday* 14:7 (2009), http://firstmonday.org/article/viewArticle/2417/2240, date accessed: 22 July 2017.

Kumar S., "How Ashley Madison hack hurt everyone, not only cheaters", *Fortune*, http://fortune.com/2015/08/20/ashley-madison-hacks-cybersecurity/, date accessed: 1 April 2017.

Lovink Geert, "The ABC of Tactical Media", *nettime*, http://www.nettime.org/Lists-Archives/nettime-l-9705/msg00096.html, date accessed: 1 April 2017.

Mason Jeff, Felsenthal Mark, "Obama Disses Snowden, Says No 'Wheeling and Dealing' Or 'Scrambling Jets to Get A 29-year Old Hacker'", *Business Insider*, http://www.businessinsider.com/obama-not-scrambling-jets-to-get-29-year-old-hacker-2013-6?IR=T, date accessed: 1 April 2017.

McCullagh Declan, "From 'WarGames' to Aaron Swartz: How U.S. anti-hacking law went astray", *C-Net*, https://www.cnet.com/news/from-wargames-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray/, date accessed: 8 April 2017.

Meisner Jason, "Chicago man plead guilty to 'Celebgate' photo hacking", *Chicago Tribune*, http://www.chicagotribune.com/news/local/breaking/ct-celebrity-photos-hacking-plea-met-20160927-story.html, date accessed: 1 April 2017.

Mullin Joe, "Obama says he can't pardon Snowden", *ArsTechnica*, https://arstechnica.com/tech-policy/2016/11/obama-says-he-cant-pardon-snowden/, date accessed: 1 April 2017.

Nakashima Ellen, Warrick Joby, "Stuxnet was work of U.S. and Israeli experts, officials say", *The Washington Post*, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.920c5dae260b, date accessed: 1 April 2017.

Nayar Pramod K., *An Introduction to New Media and Cybercultures*, (Malden–Oxford Chichester: Wiley-Blackwell) (2010).

Palmer Danny, "What's the difference between state-backed hackers and cybercrime gangs? Nothing at all", *ZDNet*, http://www.zdnet.com/article/whats-the-difference-between-state-backed-hackers-and-cybercrime-gangs-nothing-at-all/, date accessed: 1 April 2017.

Peterson Andrea, "The Sony Pictures Entertainment hack, explained", *The Washington Post*, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.b7f9226e319d, date accessed: 1 April 2017.

Porche Isaac R., III, Paul Christopher, York Michael, Serena Chad C., Sollinger Jerry M., Axelband Elliot, Min Endy Y., Held Bruce J., *Redefining Information Warfare Boundaries for an Army in a Wireless World*, (Santa Monica–Arlington–Pittsburgh: RAND Corporation) (2013).

Annika Richterich, Karin Wenz, "Introduction: Making and Hacking", *Digital Culture & Society* 3:1 (2017), p. 8.

Ricker Schulte Stephanie, *Cached: Decoding the Internet in Global Popular Culture*, (New York–London: New York University Press) (2013).

Shamah David, "Latest viruses could mean 'end of world as we know it', says man who discovered Flame", *Start-up Israel*, http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/, date accessed: 1 April 2017.

Rebecca Slayton, "The Paradoxical Authority of the Certified Ethical Hacker", *Limn* 8 (2017), http://limn.it/preface-hacks-leaks-and-breaches/, date accessed 22 July 2017.

The White House, Office of the State Secretary, *Executive Order on Improving Critical Infrastructure Cybersecurity*, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0, date accessed: 1 April 2017.

Douglas Thomas, *Hacker Culture*, (Minneapolis–London: University of Minnesota Press) (2002).

"VAULT 7: CIA Hacking Tools Revealed", *WikiLeaks*, https://wikileaks.org/ciav7p1/, date accessed: 1 April 2017.

Zetter Kim, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon", *Wired*, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, date accessed: 8 April 2017.