Hacker*

A: qurṣān aš-sifra. – G: Hacker. – F: hacker. –
R: chaker. – S: hacker. – C: heike 黑客

The rise of the computer leads to the emergence in capitalism of a novel formation of high-tech actors who ironically understate their virtuosity as simply >hacks< (**Levy** 2010, 10). – They appropriate the new forces of production through their further development and oppositional refunctioning, combining work, mode of living, ethics and sports into countercultures rebelling against corporate and state bureaucracies. The rule breaking and border crossing constitutive of hacking operate on the fringes of criminality and can in some instances cross this threshold as well. In turn, private and public security agencies can recruit hacker competency.

Hack – this denotes, among other things, >a waged scribbler, who hammers down line of text after line of text on his typewriter< (**Freyermuth** 1998, 30) – by the 1960s, it stood for a solution to problems facing electronics hobbyists and programmers at US universities, exhibiting three main characteristics: >1 Simplicity: the act has to be simple but impressive. 2 Mastery: the act involves sophisticated technical knowledge. 3 Illicitness: the act is ^against the rules^^< (**Taylor** 2005, 16). By linking together technical virtuosity and rule breaking (up to and including social rebellion), hackers of the 1960s and 1970s

* Originally published as *Hacker* in: *Historisch-kritisches Wörterbuch des Marxismus*, vol. 5: *Gegenöffentlichkeit bis Hegemonialapparat*, edited by Wolfgang Fritz Haug, Argument-Verlag, Hamburg 2001, col. 1115-1121.

made a decisive contribution to the development of new programming languages, the PC, and the Internet (**Raymond** 1999, 231 et sq.; **Gröndahl** 2000, 52 et sq.). Distinctive, mutually delimiting hacker cultures subsequently emerged, active in different fields and seeking to draw on the work culture of hacker pioneers.

1. *Digital Transgression*. – Computer networks spanning across enterprises also further sharpens the contradiction whereby the same technology in which top secret, complex knowledge for the sake of domination as well as sensitive medical data are locally concentrated also contain within them the possibility to inspect – and alter – this information from various points outside of a given enterprise. Here, the hacker emerges as >one of neoliberalism's new forms of individuality< (**Haug** 1999, 185) – the digital border crosser, transforming himself from the subaltern trespasser into the digital doppelgänger of a >legal< system user (such as by acquiring such a user's password). The hacker can appropriate the digital identities of many users of different systems through network exploration, his power of anonymous border crossing increases steadily. Roland **Eckert** et al. (1991) demonstrate to what extent hackers are fascinated by worldwide >data journeys< in which data are only inspected. There are also hackers who successfully look for the password of the >superuser< or >sysadmin< (the system administrator with access to highly sensitive files who decides who can access them, etc.). Insofar as hackers possess the necessary technical qualifications, they can manage to lock the legal sysadmin out of the system: >The pinnacle for every hacker is to achieve total control over the other network< (169).

As the hacker may have acquired several important passwords, the sysadmin will potentially neglect to eliminate his access immediately, finding it more important to trace the different digital trails of the hacker in order to identify the person itself. These dog fights can extend over months, and have spawned an entire literary genre (**Stoll** 1989).

The individuality form of the hacker as a >system intruder< reproduces itself in transnational High-Tech Capitalism on an ever-expanding technical scale due to the dynamic equilibrium of mutually constitutive learning between hackers and software industry programmers. New programs manage to plug previous security leaks, yet also contain new ones – not least because it is more profitable for the industry to sell a new product quickly, even with security flaws if necessary. When hacking activity turns these flaws into public scandals, new programs are issued to resolve them, but are (for example) often installed in enterprises at a delayed pace (**Taylor** 2005, 67 et sq.). Accordingly, less qualified hackers also manage to achieve spectacular successes, while qualified hackers analyse complicated systemic weaknesses. Furthermore, some computer scientists believe hackers to be particularly well-suited due to their practical-experimental approach (77).

Some hackers switch over to corporate security departments, found their own companies or become >samurai< hackers with specific professional ethics, renting out their services to illegal but legitimate aims (Raymond 1998, 396). Criminal organisations also seek to recruit hackers. The individuality form of the hacker which cultivates itself through the dedicated exploration of foreign systems can be incorporated into diverse political projects.

2. *Software-/Datapiracy*. – Prior to the internet age, a >cracker< and >demo< scene developed around groups which made a sport out of >cracking< the copy protection of new computer games and programs, inserting >^Intros^^ with sophisticated graphics and sound effects< (**Eckert** et al. 1991, 263) in front of them, and distributing them at no cost. The Internet provided this scene with newfound significance, as sales totalling in the billions hung in the balance. Electronic commerce means transforming products like music, books, movies, programs, etc. into digital products for the sake of digital distribution. They are expensive to produce, yet cost almost nothing to copy. For this reason, they along with the devices used to play them are reconfigured into digital commodities (such as through encryption), which only those who purchase them can access. 180 music and technology companies banded together in 1998 to form the >Secure Digital Music Initiative< (SDMI), yet its technology was already cracked by hackers in its planning phase. Some forms of particularly sophisticated copy protection (such as >dongles<) can only be cracked by >three or four crackers in the world< (McCandles 1997). Results of one's labour and the code name of the successful hacker and his group spread throughout the Internet.

Restoring general usability of digital commodities is the goal of the hacker as >cracker<, but hackers also ran ahead of capital and consolidated a new form of mass digital product distribution on the Internet (such as >Napster<); in some cases, they laid the groundwork for later profitable pathways, encouraging individual hackers to commercialise their capabilities. The >cracker< formation,

however, continually reproduces itself through the general labour of unlocking products of general labour >protected< from general use, or to utilise yet unlocked products before the chains of the commodity form are laid upon them (**Ohm** 2000, 731 et sq.).

The state intervenes in the wake of hacking's success. The Digital Millennium Copyright Act (DMCA) passed in the US in 1998 made the modification of >technological measures designed to protect copyrighted works< a punishable offense (with up to five years of imprisonment). European law pursued a similar orientation. – New contradictions emerge, as not only hacking but also computer science research into certain encryption technologies face the threat of repression.

3. *>Virus< Production*. – Computer viruses were initially developed by young people in the US in the early 1980s; the first global virus outbreak occurred in 1986; by 1987, a scene of virus programmers began to emerge (the so-called >Vx scene<); by the late 1980s, companies began producing anti-virus programs. Although most viruses circulated >only within the scene< and >only a marginal portion ever [infected] uninvolved computers< (**Röttgers** 2001, 63), the transition from sport to criminality is particularly evident in virus production. According to Sarah **Gordon**'s estimates, roughly 100 people in about 20 active groups regularly produced new viruses in 1994. Competition among and between groups is a central motivator behind virus programmers, although some – anonymously – >release< viruses. This brutality is potentiated by the Internet, as a successfully circulated virus can irrevocably destroy millions of users' data.

The Internet is also the medium by which a technically unqualified hacker today can download entire virus assembly kits; it thereby functions as a multiplier of the lethal capabilities of a small number of virus programmers. That youthful hackers who themselves use computers acquire destructive viruses and allow them to circulate may be related to formation-specific moments of the process by which hackers work themselves into the hacking >subject form<. Appropriation of technical capability often occurs as ^dismantling^^ (Zerspielung) (**Wulff** 1987) of reality: on one hand, hackers in the making appropriate through PC and Internet usage enormous technical and cooperative know-how at a young age; on the other, the world of computer games – thematically and dramaturgically constructed by the gaming industry as a substitute for reality – alters perception of reality. The sneaking into foreign computer networks, the battle with the sysadmin, destroying data he administrates, is a kind of continuation of computer battle games in the style of >reality TV<. In children's and young adult literature there is a common recourse – not necessarily illusionary – to the actions of young hackers combining the hunt and battle against destruction: seven 10–16-year-old cyberkids cooperate via Internet across continents against a virus producer (**Balan** 1999). – State actors seeking to combat hacking activity with the legal system face the dilemma that many hackers are children and young people and thus not liable to punishment.

4. *Software Development*. – Hackers who consciously identify as such and thus draw on the traditions of the technologically ground-breaking hackers of the 1960s and 1970s join together into a globally networked collective worker in a core area of transnational high tech-capitalism

on the basis of unpaid labour, encompassing more people than the largest software company, Microsoft, and develop the open-source software operating system Linux. Many reasons are given for the prospective superiority of these hacker collections of the Linux type (**Raymond** 1999). – It is possible that this form of non-capitalist software development will assert itself worldwide, as software development has developed into a form of general labour which requires forms of self-socialisation incompatible with – even radically modernised – capitalist production regimes. For Linux hackers, only their new mode of production is compatible with their sense of producer pride, making them productive as producers, as the programs (and the names of their authors) are published on the Internet and made available for further critical development. – That said, transnationally operating hightech capitalism is not threatened in its existence if the development of productive forces in important sectors occurs in a non-capitalist fashion.

5. *>Hacktivism<*. – The concept is formed through the contraction of the words >hack< and (political) >activism<, that is, the use of hackers' technical capabilities for political projects. One of the goals is to utilise the medium of the Internet as public space against privatisation and other strategies of enclosure, that is to transpose the freedom of assembly and demonstration once asserted for public spaces prior to the Internet's emergence as electronic public space, by construing structural analogies to sit-ins and blockades. Here, network-technical competence is needed alongside political networking capacity. According to Stefan **Wray** (1998), enthusiasm for political projects increasingly emanates

from technically-oriented hackers. One such group, the Electronic Disturbance Theater (EDT), organised virtual sit-ins against Mexican government websites in support of the Zapatistas: those involved used a program to leave a critical message at the target server every several seconds. Should enough internet surfers participate, the server can no longer be accessed from outside. A group in Britain inspired by EDT are the Electro-Hippies, who reject clandestine actions and work on further developing protest forms and are less interested in disabling a target server so much as activating as many people as possible to engage in spontaneous participation. – To what extent the disturbance of communication flows on the Internet is politically wise, given that the opposing side can also utilise this weapon, is highly controversial among hacktivists.

Unlike hacktivism, the goal of cyberterrorism (Dorothy **Denning** 2001) is to cause catastrophes and kill people through network attacks. To the extent it can, the US military has been working on a concept for Cyberwarfare for ten years, while a plethora of further states have begun working on this model of warfare since.

6. *Hacking-Ethic(s)*. – Processes of self-socialisation, that is, the diversion of young hackers' aggressive labour energies towards projects of recognisable civil-social value, are initiated by hacker associations such as the Chaos Computer Club (CCC). The CCC's hacking conferences, for example, always feature >sessions< in which respected hackers from the hacking world urge >script kiddies< to become >real hackers< – such as by not attacking institutions with which they disagree. (Relevant literature for young people such as Bruce **Balan's** *Cyber.KDZ* series

follows a similar perspective). – The CCC was founded in West Germany in the early 1980s and operates today as an umbrella association, in which many hackers across Germany have convened. The group developed a widely accepted hacker code of ethics, the first imperative of which stipulates: >Access to computers - and anything which might teach you something about the way the world really works - should be unlimited and total.< In light of prevailing social relations, this ethics is simultaneously a manifesto for breaking through the secrecy of the capitalist state.

A central topic of CCC congresses is uncovering the technical weak points of computer networks, which is only possible through practical-experimental approaches, and presenting their findings to the public. These also reveal possible points of entry for computer criminality, which exploits such weak points and can always rely on the discretion of affected companies and authorities. In this sense, the investigative work of the CCC and the hackers organised under its umbrella is socially indispensable. – The terror attacks of 11 September 2001 served as the pretext for introducing new forms of electronic citizen surveillance, which in turn has created a new civil-socially relevant sphere of activity for the CCC and the hackers gathered in it.

Bibliography

B.**Balan**, *Cyber.KDZ 1: In Search of SCUM*, New York 1997; id., *Cyber.KDZ 2: A Picture's Worth*, New York 1997; id., *Cyber.KDZ 3: The Great NASA Flu*, New York 1997; D.**Denning**, >Cyberwarriors. Activists and Terrorists Turn to Cyberspace<, *Harvard International Review*, vol. 23, 2001, no. 2, 70-5; R.**Eckert** et al., *Auf digitalen Pfaden. Die Kulturen von Hackern, Programmierern, Crackern und Spielern*, Opladen 1991; G.S.**Freyermuth**, *Cyberland. Eine*

Führung durch den High-Tech-Underground, Hamburg 1998; S.**Gordon**, >The Generic Virus Writer<, *Proceedings of the International Virus Bulletin Conference*, Jersey, Channel Islands 1994, 121-138; B.**Gröndahl**, *Hacker*, Hamburg 2000; id., >The Script Kiddies Are Not Alright<, Medosch/Röttgers, 2001, 143-52; W.F.**Haug**, *Politisch richtig oder Richtig politisch. Linke Politik im transnationalen High-Tech-Kapitalismus*, Hamburg 1999; S.**Levy**, *Hackers. Heroes of the Computer Revolution* (1984), Sebastopol, CA 2010; D.**McCandless**, >Warez Wars<, *WIRED*, 4 January 1997; CCC (Chaos Computer Club), *Hacker Ethics* (n.p., n.d.); A.**Medosch** and J.**Röttgers** (eds.), *Netzpiraten. Die Kultur des elektronischen Verbrechens*, Hannover 2001; C.**Ohm**, >Hacker – das Ethos der neuen Kämpfe im Internet-Zeitalter<, *Argument* 238, vol. 42, 2000, 720-40; E.S.**Raymond**, *The New Hacker's Dictionary*, 3rd ed., Cambridge 1998; id, *The Cathedral & the Bazaar. Musings on Linux and Open Source by an Accidental Revolutionary*, Beijing-Cambridge 1999; J.**Röttgers**, >Sie lieben uns.txt.vbs<, Medosch/Röttgers, 2001, 53-72; P.-A.**Taylor**, *Crime in the Digital Sublime* (1999), New York 2005; *Telepolis, Elektronische Zeitschrift*, www.heise.de/tp; S.**Turkle**, *The Second Self. Computers and the Human Spirit* (1984), Cambridge, MA 2005; C.**Stoll**, *The Cuckoo's Egg. Tracking a Spy Through the Maze of Computer Espionage*, New York 1989; S.**Wray**, >Die Umwandlung des Widerstands der Maschinenstürmer in einen virtuellen Widerstand – Die Herstellung eines World Wide Web des elektronischen zivilen Ungehorsams<, *Telepolis*, 5 May 1998; E.**Wulff**, >Zementierung oder Zerspielung. Zur Dialektik von ideologischer Subjektion und Delinquenz<, *Fremde Nähe. Festschrift für Erich Wulff*, edited by W.F.**Haug** and H.**Pfefferer-Wolf**, Hamburg/West Berlin 1987, 171-212.

Christof Ohm

transl. by Loren Balhorn

--> Appropriation, Collective Worker, Counter-Power, Counter-Public, Destructive Forces, Development, General Labour, High-Technology Mode of Production, Immaterial Labour, Individuality Form, Internet, Neoliberalism, Play, Power, Private Property, Productive Forces/Relations of Production, Security, Self-Determination, Subject, subversive, technical development/technical revolutions, Zapatismo

--> Allgemeine Arbeit, Aneignung, Destruktivkräfte, Entwicklung, Gegenmacht, Gegenöffentlichkeit, Gesamtarbeiter, hochtechnologische Produktionsweise, immaterielle Arbeit, Individualitätsform, Internet, Macht, Neoliberalismus, Privateigentum, Produktivkräfte/ Produktionsverhältnisse, Selbstbestimmung, Sicherheit, Spiel, Subjekt, subversiv, Technikentwicklung/technische Revolutionen, Zapatismus