On Hacking Cultures
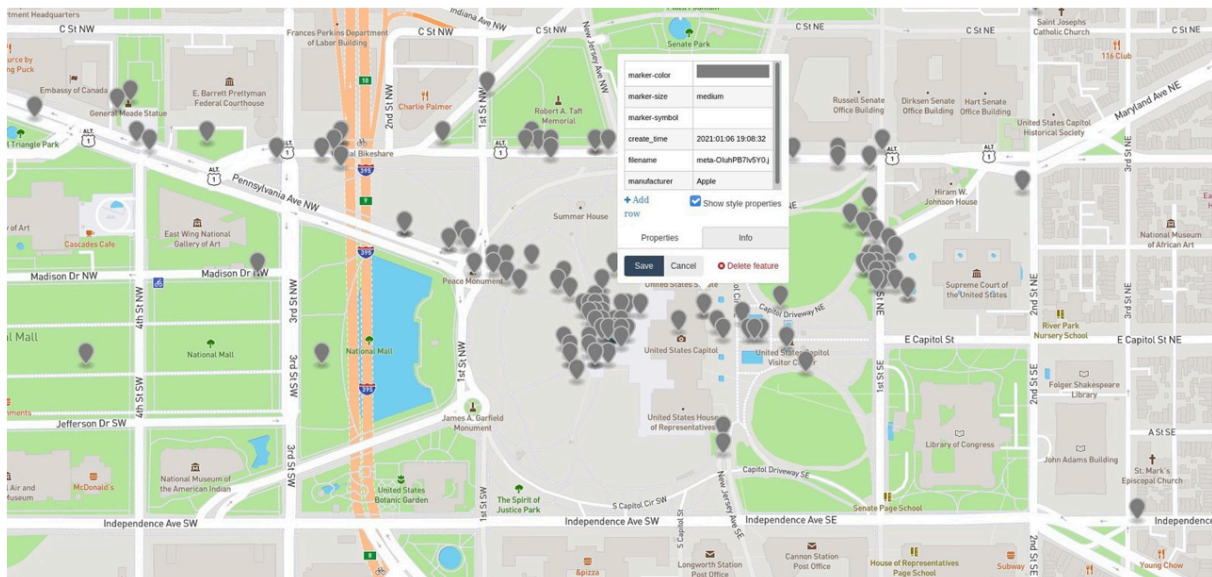
Alexander Matthias Gerner, CFCUL

amgerner@fc.ul.pt

Summerschool: Hacking- Technical Practice and Cultural Meaning

Darmstadt, 20-24.9.2021

SOME OF THE PLOTTED PARLER GPS DATA. IMAGE: MOTHERBOARD

*

On Wednesday, 6 Jan. 2021, an incited mob stormed the US Capitol in Washington, resulting in 5 death. Only days later, a small group of hacker archivists such as *donk_enby* [1](CrashOveride) (Nally, 2021) scrapped "(o)nly things that were available publicly via the web" @donk_enby from the non-secure (via an "insecure direct object reference") app *Parler* -between *Twillio* dropping *Parler* as a costumer and the consequent disabling of their two-factor authentication - and before it was de-platformed by *Amazon Web Service*, and thrown out of *Google Play* and *Apple App Store* and uploaded all publicly accessible information of that day and place to the www so that this archiving "allows analysts to extract the EXIF metadata from photos and videos uploaded to the social media site en masse and to examine specific ones that were taken at the insurrection on Capitol Hill." (Coebler & Cox, 2021). This hacktivist action was justified as follows: "I saw what online disinformation could do first hand ...I hope to inspire people like me to use their skillset for political purposes - hacking IS political,(...) we've been slipping down a slippery slope that got us to what happened on Wednesday for a very long time." Against the reading of hacker as mere deployers of bots or destroyers of infrastructures of hacker

---

[1] https://twitter.com/donk_enby

states (Follis & Fish, 2020) a whistleblower culture (Snowdon 2019, Assange 2018) is debated today-despite persecution and legal offenses that intruders face- as the cybersecurity[2] dilemma (Buchanan, 2016; 2020). Webb (2020) not only interprets hackers as vital disrupters, but as well as citizens that invent and build out new forms of distributed, decentralized democracy in the digital age and into cyberspace while we are being confronted with powerful technological mass surveillance and rising authorianism enabled by new technology and hacker ethics that may push for exploiting the weakness in computers and systems of the powerful in the sense of Hackers Ethics: "Privacy for the weak, transparency for the powerful" (Anderson, 2020; Assange et al., 2012).

<p align="center">*</p>

Hacking as performing Technology - Method of Hacking

Hacking can be understood as a method of probing and investigation in a sense initially proposed by P.R. Samson[3], of an unconventional application of technology that may enhance the potential of human experience by multiplying its energy, by transforming its habitual uses to open up new perspectives of interacting with and becoming an "Other." Hacking as "the performance of technology" (Douglas, 2002) should heed performance metaphors in the philosophy of technology (Coeckelbergh[4] 2019) that include *re*-booting or *re*-arranging and transforming how machines and technology stage our thinking and mold our language games and choreograph our knowledge, social engineering[5], and our access (passwords) to how by hacking into technologies we may be able to act, think and share knowledge differently. Hacks do not only explore pre-given rules and territories but as well show *acts of user rebellion* (transgression of game rules) and thus imply re-appropriation of activity in augmentations of technical, social, and political affordances, that today ask as well how a person became a user in the first place (McNeil[6], 2020) and how to change our "Use-Age" (Fassler[7], 2020) in a time of necessary (climate) change of habits (green hacks).

---

[2] " Hacking is in a persistent state of flux. It is pervaded by normative and legal ambiguities surrounding the status of the practices, software, artifacts, and actors that operate in this field. Not only do actors in the digital sphere have different rights and responsibilities under the law, but the relationships, processes, technologies, and practices that produce the cybersecurity foundations of our collective digital reality are also poorly understood, undercodified, decentralized, and piecemeal." (Follis & Fish, 2020: 78)

[3] "**Peter Samson** MIT Hacker (on of the first), who loved systems, trains, TX-0, music, parliamentary procedure, pranks, and hacking.(...)Just why Peter Samson was wandering around building 26 in the middle of the night is a matter that he would find difficult to explain. Some things are not spoken" Levy (2010),xiv-3

[4] Coeckelbergh, M. (2019). *Moved by machines. Performance Metaphors and Philosophy of Technology*. New York: Routledge.

[5] "Social Engineering:n. Term used among crackers and samurai for cracking techniques that rely on weakness in wetware rather than software"Hacker´s Jargon Dictionary cit. in Douglas (2002:61)

[6] McNeill, Joanne (2020). *Lurking. How a person became a user.* New York: MCD Books.

[7] Fassler, Manfred (2020). *Partizipation ohne Demokratie. Über die Folgen der Netz- und Geopolitik von Facebook, Google, Amazon & Co*. München: Wilhelm Fink.

*

Hacking is *a way of doing things*, technically, ethically, aesthetically, and politically. Hackers have been differently looked upon in history in their cultural function as "creative problem solving" (Erikson, 2007) and criticized equaled with postmodern intellectuals as mere *crackers of code* (Dirk Becker[8] 2008), or as counterculture[9] such as the *Algorithmic Justice League[10]* aligning art, AI with justice that besides being educated in the Silicon bay area, their impact of action go way "beyond the Valley" (Srinivason[11], 2020). Some call hacking a sublime art to discover how things are made and break them up to transform them. Engineering, Tinkering, and Hacking as methods and media of reverse-engineering (Friesinger & Herwig 2014) are related. Hacking could be described as a method of *tinkering* with stuff (the brain[12], bodies, computers, programs, phones, or musical instruments, among others) and systems (information distribution, circuits, habits, rules, political) and DIY forms of living (status quo, life[13], programmed sociality) often going *against* the grain of pre-programmed *technological determinism*.

*

By Hacking, we play games with technology in between subversion and stabilization of rules: A hack does not only produce a particular "rush of functionality" (Pias 2014: 149) to fulfill a constructive goal- such as taking down an opponent in a game (pawn) but as well "wild pleasure taken in mere involvement" (Levy 1984, cit. in Pias, 2014: 147) or following a sci-fi vision of the future (cf. Milburn, 2018). Pias (2014) pinpoints two motifs in the early history of hacking a) subversion (offense) with a certain emancipatory potential for unknown applications of its users to play around b) stabilization (defense) to demarcate and shield information and knowledge as someone's (states, companies, public) property in which Hacking even can be defined as in the case of the *Chaos Computer Club* (CCC) as a "community service with non-profit purpose" (Ibid., 153) in which in a first wave of hackers in the US hands on imperative and a hackers ethos was started as a vision that "access to computers and

---

[8] Baecker, Dirk: Intellektuelle I, in: Nie wieder Vernunft. Kleinere Beiträge zur Sozialkunde, Heidelberg: Auer 2008, S. 74-81

[9] Himanen, P., Torvalds, L. and Manuel Castells (2001). The Hacker Ethic: And The Spirit of the Information Age. New York: Random House 2001

[10] https://www.ajl.org

[11] Srinivasan, R. (2020). Beyond the valley. *How innovators around the world are overcoming Inequalityand creating the Technologies of tomorrow.* Cambridge, Mass. The MIT Press.

[12] Dresler, M., Sandberg, A., Bublitz, C., Ohla, K., Trenado, C., Mroczko-Wąsowicz, A., . . . Repantis, D. (2018). Hacking the Brain: Dimensions of Cognitive Enhancement. *ACS Chemical Neuroscience,10*(3), 1137-1148. doi:10.1021/acschemneuro.8b00571

[13] cf. Reagle, Joseph (2019). Hacking Life. Systematized Living and its discontents. Cambridge Mass.: MIT Press

anything that teaches you how the world works should be unlimited and total.[14]" (Levy 2010: 28; cf. Webb 2020: 1-32).

<div align="center">*</div>

Hacking Humans? - Edit yourself!

The relation between *hacking* and *cyberpunk, grinders* and its derivates (e.g., Assanges Cypherpunk), that advocate using technology to improve natural human capabilities as well as the relation between cyborgs (Harraway's Cyborg manifesto and Neill Harbinson) and biomedical Hacking and enhancing will be treated in the Summerschool.

Against Big Science projects and their methods of corporate science, bodyhacks and biohacks of DIY synthetic biologists[15] seem to be an opposed view on how to apply an open concept and hack into closed and "safe" science and technology spaces such as biohazard risk protected labs such as the development of a Covid-19 vaccine[16]. In relation to the technology of exact genome editing by CRISPR-Cas9 and similar techniques, a DIY Biohacking community puts up against unlawfulness. Starter kits- as we know from chemistry, starter kits for school children with basic notions about CRISPR tools are being marketed on the internet, such as DIY Bacterial Gene Engineering CRISPR Kit[17].

Harari proposes that in our present time, humans have become the "*hackable animal*" (HARARI, 2018b)[18], much in the sense that Elon Musk (Fourneret[19], 2020) envisions our brains to be connected to the internet. The growing importance of biocybernetics leads to increased hackability of embodied human beings even if by non-invasive wearable near-body technologies that change and hack into our body schema (Tajadura- Jimenez[20] et al., 2020) implies prediction, control, persuasion, and

---

[14] besides: "2. All information should be free(....)3. Mistrust authority. Promote decentralization (...) 4.Hackers should be judged by their hacking, not by bogus criteria such as degrees, age, race or position (....)5 You can create art and beauty on a computer (...) 6 Computers can change your life for the better(...)"Levy (2010: 28-34)

[15] cf.: https://www.ted.com/talks/ellen_jorgensen_biohacking_you_can_do_it_too

[16] "Josiah Zayner's plan was simple: replicate a Covid-19 vaccine that had worked in monkeys, test it on himself and then livestream the experiment online over a period of months. Now, that improbable bid is over."
Brown , C.(2020, Oct.10) "Home-Made Covid Vaccine Appeared to Work, but Questions Remained". Bloomberg Retrieved online 11.1.2021: https://www.bloomberg.com/news/articles/2020-10-10/home-made-covid-vaccine-appeared-to-work-but-questions-remained

[17] https://www.the-odin.com/diy-crispr-kit/

[18] Cf. Harari (2018b): "In order to survive and prosper in the 21st century, we need to leave behind the naive view of humans as free individuals – a view inherited from Christian theology as much as from the modern Enlightenment – and come to terms with what humans really are: hackable animals. We need to know ourselves better." cf. "The most important thing to know about the 21st Century is that humans are becoming hackable animals (...) How to live in a world where human beings can be hacked? How to protect democracy and the very meaning of human life when a computer algorithm could know us better than our mothers do? That's the most complicated challenge your generation faces." (HARARI, 2020)

[19] Fourneret, E. (2020) "The Hybridization of the Human with Brain Implants: The Neuralink Project", *Cambridge Quarterly of Healthcare Ethics (2020), 29*, 668–672.

[20] Tajadura-Jiménez A, Väljamäe A and Kuusk K (2020) Altering One's Body-Perception Through E-Textiles and Haptic Metaphors. *Front. Robot. AI 7:7*. DOI: 10.3389/frobt.2020.00007

deceptive as well as non-deceptive manipulation of what people do, how people decide and vote for, how people act, and how people feel towards themselves and others as social beings. Bucher (2018) speaks of programmed sociality and xx in re-engineering humanity in algorithmic rationalities that influence the constitutive levels of self-and personhood as, in post-human visions of experience engineering (Olaf Blanke) in which we can use Neuro-inspired embodiment and multisensory teleportation employing Virtual and Mixed Reality technology (Robotics/Haptics; critical: Madary &Metzinger[21] 2016) technically induce out-of-body experiences by robot and electromagnetic stimulation of the body and the brain. Brain-to-brain interfaces hack the autonomy in playing a video-game remotely by manipulating the hand to a mouse-click of another person. Optogenetics lets mice be remote controlled and hack into the emotions they feel.

*

Second-wave Hackers, including the GNU manifesto from 1985 and the *free software foundation,[22]* worked on distribution and access to free (system[23]) software and code and the *right to repair[24]* to the people. As a result of this, volunteer communities and social movements of not only DIY but as well open access movement and citizen science entanglements of maker and hacker cultures (Richterich et al., 2017) should be distinguished from Hackerspaces[25] despite sharing with Maker Labs a particular *way of doing,* but are less linked to leisure or any (pre-) startup industrial fabrication.

Besides *phreaking* and *exploit* or security measurements to counter-hack certain crackers, Hacking has a strong relation to art and music. Landwehr (2014) underlines the *interference with a system* as an artistic strategy, for example, in *The! Mediengruppe Bitnik.* For Kuni (2014: 194), starting with hardware hacking is about "manipulations, transformations and unconventional redesign of technical appliances which contain both analog-electronic as well as digital components." Heed Faubel (2020; 2016) - in the tradition of Collins (2018) and hardware music hacking- who works on the interface of performance art and sound hardware avoiding protocols by non-digital synchronization sound hacks

---

[21] Madary, M. and Metzinger, T. (2016) Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology. *Front. Robot. AI* 3:3. doi: 10.3389/frobt.2016.00003
[22]https://www.fsf.org/blogs/community/watch-fight-to-repair-demand-the-right-to-repair?mtm_campaign=frsfall2020&mtm_source=ftrvidpage "The FSF's campaigns target important opportunities for free software adoption and development, empower people against specific threats to their freedom, and move us closer to a free society."
[23] here: the GNU/Linux operating system
[24] "to support right to repair initiatives around the world, and warn against the day-to-day use of proprietary software in hardware as diverse as self-driving cars, printer cartridges, and "smart" home assistants." https://www.fsf.org/campaigns/campaigns-summaries#ftr
[25] "*Hackerspace* is roughly interchangeable with *hacklab*, *makerspace*, or *hackspace*, though connotations vary. See Davies 2017a, 2017b; Maxigas 2012; Toupin 2015. Makerspaces in particular may share an ethos of democratized fabrication, but they ultimately boil down to leisure and lifestyle, at quite a remove from more radicalized strands of hacking and hacktivism (see Davies 2017a, 2017b)."Dunbar-Hester (2020:41, note 45)

that re-value the analog concerning the digital by social and systemic synchronizations[26], resonances and oscillations. Hacking sounds and musical instruments by sampling, creating sonic forms of resistance of the overheard or different use of preexisting sound-producing technology by parasitic noise (Michel Serres).

*

Hands-on Imperative!, DIY, Hardware Hacking,

Game Hacks, Music hacking, sampling, and AI tinkering

Hacking face-recognition: In her work "Face Detection," JOHANNA REICH explores the relationship between man and machine in the digital age. In front of a smartphone camera with face detection, she forms clumps of clay until they were recognized by the smartphone's facial recognition program as humans. At the point of recognition, she stops forming. When does the human appear? When does it disappear? Has hacking into automated facial analysis[27] in facial recognition biases (BUOLAMWINI[28] & GEBRU, 2018) *coding with a white mask* helped change the policy of using AI Face recognition to hack for inclusion *politics* (Dunbar-Hester, 2020)? How about the Surveillance Hackers of Hong Kong that go against the hyper-controlled and ubiquitous algorithmic control of permanent face screening and automated decision-making by strategies of obfuscation, camouflage, mimesis - and we could add aesthetic principles such as leaps- to distract or deviate the ubiquitous algorithmic rationality of programmed attention of systematic data collection and analysis as well as value attribution such as by the Chinese Social Credit System (cf. Gerner, 2020).

---

[26] "Synchronization is the most fundamental indicator for the exchange of information. In these analogue oscillators this exchange is realized through a direct coupling, no encoding and no decoding has to be effectuated. Not one oscillator is dominating the communication, they mutually negotiate their timing. This capacity for non-hierarchical communication is a signature of analogue systems. They allow for information exchange without having to recur to symbols or to detect the presence of a signal, already the softest input may modify and modulate the behaviour of an analogue system." Faubel, C. (2016) Machine- machine communications without hierarchies and protocols. coax

[27] Buolamwini, J. (2020). Automated Facial Analysis. *Definitions*. doi:10.32388/8kwdxw

[28] The EU created an ethical AI label for EU companies. In its white paper of the European Commission (EU; 2020: 11) quotes Buolamwini & Gebru (2018): "Certain AI programs for facial analysis display gender and racial bias, demonstrating low errors for determining the gender of lighter-skinned men but high errors in determining gender for darker-skinned women." Buolamwini, J., Gebru (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, *Proceedings of machine learning research*, 1-15.

Basis texts:

Hacker/ Hacker-culture/ conceptual history / Hacktivism/ Cypherpunk

Anderson, Patrick D. (2020). Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange. *Ethics and Information Technology* https://doi.org/10.1007/s10676-020-09571-x

Assange, J. (2016). *When Google met WikiLeaks*. New York: OR Books.

Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2012). *Cypherpunks: Freedom and the future of the internet*. New York: OR Books.

Avila, R., Harrison, S., & Richter, A. (2017). *Women, whistleblowing, WikiLeaks: A conversation*. New York: OR Books.

Buchanan, B. (2016). *The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations*

Oxford: OUP.

Buchanan, B. (2020). *The Hacker and the State. Cyberattacks and the new normal in geopolitics.* Cambridge Mass.: Harvard University Press.

Coleman (2013). *Coding Freedom. The ethics and aesthetics of Hacking*. Princeton University Press; Illustrated edition (30 Jan. 2013)

Collins, N. (2018). *Handmade electronic music. The art of hardware hacking*. New York/ London: Routledge.

Davies, Sarah R. (2017a). "Characterizing Hacking: Mundane Engagement in US Hacker and Makerspaces." *Science, Technology, & Human Values*. https://doi.org/10.1177%2F0162243917703464.

Davies, Sarah R. (2017b). *Hackerspaces: Making the Maker Movement.* Malden, MA: Polity Press.

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

Düllo, Thomas, Liebl, Franz (Eds.) (2005). *Cultural Hacking. Kunst des strategischen Handelns*. Wien/New York: Springer.

Dunbar-Hester, Christiane (2020). *Hacking Diversity. The Politics of Inclusion in Open Technology Cultures.* Princeton/ Oxfordshire Princeton University Press.

Follis, L. & Fish, A (2020). *Hacker States*. Cambridge Mass.: MIT Press.

Friesinger, G., Herwig, J. (eds.) (2014). *The Art of Reverse-engeneering. Open - dissect-rebuild.* Bielefeld: transcript.

Gerner, A.M. (2020). "Smile to pay with your face. Hacking into programmed faciality

in the age of Big Data and AI" In: Alves de Sousa, E., Broens, M.C., Gonzalez, M.E.(Org.)

Big Data: Implicações Epistemológicas e Éticas (= Coleção CLE, Vol.88)

São Paulo: Filoczar, pp.177-209. ISSN: 0103-3247

Grimes, R. A. (2017). *Hacking the hacker: Learn from the experts who take down hackers*. Indianapolis, IN John Wiley & Sons.

Gupta, Aditya (2019). The IoT Hacker's handbook. A practical guide of hacking the Internet of Things.apress

Levy, Steven (2010). *Hackers. Heroes of the Computer Revolution*. 25th Anniversary Edition.

Sebastopol: OReilly.

Maxigas. "Hacklabs and Hackerspaces—Tracing Two Genealogies." *Journal of Peer Production*

2 (2012). http://peerproduction. net/issues/issue-2/peer- reviewed-papers/hacklabs-and

-hackerspaces/.

Menn, J. (2020). *Cult of the dead cow: How the original hacking supergroup might just save the world*. PUBLIC AFFAIRS.

Pias, Claus. (2014) "Cultural History of Hacking." In Landwehr, Dominik (Ed.) *Hacking*. (bilingual edition German/English) Zürich Christoph Merian Verlag, p.142-153.

Reagle, Joseph (2019). *Hacking Life. Systematized Living and its discontents*. Cambridge Mass.: MIT Press

Richterich, A. (2017) eds. "Making and Hacking". *Digital Culture & Society (DCS): Vol. 3, Issue 1/2017*. Bielefeld: transcript.

Snowden, E. (2019). *Permanent record*. New York: Metropolitan Books.

Walter, Bruno (2019). *Hacking e práticas de liberdade: conspirando com Hackers outros mundos*. Tese de doutoramento UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL PROGRAMA DE PÓS-GRADUAÇÃO EM PSICOLOGIA SOCIAL E INSTITUCIONAL. Porto Alegre, Brasil. pp.177. online: https://www.lume.ufrgs.br/handle/10183/205499

Webb, Maureen (2020). *Coding Democracy. How Hackers are Disrupting Power, Surveillance and Authoritarianism.* Cambridge Mass. MIT Press.