GABRIELLA COLEMAN (2012) *CODING FREEDOM: THE ETHICS AND AESTHETICS OF HACKING*. PRINCETON: PRINCETON UNIVERSITY PRESS. ISBN 978-0691144610.

Sebastian Kubitschko

Hardly a day goes by without some minor or major news report about "hackers." Cyber warfare, Distributed-Denial-of-Service (DDoS) attacks, Guy Fawkes masks, and leaked information have become catch phrases that seem to matter and that seem to sell. In rare cases the protagonists are glorified, sometimes they are treated with interest and many times they are still stereotyped as anti-social, possibly dangerous teenage boys holding disproportionate power in their hands. Much needed differentiations between hackers, whistleblowers and activists are more often than not swept under the carpet. Instead, the individuals or collectives are either praised as heroes of the digital age or personalized as the troll, the intruder, the freak, the criminal, the spy, the enemy, and the terrorist all at once. *Anonymous*, Aaron Swartz, *WikiLeaks,* Bradley Manning, Edward Snowden, to mention only a few whose stories continue to travel around the globe's newsfeeds.

But media outlets are by far not the only powerful institutions defining the discourse around "hackers" and those who are marked as such. Over the past decade, federal governments – in democratic as well as authoritarian states – have intensified the criminalization and demonization of activists that practice politics by creatively engaging with technological equipment. In the USA, for example, the Computer Fraud and Abuse Act (CFAA) of 1986 functions as an increasingly powerful law that appears to be immune to recognizing "good" or "productive" geeks. The basic rationale behind the CFAA is to protect national security, critical infrastructure and the economy from cyber attacks. There is nothing wrong with that in principle. But, as legal scholars have shown and as a wide range of activists criticize, since its approval in 1986 the CFAA has been amended and tightened to such an extent that

differentiating between a benign trespass and a serious crime related to computers has become impossible, resulting in the over-criminalization of offenders. On a global scale, NATO's recently published *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013) explicitly permits the elimination of civilian hackers in "war scenarios."

At the same time, and in stark contrast to this 21st century witch-hunt, educational institutions across the globe are training legions of graduates in order to procure supplies for the cybersecurity industry and the digital economy. In the USA, the professional training of "geeks" has a history that goes back to at least the 1960s, but it has never been mushrooming like it has over the past ten years. With the digital economy increasingly in the driver's seat and intertwined with traditional sectors, the education and recruitment of skilled developers, coders, and programmers has reached an all-time high. On more than one occasion boundaries between the private sector and state security have become blurred. The National Security Agency (NSA) as well as other intelligence services are not only recruiting talented information and computer scientists, they also have attractive scholarship programs that enable students to visit elite universities and to graduate without a mountain of debt. It is also worth taking into consideration Matthew Aid's article for *Foreign Policy* that illuminates the activities of the Office of Tailored Access Operations (TAO) – an NSA "secretive" hacker group specialized in accessing Chinese computer systems for over 15 years (Aid, 2013). Recently, the Israel Electric Corp (IEC) inaugurated a "Cyber Gym" where tech and infrastructure companies train up-and-coming hackers to defend the country against cyber attacks.

One way to summarize the above scenario is that governmental actors have a love-hate or what psychologists refer to as a schizophrenic relationship to computer experts. Another, probably more realist but still oversimplified conclusion to draw is that the national economy and security – justified by a somewhat paranoid fear of terrorism and loss of control – are higher valued than constitutional foundations. So, differentiations are made, but only between "us" and "them." The middle way between commercial or governmental employers and the (criminal) underground is a blank area on the political map. As technology related issues have taken centre stage in everyday life as well as in governmental decision-making processes, numerous individual and collective actors have decided to use their technical expertise to advocate for privacy, freedom, liberty and democracy. So far, their aims, motivations and

strategies are seldom heard, let alone thoroughly investigated. This is not only true for the media or institutional politics, but also for academic research.

Gabriella Coleman's *Coding Freedom: The Ethics and Aesthetics of Hacking* (2012) is a persuasive piece of writing that tackles some of the questions central to the current political climate. To summarize it in a single sentence, for Coleman the book aims to show how 'Hackers sit simultaneously at the center and margins of the liberal tradition' (3). Coleman gives her reader an in-depth picture of *who* hackers are, *what* they do and *why* they do it. The lens through which her investigation takes place is that of free and open-source software. Made up of six chapters, divided conceptually into pairs of two, *Coding Freedom* opens by giving a historically informed view of free software, carries on with a close ethnographic analysis of free software production, and concludes by engaging more directly with the politics of free software. Coleman is something like an ideal mediator for the "culture" of computer expertise and hacking. Intrigued by geek culture since the mid-1990s, she has pursued an academic career that allows her to reflect on the wider significance of this phenomenon without necessarily gaining financial profit or propagating a political agenda.

Her background in anthropology allows her to avoid any form of technological determinism or to lose touch with the human actors involved. Chapter 1, for example, compiled from over seventy life histories, demonstrates 'how hackers interact and collaborate through virtual technologies, how they formulate liberal discourses through virtual interactions, how they came to learn about free software, and how they individually and collectively experience the pleasures of hacking' (21). Yet, the focus of attention is never on the technologies but on the actors that use them and tinker with them. Through a number of engaging examples we learn about "hacking" not only as a technical endeavor, but also as an aesthetic and a moral project that converges powerfully with humour, cleverness, craft and politics. The cultural significance of geek humor is a particularly prominent and amusing theme throughout the book.

Initiated in the winter of 2000, most of Coleman's ethnographic research, including periodically partaking in a hacker "lifestyle" and joining people in both day-to-day and extraordinary activities over several years, took place in the Bay Area. In particular, Chapters 3 and 4 introduce the outcomes of these qualitative explorations and demonstrate the value of doing ethnographic work. Echoing her

methodological approach, Coleman's book is not aiming to explain hackers or geek culture per se, but instead stresses the specificities of a collective – embedded in social, cultural and legal contexts.

Unlike many academics and journalists engaging with hacker culture and what is often framed as "hacktivism", Coleman takes a step forward by stressing the scene's diversity and complexity. She agrees that hackers overall tend to adore computers, playfulness and a set of liberal principles like freedom, privacy, and access. At the same time, Coleman remarks that hackers 'evince considerable diversity and are notoriously sectarian, constantly debating the meaning of the words hack, hacker, and hacking' (17). So, 'once we confront hacking in anthropological and historical terms, some similarities melt into a sea of differences' (18). Consequently, stereotyping is out of the questions as a helpful access point. Instead, individual as well as regional, national and global differences amongst and within hacker culture call for diverse forms of consideration.

My own research on the Chaos Computer Club (CCC) – Europe's oldest and one of the world's largest hacker communities – confirms this credo, as it paints a different picture of how hackers and politically motivated computer experts can form part of society and the political landscape (Kubitschko, forthcoming). The CCC is not only a registered association but also an approved lobby group advising most major political parties in Germany, participating in governmental committees and acting as an expert for Germany's constitutional court. While I am far from claiming that the situation in Germany approaches that of perfection, it is still a rather positive example of how "traditional" and "emerging" ways of doing politics correlate.

If one wants to find a point of criticism in Coleman's analysis, it might be that her discussion of the "dark" or illegal side of hacking falls a bit short. Coleman states that 'the degree of illegality varies greatly (and much of hacking is legal)' (17). This gap leaves room for critics that could interpret it as a sign of glorification of hacking. While the narrative arc of the book demonstrates that this is clearly not the case, a more explicit position taking addressing this gap would not have done any harm clarifying Coleman's take on the legal-illegal divide.

Perhaps the most important lesson we learn from Coleman's book is that the stereotyping and criminalization of hackers is not simply done on the level of the individual. Rather, it is about freedom and

civil liberties, the core components of a healthy democratic environment. *Coding Freedom* is a successful balancing act between 'exploring in detail free software's sociocultural dynamics' (20) and accentuating that hackers, coders, and geeks are behind a relevant political culture that often lets them act as guardians of civil liberties. As Coleman points out in her conclusion, although actors engaging with software freedom are anchored by a technical craft, they have also ensured broader political and economic transformations because they act 'as a politics of critique by providing a living counterexample' (185). In the context of other scholarship on the societal roles free software can play, particularly Chris Kelty's much-praised *Two Bits* (2008), Coleman goes one step further by highlighting the significance of civic actors who argue with, through and about technology for democratic politics as an end in itself.

References

Aid, M. (2013) 'Inside the NSA's Ultra-Secret China Hacking Group', in *Foreign Policy* (Oct 15). foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group (last accessed 9 Dec 2013).

Coleman, G. (2012) *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press.

Kelty, C. (2008) *Two Bits: The Cultural Significance of Free Software*. Durham: Duke University Press.

Kubitschko, S. (forthcoming) 'Hacking Authority', in C. Calhoun and R. Sennett (eds.), *Creating Authority*. New York: NYU Press.