View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

The Hacker Imaginaire: Recoding Futures? Technoscientific Promises from the Inventors of the Internet

Simone Ines Lackerbauer

ABSTRACT In the 1970s, researchers and engineers built the technical predecessor of today's global digital networks, but more importantly, they created an "Internet Imaginaire" (Flichy 2007) with the aim of building a global virtual society. In the 1990s, most supporters of the utopian digital community fell silent. The hackers, however, remained, and they still adhere to rules put down in the so-called "hacker ethic" (Levy 1984; Coleman 2015), such as decentralization and freedom of information, which contribute to a sociotechnical "Hacker Imaginaire." With the Sociology of Knowledge Approach to Discourse (SKAD) as a research programme, this paper investigates the genesis and perseverance of this imaginary by uncovering technoscientific promises in media documents and interviews, which were formulated in response to the continued development of Internet-based technologies and fuel this imaginary; and by describing its phenomenal structure.

KEY WORDS internet research, sociotechnical studies, sociology of knowledge approach to discourse (SKAD), discourse analysis, sociotechnical imaginary, cyberculture, hackers

Introduction

In the 1970s, researchers and engineers built the technical predecessor of today's global digital networks, but more importantly, they created an "Internet Imaginaire" (Flichy 2007) with the aim of building a global virtual society. Once commercial and political actors entered the Internet in the 1990s, most supporters of the utopian idea of a digital community fell silent; largely, only open source advocates and hackers remained. Especially the latter still adhere to rules put down in the so-called "hacker ethic" (Levy 1984; Coleman 2015), such as decentralization and freedom of information. Research on hackers and hacking has been conducted in various disciplines, such as anthropology, media research, communication studies, cultural studies, criminology, computer sciences, law, economics, and various sociological subfields in the Anglo-Saxon, German, and French traditions, including STS (science, technology, and society studies – or science and technology studies), Internet sociology, sociology of crime, *sociologie des usages* ("sociology of usages"), and *sociologie des réseaux* ("network sociology").

In social research, the figure of the "hacker" has been established as a border crosser (Pias 2002), as a tinkerer and maker (Lackerbauer 2014b), as a utopianist (Turner 2006),

Sociální studia / Social Studies 2/2019. S. 51–70. ISSN 1214-813X.

and as a criminal (Hafner and Markoff 1991). Individuals, activist groups ("hacktivists"), administrative bodies like the National Security Agency (NSA), and even entire countries can hack. The practice of "hacking" refers to a wide range of activities from biohacking (Haraway 1991) and self-optimization (Lackerbauer and Roche 2016), social engineering and Internet activism to unauthorized access through programming, from manipulation of the media and of democracy to cyberwarfare (Carr 2011). Scholars have investigated hacker groups like Anonymous (Coleman 2015) and WikiLeaks. The perception of the hacker ranges from idealization based on their computer skills (Rheingold 1993), heroization for their quest to defend the freedom of information (Levy 1984), to criminalization (Hollinger 1997). Hackers can be framed as agents in a "user society" (Lackerbauer and Roche 2016) who actively modify reality. Hacking has become synonymous with acts of wilful intrusion or modification to achieve certain goals, notwithstanding the means or the possible moral and legal implications. This definition from the common knowledge, however, bears no resemblance to the meaning of the word "hack," as it is still widely used among hackers:[1]

1. Originally, a quick job that produces what is needed, but not well.
2. An incredibly good, and perhaps very time-consuming, piece of work that produces exactly what is needed.[2]

This definition of the "hack" is two-sided: a quick-and-dirty solution, and a sophisticated solution at the same time. It may refer to the ingenuity of the hack itself as a solution to a problem, or to the ingenuity of the hacker who conceived of the hack. By the 1970s, the definition of the hack had evolved into a large collection of hacker-related information and documents; a "guidebook" of hacker culture, named the "Jargon File." In the early stages of the hacker community and generations in the 1970s and 1980s, researchers and tech journalists already showed interest in the activities of hackers, not least because some hackers – even teenagers – were prosecuted and convicted for tinkering with technological systems in ways the layperson could not easily understand. Fascination with hackers' technical skills and the emerging cyberspace technologies went hand in hand with dystopian visions of technicized futures, as constructed in "cyberpunk" science fiction,[3] which would often frame hackers as tech-savvy anti-heroes and stir up emotions, for "[t]echnological innovation often follows on the heels of science fiction" (Jasanoff 2015: 1). Regardless of public attention or the lack thereof, the hacker community thrived with the technological advancements.

---

1 For this article, the hacker is defined as someone who identifies with the "hacker ethic," which is explained below.

2 http://www.catb.org/jargon/html/H/hack.html, accessed on March 14, 2019. This definition can be traced back to the "philosophy" of students at the MIT, especially at the MIT model railroad club, who used the term "hack" to describe sophisticated pranks they would play on others. From there, it evolved with the use of the first mainframe computers and the related user culture.

3 Cyberpunk science fiction emerged in the 1980s and was established as a science fiction genre with William Gibson's novel *Neuromancer* in 1984. The setting of most publications is low-life/high-tech.

I propose one possible explanation for this perseverance: hackers dispose of a common "constructed communicable model" – a set of rules they share that would connect them and infect those who seek to become hackers, and a "sociotechnical imaginary" previous research has not investigated. By framing hackers, hacking, and hacker "culture" as parts of such an imaginary, and by assuming a theoretical perspective based on the sociology of knowledge, it is possible to overcome the methodological limitations imposed by focusing on only one of these aspects. To develop this approach, I will briefly refer to the original "Internet Imaginaire" (Flichy 2007) and derive a "Hacker Imaginaire" from it. I argue that technological change pressures agents of this imaginary to permanently actualize it by formulating "self-contained" technoscientific promises, TSPs (Joly 2010, 2015), as events that trigger and update a hacker discourse. By drawing on aspects from the Sociology of Knowledge Approach to Discourse, SKAD (Keller 2011), as a research programme, I will analyze the Hacker Imaginaire as a sociotechnical vision based on discursively processed knowledge from the Hacker Ethic. In doing so, this paper attempts to reconstruct two of the technoscientific promises and to examine possible reasons for TSP failure and the phenomenal structure of the Hacker Imaginaire.

Theoretical section

From social imaginary to Internet Imaginaire

To talk about the imaginary, it is necessary to briefly investigate the matter of knowledge. This article refers to the sociology of knowledge as one theoretical perspective that can be assumed to investigate the phenomena associated with hacking. The sociology of knowledge tradition linked to the SKAD perspective[4] is not only concerned with "a society's authoritative ideas and formal knowledges [and] those who operate in the realm of everyday life: informal knowledges" (McCarthy 2000). More importantly, it focuses on the construction of knowledge, based on Berger and Luckmann's concept of a social construction of reality: "[T]he sociology of knowledge must first of all concern itself with what people 'know' as 'reality' in their everyday (…) lives. In other words, common-sense 'knowledge' rather than 'ideas' must be the central focus (…) [It] constitutes the fabric of meanings without which no society could exist. The sociology of knowledge, therefore, must concern itself with the social construction of reality" (Berger and Luckmann 1969: 27). Against this background, the imaginary can be perceived as an aspect of knowledge anchored in a shared perception of reality.

In the description of the "social imaginary" working group in the sociology of knowledge section of the German Sociological Association,[5] the authors acknowledge a variety of approaches to conceptualize "the imaginary" in Anglo-Saxon, French, and German

4 Cf. Keller (2011) for a brief genealogy of the sociology of knowledge as used in the SKAD framework.

5 PDF file of the self-description: http://wissenssoziologie.de/wp-content/uploads/2016/12/Arbeitskreis-Abstract-f%C3%BCr-HP-final.pdf, accessed on March 14, 2019.

sociological traditions alone; a fact that complicates research, given that sociology itself is defined differently in the respective scientific environments. The working group seeks to find new ways to achieve a common understanding of the imaginary and its potential for theory development in the sociology of knowledge – an *intra*disciplinary approach, so to speak. To further a common understanding of the social imaginary as *inter*disciplinary multiplies the potential interpretations, especially when imaginaries themselves cross geographic borders and socio-structural limitations, as is the case for what Patrice Flichy calls the "Internet Imaginaire."

Flichy conducted extensive observations at the birthplace of Internet technologies in California and analyzed them based on his research background (media history and communication studies). US scholars like Fred Turner (2006) rooted an Internet-based imaginary in the countercultural movements of the late 1960s in this area and took this as the basis for an analysis of a "cyberculture" imaginary, with cultural studies as the main theoretical basis. Yet another angle on the social imaginary aspects of the Internet was investigated by Turkle (1997) with her study of the socio-psychological aspects of the Internet, focusing on the meaning of the Internet for communication processes, identity-building, self-presentation, and the multiplication of the self in virtual environments. Other social science works focus on the social imaginary of a virtual economy, e.g. in games (Castronova 2005), or with regards to innovation (Von Hippel 1988), or the social imaginary of a virtual community on the electronic frontier (Rheingold 1993). What unites them is a translation of real-world social aspects, actions, and behaviours into virtual environments. Parallels between them exist and some can be "translated" into others, e.g. Turkle's identity aspects can be found in Cardon's (2011) typology of Internet users. This means that connections between different perceptions of a *social* Internet imaginary can be established in spite of disciplinary and cultural limitations over time; knowledge gaps can be bridged, or the lack of awareness of research conducted on similar questions in different scientific environments by focusing on the imaginary as socially constructed knowledge.

Still, Flichy's research on the Internet Imaginaire stands out. According to Flichy, the historical research of technology had been "confined for a long time in a purely technical vision" (Flichy 1991). Early social research on communication or networking technologies was limited by the impact of such technologies in the public or professional spheres (e.g. cybernetics or Fordism), whereas later social research might take the technology "as is" and focus on its social impact for the individual. In contrast, Flichy focuses both the *social* aspects and the *technical* aspects in the "circulation of the technical object" (Flichy 1991). The genesis of a new communication technology is as important as its distribution and appropriation, and both the inventors' and the users' visions for the technology affect the entire process. Under the heading "Technical utopia, social utopia," Flichy (1991) explains that a technical vision – shared by a group of engineers and inventors – enables them to tackle a technological challenge to make their vision come true. Once the new technology is released, it fosters a social imaginary of adoption and adaptation: a new tool will only be successful if it is accepted by a sufficiently large group of users (adoption), and only if it leaves enough possibilities for these users to customize its use to fit in with their lives

(adaptation).[6] While this interplay of sociotechnical factors for the imaginary and others, including sociotechnical imaginaries, are now investigated in numerous disciplines, Internet research is different for at least two additional reasons. First, individuals are not only prompted to adopt/adapt a new technology based on or connected with the Internet, but they are also "invoked" to develop their own "uses" for it, which might be reintegrated into the original technology as user-generated content – or even result in a new technology. The imperative of making and creating marks an active "user society" (Lackerbauer and Roche 2016), and constantly changes existing, or generates new, imaginaries. For sociotechnical imaginaries linked with the Internet, time is also an important factor and the second difference from other imaginaries. On the one hand, it can be factored out: Internet technologies may have evolved, but the social structures connecting the humans who use them have largely stayed the same.[7] Hence, research conducted on Internet-based imaginaries from the 1980s is still relevant today, especially given that virtual assistants, 3D applications, or (basic) artificial intelligence had already been imagined and partly existed back then. On the other hand, time plays a crucial role for Internet-based imaginaries in that it dictates the velocity of new technologies. Hardware and software are in a status of permanent beta phases, evolution, updates, and iteration processes; never complete or "done." Change is an invariable, deeply rooted in Internet-related visions.

It may be argued that Flichy's "Imaginaire" could be replaced by the more common term "imaginary" in the context of social practice, as described by Jasanoff: "Modern societies prize imagination as an attribute of the creative individual (…) to see beyond the limits of constraining reality and to make or do things that are out of the ordinary. (…) But imagination also operates at an intersubjective level, uniting members of a social community in shared perceptions of futures that should or should not be realized" (Jasanoff 2015: 5–6). This socially shared imaginary then leads to action, like the manufacturing of a new technology. However, it seems that "imaginary" does not take into account that imagination is involved in the production, the adoption, and the adaptation of a technology over time – possible even perpetually, leading to new imaginaries for new related technologies. This could especially be true for the Internet and virtual worlds, as stated before, for production cycles are shorter and nothing is ever unchangeably finished. Overall, these considerations call for a different term instead of "imaginary," and therefore I use Flichy's Internet Imaginaire as the basis for the "sociotechnical loop of imaginaries" under investigation, which I link with considerations on the "user society" and time. Subsequently, a connection between this Internet Imaginaire and hackers must be established.

---

6 The success of an innovation is often defined by using Everett Roger's (1962) theory on the diffusion of innovations. It includes a normal distribution curve with different types of adopters for an innovation. In this curve, an innovation is successful when a critical mass of actors has adopted it.

7 Another aspect related to the social structures is the assumption that virtual worlds reflect the social order from the real world (with hierarchies and biases) – and that individuals using Internet technologies apply the same norms/values online which they adhere to in the real world.

From the definition of the hack as mentioned above and from the guide on "How to Become a Hacker" in the Jargon File,[8] it can be said that hackers are problem-seekers and problem-solvers. This means that hackers are actively looking for riddles and quests they can complete. It may be the attempt to penetrate seemingly impenetrable online security systems, or to write a perfect piece of code for any given task. A practice named "phreaking," discovered in the late 1950s (Sterling 1993), was one of the first hacks before the term had even been invented: it consisted of emulating a 2600 hertz tone in a phone system to operate free long-distance calls. In this case, the "problem" was self-proclaimed, and the "solution" was a legal grey zone – typical for many hacks. With this behaviour, hackers are "users" who adopt/adapt technologies and create new uses for them, including uses the inventors never conceived of; "making" or contributing to the shared hacker knowledge is an important value for hackers:

> The world is full of fascinating problems waiting to be solved. Being a hacker is lots of fun, but it's a kind of fun that takes lots of effort. The effort takes motivation. (…) [T]o be a hacker you have to get a basic thrill from solving problems, sharpening your skills, and exercising your intelligence. (Jargon File 1983)

The second aspect, time, can be factored out because the hackers' desire to seek and solve problems has not changed over time. Time must also be factored in, as Internet technologies constantly change, thus generating new problems hackers can seek and solve. Since hackers use Internet technologies unlike other Internet users, the assumption is that hackers foster their own version of an Internet Imaginaire, which others do not share or do not have access to for lack of knowledge or interest. While Internet users also modify or tinker with Internet technologies, hackers do so on the basis of their own set of rules, norms, and values: The Hacker Ethic, as the manifestation of their sociotechnical imaginary, written down by Levy (1984) in six tenets:

1. Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On imperative!
2. All information should be free.
3. Mistrust authority – promote decentralization.
4. Hackers should be judged by their hacking, not 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.

In this paper, this set of rules is framed as the foundation of a Hacker Imaginaire – a "sociotechnical loop of imaginaries" shared by a certain type of users of Internet-based technologies. Research on hackers shows that these principles are not limited only to hackers' uses of technology. In fact, they may be interpreted as a "phenomenology" (Lackerbauer 2016), or as a way to perceive and interact with the world.

---

8 http://www.catb.org/esr/faqs/hacker-howto.html; accessed on March 14, 2019.

An imaginaire actualized by technoscientific promises

The constant technological change requires the permanent actualization of the Hacker Imaginaire to ensure its continuation: a single imaginary built on an outdated reality might be less likely to endure. Speaking in the terms of SKAD, events and actors to perform these actualizations are needed to ensure the proliferation of the Imaginaire – including new technologies and ways to interact with them. Such events to actualize the Imaginaire can be technoscientific promises, or TPSs (Joly 2010, 2015), formulated on the basis of knowledge and imaginaries shared in the development process of a new technology, such as the Internet. Flichy (2002) describes the development of ARPANET, one of the Internet's predecessors, as a decentralized communication network, built by "computer specialists who had a new view of computing, suited to communication between machines with the same status." The scientists working on ARPANET built this network with themselves as its users and their own visions in mind, e.g. maximizing the freedom of work organization. Usenet, another precursor of the later Internet, was built by computer scientists from research centres "who participated on a voluntary basis" – sharing their knowledge for free – and the Internet, as the network of networks, was built with the vision of "a metaprotocol for interaction between networks built on different principles" with the idea of an open architecture including different modes of functioning in networks, and with no central authority: "The two main principles of decentralization and free access in which the Internet is grounded stem essentially from the academic functioning of its founders" (Flichy 2002: 190). Engineers thought that "computing was not only a calculation tool but also a means of communication. (…) This theme of the creation of collective intelligence through networking was to mobilize many computer specialists in the 1970s and 1980s, and to appeal strongly to users" (Flichy 2002: 190).

These principles can be identified as the promises that actualized the original ARPANET Imaginaire, stating that the Internet would be decentralized and free to access. They qualify as technoscientific promises, since they were formulated by the experts in the process of developing the technology that would perform them. Additionally, Joly (2010) states that a TSP requires a sense of urgency on which it can be formulated; that is, a problem and the need to change the status quo, which would only be possible with the solution proposed in the promise. In the case of the ARPANET, the risk of a nuclear war demanded a system for decentralized information distribution and storage and established this initial sense of urgency. Once it has been formulated, a TSP needs to be performed: it needs to be injected into an existing discourse (e.g. the discourse of the Internet Imaginaire) or trigger a new discourse, so its addressees will act upon it. A promise materializes in various forms, the most obvious of which is that it is spoken out loud. Language serves as a means to construct promises and the related expectations on the basis of what is known or not known.

The successful performance of a TSP then depends on different factors: it needs a sound knowledge basis, it must be linked to a given problem (to produce legitimacy for actions to be taken) and credible (determined by the past actions and the social network of the promise-maker), and there must be resources available to enact it.[9] A successful promise is one that

9 Joly's regime of technoscientific promises is far more complex and includes additional factors which could not be taken into account for this paper.

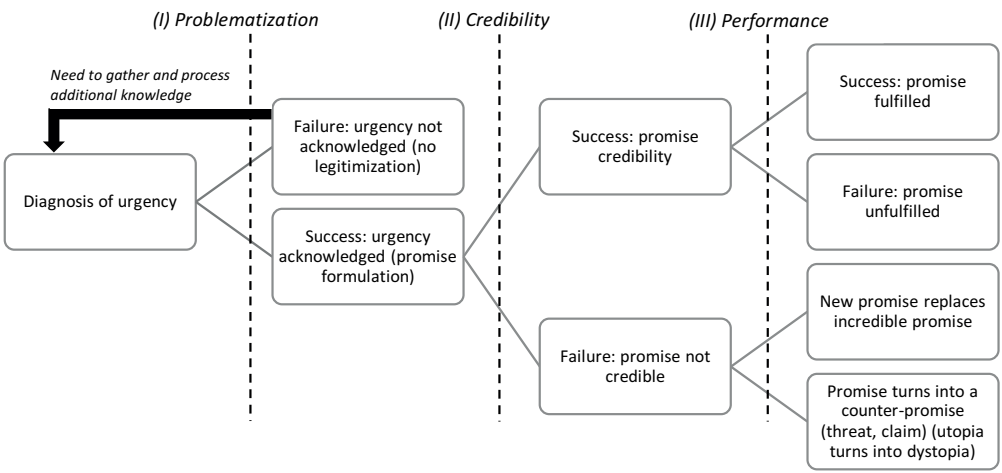
not only technology developers but also the public will believe. It may then be accepted as a truth and become part of an established reality. Because of their performativity in directing people's beliefs and actions, promises can therefore be thought as instruments of power. TPSs can fuel an Imaginaire or be a result thereof, and the scope of a TSP depends on the respective technological situation in which it is formulated. In this paper, TSPs are identified as events that actualize the Hacker Imaginaire, which itself is framed as the basis of a hacker discourse. The specific characteristic of these hacker TSPs is that they are both produced and executed by hackers – hackers create sociotechnical imaginaries for hackers based on the Hacker Ethic and hackers adopt/appropriate them.

However, the fact that people interact with the promise does not mean that the promise *will come true*. A TSP would thus be successful *only if it is fulfilled*. One can then argue that failure is possible at three different stages (Figure 1): after it is formulated (production phase), after its acknowledgement (adoption phase), and after its adoption (adaptation phase). Failure in stage (II) can lead to the formulation of a new promise or result in the reversal of the promise into a threat.

The process of the technoscientific promise requires the accumulation and discursive processing of even more data to ensure its success. Failure of a TSP is possible at the aforementioned three stages:

(I) Problematization failure (production phase): the diagnosis of urgency is flawed; thus, the urgency is not acknowledged: there is no production of the promise.
(II) Credibilization failure (adoption phase): the urgency is acknowledged and the promise is formulated, but it does not achieve credibility: there is no adoption of the promise.
(III) Performance failure (adaptation phase): the promise is formulated and credible, but it is not fulfilled: there is no adaptation.

Figure 1: Stages of failure and success of a techno-scientific promise



Note: The connecting lines represent the gathering and discursive processing of knowledge. The dashes separate the stages.

The entire theoretical section of this article has been based on a sociology of knowledge and SKAD perspective. While it is not possible to elaborate on the entire process of using SKAD (Keller 2011, 2018) as the research framework for investigating the Hacker Imaginaire, certain aspects can be used to identify and analye some technoscientific promises in the Hacker Imaginaire as the underlying structure of a hacker discourse.

SKAD as a research programme

As a research programme, SKAD builds on Michel Foucault's approach to discourse and on the sociology of knowledge tradition of Peter Berger and Thomas Luckmann (1969). SKAD assumes that the perception of the social world as a reality "is mediated through socially constructed and typified knowledge" (Keller 2012b: 61). Its focus lies in the investigation of the social (re)construction of and discursive processing of knowledge, including what is or cannot be known. Several dimensions are included in this examination, from the material or institutional contexts of knowledge production (e.g. in communities, among experts, or in the media) to the social consequences of knowledge production and distribution. SKAD examines discourses as performative in that they constitute orders of reality as well as effects of power in networks of social actors, institutional settings, and knowledge systems (Keller 2011).

Two heuristic concepts from SKAD are employed in this paper. One of them is the concept of the "phenomenal structure," as the constellation of elements that are combined to constitute phenomena through discourses (Keller 2011: 114). Together with interpretative schemes, classifications, and narrative structures, phenomenal structures "create the *interpretive repertoire* of a discourse" (Keller 2012a: 67, emphasis in original). Through qualitative analysis of data on a specific topic, one or several competing discourses emerge that can each be broken down into a phenomenal structure to enable a deeper understanding of the discourse and possible comparisons with other discourses, among other things. In this paper, the phenomenal structure of the Hacker Imaginaire will be identified by analyzing the manifestations of the Hacker Ethic and of technoscientific promises in media documents and interviews. As mentioned, TSPs can trigger actualizations of discourses that may overlap or diverge over time. It would thus be unwise to speak of "the" hacker discourse – instead, this analysis focuses on "a" hacker discourse, based on the Hacker Ethic and the Hacker Imaginaire.[10]

The second heuristic concept I will use is the identification of the Hacker Ethic as a "model practice" – the SKAD term into which "constructed communicable model" could be translated. Model practices "provide templates for how one should act concerning issues that have been defined by the discourse" (Keller 2012a: 67). This can be illustrated with a practical example. The term "hacker ethic" has generated a derivate: the "ethical hacker" as a persona (and "ethical hacking" as a practice). An ethical hacker (originally: "white hat hacker") does not harm the systems he penetrates and he does not act for his own benefit. Instead, he may

10 Examples for hacker discourses might be as general as "hackers are criminals who steal people's data" in the context of cybercrime, or as specific as "ethical-moralistic motivation"/"opportunist-pragmatic hacking"/"Internet fame-seeking" in the context of Anonymous attacking Scientology in 2008 and 2009, known as "Project Chanology."

point the administrators of an unsecured system to its weakness, so they can fix it. Companies like Facebook have begun to use hackers as "bounty hunters" by asking them to penetrate their systems to find and report flawed code. Uncovering software bugs is also a common technique used by hackers to acquire jobs in high tech or tech security firms. The investigation of "ethical hacking" requires a different discourse-analytical angle, but "bounty hunting" can be identified as a "discursive model practice" based on the principles of the Hacker Ethic and on processing the knowledge about this practice and how to do it among the actors involved.

Essentially, the "hacker ethic" is a guidebook for "appropriate" behaviour for the hackers subscribing to it, and an explanation for non-hackers to understand the hackers' perception of the world. While the Hacker Ethic is non-binding, abiding by these rules may create a sense of belonging to an invisible global community. It may also foster the impression of serving a principle higher than the economic and political systems of real-world governments, whose regulations are constantly overruled by the values of the Hacker Ethic. In this sense, these six sentences form a "constructed communicable model"; communicable in that it can be communicated, but also in that can be applicable to all situations in (virtual or real) life, and in that aspiring hackers should be "infected" by it and follow it. Thus, it also serves to simplify the structure of contemporary complex societies: The Hacker Ethic is universal and not limited by national laws, and it incorporates principles based on which hackers can act. The Hacker Ethic is a discursive model practice, and additional practices serving as typical models for hacker behaviour (such as "bounty hunting") can become discursive model practices if they are established among hackers and confirmed by repetition in similar situations.

In the theoretical section, the Hacker Ethic was established as a discursive model practice that directs hackers' actions, and as the basis for a Hacker Imaginaire. With ongoing technological developments, this "sociotechnical loop of imaginaries" is actualized by technoscientific promises, formulated by hackers in concordance with the Hacker Ethic. In the empirical analysis below, such TSPs are identified as examples to contribute to the phenomenal structure of a hacker discourse.

Empirical section

Methodology, methods, and data

Empirical approaches to the study of hacking and hackers are grounded in different methodological traditions and use various quantitative and qualitative methods, ranging from data/document analyses to interaction/action observations. Although discourses about hackers and hacking have already been investigated, in the past such analyses were mostly limited to media documents or to the self-perception of hackers. However, an analysis is missing that includes not only documents and the cultural or sociohistorical background of hackers and hacking, but an understanding of hacking itself as a phenomenology, or as a perception of the world, with the Hacker Ethic as the filter according to which the "complex world" is organized to realize the Hacker Imaginaire. For such an analysis, all the components of this imaginary must be taken into account: the hackers, the act of hacking, the hacks, the artefacts used (e.g. computers, code), the actors, and the networks to connect them.

The SKAD research programme, with its specific understanding of "discourse," proposes heuristic tools to meet the needs of such an analysis, at the same time offering possibilities to modify and extend them according to the research context,[11] i.e. to introduce new concepts into SKAD, such as the Hacker Imaginaire or TSPs. The first step of my analysis was to compose a working paper on the chronology of events in the hacking discourse, the different actors (including organizations and material artefacts), and the leading arguments in the interplay of knowledge and power within the discourse. For this paper, the few documents that constitute the common knowledge base of what a hacker is and does were selected for the sample (i.e. to gather knowledge on the discourse context). While the selection is subjective and heuristic, these specific texts are repeatedly referred to in popular/scientific literature and in texts written by hackers themselves. These are:

– The Hacker Manifesto, original title "The Conscience of a Hacker" (The Mentor 1986)[12]
– The Jargon File (website hosted by Eric S. Raymond, online since 1990)[13]
– The Hacker Ethic (Levy 1984)
– A Declaration of Independence of Cyberspace (Barlow 1996)[14]

There may be more documents that may (only) have been (or be) relevant at certain points in time in the history of hacking (such as the Anonymous manifesto, the WikiLeaks statutes, and the OpenSource principles), but it can be assumed they resonate with the documents mentioned above.

The second step is a non-exhaustive keyword-based media document search and analysis of hacker discourse that focuses on the research question: the meaning of the Hacker Imaginaire. Relevant media documents are selected by theoretical sampling, e.g. by collecting documents published at the times of certain internal or external events that "disturbed" the order of the discourse (e.g. a new Internet law or activities of a hacker group), or when this hacker discourse first emerged. Following the principle of contrast, relevant documents are subject to an initial reading and targeted search queries within the scope of particular events are performed to include a broad range of different positions (e.g. opinions, speakers from different organizations) until a degree of saturation is reached, i.e. when reading additional documents does not add new knowledge to the discourse and only repeats what has already been said. In this paper, the event selected for the analysis is the emergence of the "hacker ethic." A keyword search on the international database Nexis® led to 403 results for the keywords "hacker ethic" (280), the German "Hacker Ethik" (66), and the French "éthique

11 My approach in this paper is inspired by two other concurrent projects: the DFG-funded project, "Controversies Over Hydraulic Fracturing in France, Germany and Poland: A Comparative Analysis of the Role of Ecological Justifications and Civic Epistemologies in Current Risk Conflicts" (KE 1608/11-1) and a co-authored article on the technoscientific shale gas promises in three European countries (2018); I hereby acknowledge the research conducted with my colleagues for the article which also informed this paper.

12 http://phrack.org/issues/7/3.html, accessed on March 14, 2019.

13 http://catb.org/jargon/html/, accessed on March 14, 2019.

14 https://www.eff.org/cyberspace-independence, accessed on March 14, 2019.

hacker" (20) from 1984 to 2018. From this corpus, duplicates were merged (same or similar date, headline, and word count), which limited the corpus to 285 articles.

The third step is to take the analysis beyond these media documents. In this paper, the Hacker Ethic as the basis for the Hacker Imaginaire was further investigated by focusing on media interviews with hackers from the selected corpus.[15] 65 of the 403 media results had the English/German word "interview" or the French "entretien" – 48 after omitting duplicates and false positives – and 23 of them were interviews with hackers or included data from interviews with hackers. To contrast these, interviews with hackers that were not published in national news or special interest media have been selected as a suitable addition to the corpus. There are several reasons for this approach: (I) hackers mistrust authorities and the media, which they perceive as the voices of actors they see as opponents (e.g. corporations, politicians), so there are few interviews with self-proclaimed hackers in the media who are not already legitimized speakers in the discourse; and (II) a medium has its own editorial standard, including a certain political alignment and stylistic preferences (e.g. article length). Typically, interviews are heavily redacted or shortened at the cost of authenticity. In contrast, interviews with hackers published on non-media websites (e.g. private blogs or websites on Internet/tech topics) are probably less modified. This choice is based on the assumption that, regardless of the interview situation, the Hacker Ethic will inform the answers and help identify the TSPs that fuel the Hacker Imaginaire. Results from data gathered for previous analyses (Lackerbauer 2016) and from interviews with legitimized hackers conducted in 2011-2012 (Lackerbauer 2014a) also informed the empirical analysis.[16]

The texts of this corpus are then subject to a reconstructive analysis. The texts were divided into meaningful analysis sequences, as proposed by Keller (2012b). The aim of this analysis is to identify aspects of the phenomenal structure of a hacker discourse, leading to the reconstruction of the "reality" (in this case: Imaginaire) that is socially constructed in the texts.[17] A series of general concepts (or codes) for the texts, intended as meaningful units of sense, are then formulated. These codes are collected to form cross-text interpretation patterns and to reveal the discursive genesis or failure of TSPs, as well as the phenomenal structure of the Hacker Imaginaire.

---

15 Search queries for interviews with hackers without the keyword "hacker ethic," but with one of the keywords "ARPANET," "www," or "Internet" yielded 8,357 results for the period until December 31, 2010. Reflection on the (hacker) discourse to investigate from the spectrum of possible (hacker) discourses is of great importance; this selection process is implied in the SKAD research programme as applied in this paper.

16 For previous research, traces of the "hacker ethic" have been tracked in online documents that are not part of the media discourse. Such documents include darknets, videos, and websites by hackers, or interviews with hackers conducted in 2011-2012.

17 "The principle of sequential analysis consists of developing, with regard to the particular research questions, and following the flow of the text, as many interpretive hypotheses as possible for individual sentences, whole text sections, or the entire text. These are then checked, rejected or kept and/or refined with regard to their appropriateness in the immediate continuation or the text" (Keller 2012b: 123).

The phenomenal structure of the Hacker Imaginaire

As Joly (2010) has established, a technoscientific promise requires a "sense of urgency" – i.e. the impression that something is at risk – to prompt its formulation. The basic societal setting of a "risk society" (Beck 1992) already encompasses a constant sentiment of change based on unforeseeable events, with responses to risks as the means to organize a global populace. A general orientation towards the future can be derived from this setting, with the aim to reduce existing risks and to prevent new risks by knowledge advancement and "innovation," including the development of new technologies to solve problems and, subsequently, to find solutions for the new problems arising with them.

If we apply this to the idea of a hacker community, the Hacker Imaginaire has been at risk since real-world commercial and political actors began to populate "their" cyberspace. The values of the Hacker Ethic are endangered, and a sense of urgency is created – assumedly reinforced by Barlow's 1996 declaration of cyberspace independence. The constant flow of new technologies and problems results in the permanent actualization of TSPs and the Hacker Imaginaire. Based on the SKAD research programme and on the condition of a successfully established sense of urgency, we can derive the following possible phenomenal structure of the Hacker Imaginaire:

Figure 2: The phenomenal structure of a hacker discourse based on the "Hacker Imaginaire"

Sense of urgency	Institutionalized real-world actors intrude upon cyberspace, Hacker Imaginaire is at risk, constant technological advancement and new problems
Promises	Decentralization, freedom of access and information, power through knowledge
Knowledge basis	Observations of technological progress and social implications, experience from previous hacks/hackers, hacker documents (e.g. Jargon File, Hacker Ethic, hacker manifesto, declaration of cyberspace independence)
Self-Positioning	Hackers as the keepers of the promises and values of the Hacker Ethic
Other-Positioning	Institutionalized real-world actors use cyberspace to stabilize their power over the world and unsuspecting users
Problematization/ legitimization	Dystopian visions (e.g. *1984*, Cyberpunk science fiction), cyberwarfare, questions of big data and privacy online, governmental actors as hackers, secretive behaviour
Credibility	Institutionalization of hackers (e.g. EFF, DEFCON), hackers working with/for governmental organizations and companies, hacker attitude as problem-seekers and -solvers
Resources	Technical innovations trigger actualization of the promises, invisible global hacker community sharing the Hacker Imaginaire
Solution	Keep institutionalized real-world actors under control, protect cyberspace and unsuspecting users
Obstacles	"Ethical" questions, real-world norms/values, missing legislation, different interpretations of the Hacker Ethic, reproduction of real-world hierarchies (e.g. institutionalization, media communication)
Outcome	Diversification of technologies, tools, and uses; constant reproduction of the Hacker Imaginaire

The *promises* mentioned are the general principles on which the Internet was once conceived: decentralization and freedom of access/information, with the implied power obtained through shared knowledge. These promises are informed by a *knowledge base* that consists of the main hacker documents and knowledge gathered through experience with previous hacks/hackers and the hacker documents. *Self-positioning* refers to how the hackers see themselves against the others. *Other-positioning* refers to the institutionalized real-world actors who cause the problem.

As sociotechnical innovations advance, e.g. with the smartphone, online marketing, and social networks, hackers utilize visions like Orwell's *1984* or dystopian cyberpunk science fiction to *legitimize* their concerns about certain topics, such as online privacy and big data, sects, or the secretive behaviour of governmental organizations like the NSA – and their actions against them. While other actors do voice their concerns on such matters, hackers may see themselves as the legitimate actors to formulate and execute TSPs to counter these threats and to prevent the futures implied therein, since their perception of norms and values is not rooted in real-world societal structures, political or economic systems; they act outside the real-world systems.

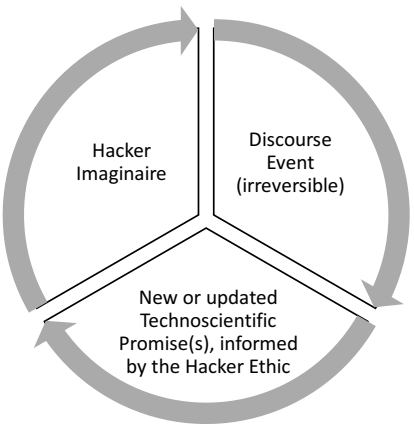
Although hacker TSPs are formulated and executed by hackers, the question of *credibility* must take two different audiences into account. First, TSPs must be credible among their peers, the hackers, for them to believe in a TSP and to act upon it. However, TSPs must also be credible for external actors in the hacker discourse, for their reaction to the execution of the promises can lead to their success or failure – and to avoid a setback in relevance. Moreover, the means of open communication (e.g. in interviews, videos on YouTube, or on websites) also serve to spread a specific version of the Hacker Imaginaire in an attempt to dominate the hacker discourse. Both internal and external credibility can be obtained by quantitative actions (e.g. a constant stream of communication) or by qualitative actions, e.g. turning a collective movement into a structured organization credible among hackers and non-hackers, with a legitimized hacker as its figurehead, such as the US-American Electronic Frontier Foundation (EFF) with John Perry Barlow; or by gaining visibility in public through the organization of a yearly conference in Las Vegas, the DEFCON.

One *resource* for TSPs is the dystopia of permanently emerging new risks, such as technological innovations or Internet regulation, which trigger a sense of urgency and thus enable the formulation of new TSPs. Another resource is the presumed large and invisible global hacker community, sharing the Hacker Imaginaire. A possible *solution* would be to keep institutionalized real-world actors under control through hacks, to protect cyberspace and its unsuspecting users.

Obstacles for hacker TSPs can be identified in norms and values from the non-digital world, including the question of what is "ethical." Moreover, self-proclaimed hackers may interpret the Hacker Ethic differently and use it as a legitimization for their actions. By using real-world means of communication and organizational structures, hackers reproduce societal hierarchies and a social order that is in discordance with the Hacker Ethic (i.e. the idea of a decentralized system, or equal freedom of and access to information). The question whether institutionalized hackers forfeit their credibility among hackers must remain unanswered at this point.

The *outcome* to derive from the phenomenal structure of the Hacker Imaginaire can be subsumed as the realization that constant technological change fosters the constant actualization or generation of technoscientific promises, with new TSPs updating the Hacker Imaginaire in the specific hacker discourse under investigation:

Figure 3: A discourse event triggers (a) new TSP(s) which update(s) the "Hacker Imaginaire"



Regardless of whether a TSP succeeds or fails at any of the stages mentioned above, it will impact the Hacker Imaginaire. Finally, internal or external events that "disturb" the order of the hacker discourse and trigger TSP(s) in the Hacker Imaginaire, as found in the data, are most likely irreversible: a new law, a security breach, a new virus, a new technology cannot be "undone." Countermeasures can be developed and injected into the discourse, but any event will cause a disturbance and might evoke a sense of urgency.

Examples for technoscientific promises in the Hacker Imaginaire

The promise of freedom of access

Based on a research project, one purpose of the Internet was to foster collaboration among researchers by facilitating communication among them and access to information and to the technology needed for this. As all nodes in the network were considered equals, the idea of decentralization and a non-hierarchical structure resonated with this and manifested in the Hacker Ethic. With the rise of proprietary systems, such as Windows as an operating system, Microsoft Office as a software package, or paywalls behind which information was stored, this freedom was suddenly restricted. In consequence, hackers started to use different networks (pre-existing or newly developed) and tools, e.g. darknets or VPN software, to hide their knowledge from outsiders and to secure its availability for insiders, resembling a *collège invisible*. Freedom of access goes hand in hand with free access, so some hackers would gain unauthorized access to proprietary data and share it for free, since "All information should be free" (Levy 1984), according to the Hacker Ethic.

The promise of power by knowledge

SKAD focuses on the generation, circulation, and utilization of knowledge as a means to obtain power. In the Hacker Imaginaire, the power of knowledge manifests in two ways. (I) In "The Conscience of a Hacker" (The Mentor 1986), it is defined as follows: "Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for." In the Hacker Ethic, Levy (1984) wrote a similar statement: "Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position." These messages imply a "promise of power by knowledge": hackers are legitimized for their actions and shall only be judged on this basis – with other hackers who share the same knowledge base as the only legitimate actors to judge them, since outsiders will apply other criteria for their judgment. The discursive processing and application of this insider knowledge, e.g. in hacks, confirms the impression of exerting power over technology. (II) However, the relation between knowledge and power is permanently challenged. When a new or updated technology is released, hackers must reaffirm their power by obtaining superior knowledge about the new tool or software. Something that is unknown is a problem for hackers that they will consequently seek to solve. As a result, a permanent race for power is initiated: hackers discover a weakness in a piece of software, the developers fix this loophole and update the technology (or policymakers pass a law to prohibit the exploitation of a particular weak point), then hackers go on to find the next vulnerability… Thereby, knowledge is instrumentalized as a means to obtain power. This resonates with hackers and their "hands-on imperative," and it fosters the impression of actively participating in the construction of the Hacker Imaginaire.

Failed and blurred technoscientific promises from the Hacker Ethic

TSPs are events that can trigger new discourses or update existing discourses. They can be actualized according to the sociotechnical environment, e.g. when a technical innovation prompts new ways for a TSP to be fulfilled, or triggers a new TSP based on a sense of urgency. TSPs from the Hacker Ethic are self-contained in that the producers of the promises are the same as those who seek to fulfil them. Some TSPs, e.g. the promise of freedom and the promise of knowledge, are unlikely to cease existing, as technical advancements enable (or enforce) their actualization.

There are, however, traces of TSPs based on the Hacker Ethic that have failed, or at least so far. One example is the attempt to establish a "virtual independence/virtual global community." Despite Barlow's 1996 cyberspace independence declaration – which actualized this TSP, which had previously been shared only among the inventors of cyberspace and the experts using it – actors from the economy and politics populated the Internet from the mid-1990s, and regulations were imposed that were partly adopted from the "real world" without adjustment to the virtual environment.[18] The promise of a self-regulated

18 A consequence of this retroactive or reactive legislative behaviour is the emergence, the ongoing existence, and the exploitation of grey zones on the Internet, e.g. the downloading and streaming of music and movies before it was forbidden by law. The current debates on "hate speech" (e.g. cyber-mobbing), which I would frame as a form of "social engineering," is an example of such a grey zone.

virtual and global community thus failed at stage III, especially because nation-specific regulations fragmented the borderless cyberspace (e.g. current European data protection regulations). With the expansion of the Internet to regions with different sign systems, the story of the Tower of Babel repeated itself in cyberspace: code was no longer the common "language," and language-specific communities, applications, and uses of the Internet developed over time. In retrospect, one might argue that the practice of leaking information was a reaction or a "counter-promise" formulated in response to the failure of the virtual independence TSP: actors from the "real world" imposed their regulations on cyberspace, so actors from cyberspace started to use real-world communication channels to expose the intrigues of these actors, basing their judgments on the Hacker Ethic instead of real-world regulations. The attempt to "domesticate" the exuberantly growing cyberspace can thus be interpreted as a reason why the TSP of the virtual global community failed.

A second reason why TSPs formulated by hackers may have failed – or may have been replaced with different promises – is the setbacks in credibility hackers have experienced since the 1990s. They had always been regarded as devious or dubious (mischievous, in the case of teenagers), but the development of tools to deploy malicious software, or to download media, made it possible for laypersons to commit acts in legal grey zones, or even to commit computer crimes. Since few journalists were familiar with the Hacker Ethic, those fraudulent users were dubbed "hackers," while according to the Jargon File, they should have been called "black hat hackers," "crackers," or "script kiddies," since their behaviour was not rooted in the Hacker Ethic. It can be assumed that this formulation of a rather dystopian counter-promise has contributed to the development of a different hacker discourse; one that regards hackers as criminals. Another setback in credibility is the portrayal of hackers as socially inept and unhealthy computer addicts, which became popular with the evolution of computer games in the late 1990s and early 2000s. This entailed a demystification of the evil hacker and a belittlement of the ingenious, non-evil hacker's ability to interact with virtual systems; and it was reinforced when media representatives attended events such as the yearly DEFCON in Las Vegas, where hackers would also act out their playful and social sides. It would be necessary to investigate this discursive turn of events further to understand how this impacted the perception of hackers both from the outside and from within the hacker communities, but it did weaken the idea that all hackers adhere to a common Hacker Imaginaire – an idea that Levy already foresaw in 1984 by naming different "true hackers" and "hacker generations" (Levy 1984). These setbacks account for a failure at stage II and they led to a de-legitimization of hackers as formulators, addressees, and executors of TSPs from the Hacker Imaginaire.

A third development that blurred the Hacker Imaginaire was the discovery of "the nerd" as a persona, and the portrayal of the hacker as a nerd in popular culture since the late 1990s. The success of cyberpunk science fiction movies like "The Matrix" and of companies like Apple from the 1990s and Facebook from the mid-2000s was linked with the abilities of computer enthusiasts to produce technology for the masses and provided heroes and anti-heroes people could identify with. As cyberculture spread with online games and an entire digital lifestyle, the term "hack" was appropriated by popular culture, e.g. lifehacks and biohacking, and turned "hacking" into a "plastic word," i.e. a term often used but deprived

of a real meaning. However, given the success of the hacker as a nerd, e.g. in the popular US TV Series "Big Bang Theory," it can be assumed that a different hacker discourse has emerged from the popular culture. Moreover, terms like lifehacking and biohacking are successfully established, and they link back to what the hack had originally been: a solution to a self-proclaimed problem. This example shows that the Hacker Imaginaire is still there but has been rethought based on recent technological and social changes, for not only technologies have advanced, but also peoples' perception, understanding, and adoption of them in their daily lives. With social networks, the disclosure of personal information online has been normalized for many Internet users; and the dystopian vision of permanent surveillance has been turned into technoscientific promises in the Internet Imaginaire, such as permanent connectedness with the entire world. Overall, this can be interpreted as a setback in relevance. If something hackers regard as a problem is no longer perceived as such, the sense of urgency may dwindle, which would be TSP failure at stage I.

TSPs in any hacker discourse can be characterized as fragile: their performance depends on successful actualization based on technological innovation; and on keeping up the sense of urgency that legitimizes the formulation and execution of such promises.

Conclusion: recoding futures?

This paper explained the genesis and persistence of a Hacker Imaginaire, derived from the "sociotechnical loop of imaginaries" that emerged with the predecessors of today's Internet. I have connected the Hacker Imaginaire with technoscientific promises hackers formulated on the basis of their Hacker Ethic. It serves as a discursive model practice in that it contains values and implied norms hackers can base their actions on, e.g. decentralization and freedom of information. From a SKAD perspective, knowledge plays an essential role in this hacker discourse: knowledge implies power, and knowledge (or "skill," i.e. the hackers' abilities) is a benchmark for judgment. The failed TSPs from the Internet Imaginaire (e.g. decentralization, freedom of information – unfulfilled, since real-world actors populated the Internet with their economic and political agendas) and the failed or blurred hacker TSPs might be some of the reasons why hackers turn away from non-virtual societal structures. At the same time, turning to real-world structures and using them as means for their ends constitutes a paradox to investigate in further research.

With technological advancement, quasi-global connectedness, and societal changes, the means and ends for hackers have evolved as well. Thinking of the Hacker Ethic as a guide and model to reduce the complexity of the modern world, it seems plausible that hackers would reach out and utilize new technical options to expand the Hacker Imaginaire beyond the borders of synthetic worlds. Old action patterns are combined with new technologies (e.g. the practice of whistleblowing, anonymous protests, or technological self-optimization in the spirit of Icarus), and backed up with different interpretations of the Hacker Ethic, which itself is being adapted according to the sociotechnical environment of its application (e.g. the use of Twitter as a tool to hack state-controlled media communication during the Arab Spring in 2011). The constant stream of technological development also demands the simultaneous actualization of knowledge, uses, and technoscientific promises to fuel

the Hacker Imaginaire; the substructure based on this specific hacker discourse is performed. This cycle of self-contained "sociotechnical loops of imaginaries" can be interpreted as protectionist: hackers formulate and execute their TPSs for themselves and to enforce their visions for the future, to the detriment of actors adhering to real-world societal structures and norms. This either constitutes recoding futures of a limited scope, or something different altogether, namely *decoding the present* by actualizing the Hacker Imaginaire on the basis of ongoing events.

References

BECK, Ulrich. 1992. *Risk Society: Towards a New Modernity*. London: SAGE Publications.

BERGER, Peter and Thomas LUCKMANN. 1969. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York: Anchor Books.

CARDON, Dominique. 2011. "Réseaux sociaux de l'Internet." *Communications* 88: 141–148.

CARR, Jeffrey. 2011. *Inside Cyber Warfare: Mapping the Cyber Underworld.* Sebastopol: O'Reilly.

CASTRONOVA, Edward. 2005. *Synthetic Worlds: The Business and Culture of Online Games*. Chicago: University of Chicago Press.

COLEMAN, Gabriella. 2015. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso.

FLICHY, Patrice. 1991. "La question de la technique dans les recherches sur la communication." *Réseaux. Communication – Technologie – Société* 50: 51–62.

FLICHY, Patrice. 2002. "New Media History." Pp. 136–150 in *Handbook of New Media: Social Shaping and Consequences of ICTs*, edited by L. A. LIEVROUW and S. LIVINGSTONE. London: SAGE Publications.

FLICHY, Patrice. 2007. *The Internet Imaginaire*. Cambridge, MA: The MIT Press.

HAFNER, Katie and John MARKOFF. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon and Schuster.

HARAWAY, Donna. 1991. *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge.

HOLLINGER, Richard C. 1997. *Crime, Deviance and the Computer.* London: Taylor and Francis.

JASANOFF, Sheila. 2015. "Future Imperfect: Science, Technology, and the Imaginations of Modernity." Pp. 1–33 in *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power,* edited by S. JASANOFF and S.-H. KIM. Chicago: University of Chicago Press.

JOLY, Pierre-Benoît. 2010. "On the Economics of Techno-Scientific Promises." Pp. 203–222 in *Débordements. Mélanges Offerts à Michel Callon*, edited by M. AKRICH et al. Paris: Presse Des Mines.

JOLY, Pierre-Benoît. 2015. "Le régime des promesses technoscientifique." Pp. 31–47 in *Sciences et technologies émergentes: pourquoi tant de promesses?*, edited by M. AUDÉTAT. Paris: Hermann Editeurs des Sciences et des Arts.

KELLER, Reiner. 2011. "The Sociology of Knowledge Approach to Discourse (SKAD)." *Human Studies* 34(1): 43–65.

KELLER, Reiner. 2012a. "Entering Discourses: A New Agenda for Qualitative Research and Sociology of Knowledge." *Qualitative Sociology Review* VIII(2): 46–55.

KELLER, Reiner. 2012b. *Doing Discourse Research: An Introduction for the Social Sciences*. London: Sage.

KELLER, Reiner, Anna-Katharina HORNRIDGE and Wolf J. SCHÜNEMANN: The Sociology of Knowledge Approach to Discourse. Abingdon: Routledge

LACKERBAUER, Simone and Matthias ROCHE. 2016. "'Glück durch Innovation'– die Aufforderung zur Problematisierung sozio-technischer Arrangements in der 'Usergesellschaft.'" Paper presented at the Jahrestagung der Gesellschaft für Wissenschafts- und Technikforschung e.V. (GWTF), 2016 (November 19, Berlin).

LACKERBAUER, Simone Ines and Matthias ROCHE. 2016. "Hacking und Tracking – Körperkonstruktion mit Automanipulationsartefakten." Paper presented at the Jahrestagung der Sektion 'Soziologie des Körpers und des Sports' in der DGS, 2016 (April 29, Munich).

LACKERBAUER, Simone Ines. 2014a. *Créer la cyberculture: L'ordinateur personnel, ses usages autodidactes et la montée d'utopies technologiques dans la cyberculture émergente*. Norderstedt: Grin Verlag GmbH.

LACKERBAUER, Simone Ines. 2014b. *La perception différenciée des hackers dans la vie numérique*. Norderstedt: Grin Verlag GmbH.

LACKERBAUER, Simone Ines. 2016. "Hacking Society – Gesellschaft hacken?" Paper presented at the 11. dgv-Doktorandentagung, 2016 (September 9, Augsburg).

LEVY, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. New York: Anchor Press/Doubleday.

MCCARTHY, E. Doyle. 2000. "The Sociology of Knowledge." Pp. 2953–2960 in *Encyclopedia of Sociology*, edited by E. MONTGOMERY and R. MONTGOMERY. New York: Macmillan.

PIAS, Claus. 2002. "Der Hacker." Pp. 248–270 in *Grenzverletzer: Figuren politischer Subversion*, edited by E. HORN and Ulrich BRÖCKLING. Berlin: Kulturverlag Kadmos.

RHEINGOLD, Howard. 1993. *Virtual Community: Homesteading on the Electronic Frontier*. Cambridge, MA: The MIT Press.

ROGERS, Everett. 1962. *Diffusion of Innovations*. New York: Free Press.

STERLING, Bruce. 1993. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam/Doubleday.

TURKLE, Sherry. 1997. *Life on the Screen: Identity in the Age of the Internet*. New York: Simon and Schuster.

TURNER, Fred. 2006. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.

Author

Simone Ines Lackerbauer is Dr. phil. candidate at the Chair of Sociology at the University of Augsburg (Prof. Dr. Reiner Keller), participant in the Graduate School of Humanities and the Social Sciences (GGS) at the University of Augsburg. Research areas: sociotechnical studies, technology and society, discourse analysis, media and communication sociology, translation studies.

Contact: simone.lackerbauer@phil.uni-augsburg.de