Fragile Computing

How to Live With Insecure Technologies

Laura Kocksch

palgrave
macmillan

Fragile Computing

Laura Kocksch

Fragile Computing

How to Live With Insecure Technologies

palgrave
macmillan

Laura Kocksch
Department of Learning and Culture
Aalborg University
Copenhagen, Denmark

The book was originally defended as PhD thesis at the Faculty of Social Sciences, Ruhr University Bochum in June 2022.

ISBN 978-981-99-9806-7 ISBN 978-981-99-9807-4 (eBook)
https://doi.org/10.1007/978-981-99-9807-4

This Palgrave Macmillan imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Paper in this product is recyclable.

To my family.

Acknowledgments

This research was funded by the NRW-Forschungskolleg "SecHuman—Security for Humans in Cyberspace" and the federal state of Nordrhein-Westfalen (Germany). The writing of this book was supported by Aalborg University (Denmark). No book is written alone, nor has academia ever been a lonely place for me. I am indebted to the participants of this study, to my PhD committee, and to many, many colleagues and friends: *Estrid Sørensen, Angela Martina Sasse, Torben Elgaard Jensen, Petra Ilyes, Gisela Welz, Matt Spencer, Lizzie Coles-Kemp, Mace Ojala, Alexander Helm, Katharina Kinder-Kurlanda, Alexander May, Andreas Poller, Mary Shnayien, Dominik Horrion, Georgi Iliev, Kerstin Hüttermann, the RUSTlab, and the TANTlab.*

Competing Interests No financial or personal conflicts of interests are to declare.

Ethics Approval All participants were informed of their participation in the study and signed participation agreements. All participants and institutions are pseudonymized. The study was not reviewed by an institutional ethics board as is common in German academia. The book underwent peer-review.

Contents

1 Introduction 1

2 Testing 19

3 Tinkering 77

4 Training 115

5 Performing 157

6 Fragile Computing 209

References 221

Index 235

About the Author

Laura Kocksch defended her doctorate with honors ("summa cum laude") at the Ruhr University Bochum in June 2022. Since August 2022, she works as a post-doctoral researcher at the Techno-Anthropology Lab (TANTlab), Aalborg University, Copenhagen.

Kocksch completed her education in Cultural Anthropology and European Ethnology, Political Science and Sociology at the Goethe University in Frankfurt in 2016. Since 2014, she has been an active publishing author, reviewer, and publication chair for conference proceedings and journals in Computer Science, STS, and Anthropology. She conducts participant observation, interviews, and mixed-method ethnographies in various fieldsites such as social media, software development, critical infrastructures, universities, and small- and medium-sized enterprises. Kocksch engages with concepts in feminist STS, environmental anthropology and actor-network-theory.

List of Figures

Fig. 3.1 Access policy code (https://aws.amazon.com/de/blogs/security/how-to-get-read-only-visibility-into-aws-control-tower-console/ by Bruno Mendez 2020) 78
Fig. 3.2 Access policy code identity management AWS 79
Fig. 5.1 Two-dimensional model 180
Fig. 5.2 Schematic drawing by a data scientist 180
Fig. 5.3 Simplified drawing by author 181

1

Introduction

Between 2007 and 2010, the "Stuxnet" worm infiltrated industrial machines employed in nuclear energy plants in Belarus and Iran, becoming declared the first-ever cyber weapon.[1] In 2021, the breach of the Colonial gas and oil pipeline caused week-long panic buys and price explosions in the Southern US.[2] Computational systems underlying our critical infrastructures no longer stay idly in the background. They have begun to cause "drama" (Star, 1999).

In 2016, I became intrigued by the use of data science in two large-scale critical infrastructure companies in Germany. When getting field access and talking to data scientists, all they could talk about were the opportunities they were hoping to generate with new algorithms and data sources. Being an insurance and financial company, Covy felt pressure to modernize based on data companies venturing into the insurance industry. Google, they argued, would soon know their customers better than they do, having access to their daily search patterns instead of self-reported health statements. Powino, a subsidiary of one of Europe's

[1] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. For a material semiotic analysis of Stuxnet, see Balzacq and Cavelty (2016).

[2] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

L. Kocksch, *Fragile Computing*, https://doi.org/10.1007/978-981-99-9807-4_1

largest energy companies, argued that new data and data analytics had become essential to coordinate the shift from steadily producing coal and nuclear power plants to decentralized and weather-dependent renewable energy production. The idea circulated that with a modernized data infrastructure, they could remain relevant to an energy market that may sooner or later pivot to locally contained energy sharing economies.

Being educated in anthropology and science and technology studies (STS), I could barely contain my excitement to follow such innovation processes through the work of data scientists. And I could not have been luckier, having entered the companies right at a time when data scientists began building the computational infrastructure that was designed to support new data, tools, and access. When I began interviewing data scientists and joined meetings in their "labs", one issue continued to come up: Data scientists felt their work was held back or burdened with data security and data protection regulations. "The department of no" became a common explanation why a certain data set or tool could not be explored any further. Data scientists were annoyed, or outright furious, that their projects kept being rejected or cancelled by data security officers.

Luckily, they thought, they now had a scientist lurking around, and having no discernible qualifications to help with the data science, maybe she could be of some help with the pesky security department.

I had studied security requirements in developing practices before, assuring them that I had some sympathy for the difficulties to implement security department's wishes in software development (Poller et al., 2017). But my own interest was also piqued: Had I become pulled into the spirit of innovation and renewal that the labs were proclaiming? Within a few days, I had assumed that the most interesting story to tell about these companies was their data innovation, forgetting about the various efforts of developing technologies securely. I had become a manager, in the words of the post-actor-network-theory: I saw the companies through the keyhole of data science innovation—where technologies were planned anew, as if on a plain field; not through the eyes of the security departments where the tedious work of maintaining and repairing prevailed.

What started after this was a one-year exploration of the digital security practices of data scientists and security officers in the two companies. It is a timely moment to study digital security: Technologies, especially

those being introduced newly, are subject to scrutiny of various kinds. Technologies are brittle and frail from their beginning, and continue to be patched up, updated, and prolonged.

Digital security is commonly portrayed as either a matter of technological finesse (writing "good" code, updating regularly, encrypting correctly), individuals' awareness (knowing about insecurity, and being incentivized to do something about it), or regulation (establishing rules). In practice, however, digital security is a site of collective negotiation, material action, delegation of responsibility, and establishing improvised, temporary, and fragile solutions. In practice, digital security illustrates technologies as *fragile*—more "good enough" than robust, more awkwardly patched together than planned out, more dependent on local adaptations than determining them.

The book traces digital security within, in tension and through the process of innovation in the labs, offering insights into ubiquitous, but often mundane practices of securing. Approaching digital security as practice opens it up for ethnographic observation. Four practices are portrayed over four chapters: testing (Chap. 2), tinkering (Chap. 3), training (Chap. 4), and performing (Chap. 5). The four practices are not encompassing, nor do they aim to be representative in any way. But they are not unique to the companies of this study either. Portraying one practice per chapter allows to stay with a way of securing for a while, without falling into the fallacy of judging if security is being done "right" here or there. The four chapters are not to be read independent, nor do they fully add up. They allow to discuss how securing practices conflate, conflict and are coordinated. They may stand in friction, sometimes partially connect. The goal is to "open up" digital security (Liebetrau & Christensen, 2021) by locating it in concrete material practices. By doing so, the chapters "populate" the matter of digital security with a plethora of objects, human- and non-human actors, action and inaction, as Bruno Latour would put it (Latour, 1992).

In contrast to the alluring world of data innovation that the labs so convincingly lured me into, the work of securing is slow, tedious, and "boring" (Star, 1999). Turning away from the innovative technology to mundane worlds of securing resonates with contemporary streams in STS and anthropology. By suggesting to engaging in fragile computing

(rather than innovation computing, let alone computational innovation), we encounter technological practice differently.

Fragile computing does not mean "bad" computing: it does not mean practice that produces insecure technologies. Fragile computing encompasses practices aimed at attending to, maintaining and becoming affected by digital insecurity. Fragility thereby stands in contrast to "vulnerabilities" or "weaknesses"—more common terms in digital security research. What is fragile is precious and delicate; its frailness does not make it worth less, but often more. What is fragile is cared for not to eradicate weaknesses but to curate finesse.

Engaging with digital security as fragile computing allows to engage in competing goods involved in maintaining digital technologies. Securing entails continued worries, being affected by and responsive to technologies rather than solving contained security issues. The material work of securing is more ambiguous and conflicting, or "messier" (Jackson, 2014) than the world of innovation. Fragile computing is located in the realm of maintenance where what is locally "good" may appear "bad" from the distance, and vice versa (Danyi, 2022).

Perceiving of digital security practices as fragile computing allows focusing on mundane practice, their material components and often ambiguous morality. Where technologies are secured, things only partially stick, are improvised, contested, and blamed. Digital securities' "multiple ontologies", borrowing from Annemarie Mol (2003), spawn at such sites of practice. The resulting multiplicity can be particularly disconcerting in security matters: Do we not wish for a "baseline" of security to rely on? Of course! Multiplicity becomes uneasy, precarious, dangerous. This does not mean that we can dream it away. It is important to understand different enactments, not in order to commensurate them, but in order to cherish what is contested; understand its finesse and precarity.

The book concludes with a concretization of the term "fragile computing" by drawing together the four practices and literature in STS and anthropology. Dealing with fragility means noticing the various material flows, attending to what is frail but precious, fluid but refractory. Such attending is partially subverting, relational but not resolving, forges relations over time. Fragile computing does not call for generalist solutions

but thinking that engages in ambiguities and dilemmas. How to live with insecure technologies includes living with fragility, crafting fragile relations and honing abilities to endure, be patient, do and undo. To STS readers, enduring fragility also entails conceptual challenges. It is uneasy to live in fragility which is why the book offers four tactics for research (Chap. 6).

STS and most prominently Infrastructure Studies have pointed out that repair and maintenance remain invisible to the users of infrastructures, this invisibility makes infrastructures seem frictionless and stable (Denis & Pontille, 2015). Being familiarized with every detail of operation may be hindering to the users of a system. On the other hand, it has been argued that any act of adapting (to) infrastructures may be perceived as an act of repair or maintenance in its own right; re-configurating the purpose and needs of a technology in perennial acts of use. Instead of understanding technologies as objects *on* which users act, it has been suggested to understand how they are being acted with, taking their material agency more seriously. To others, thinking with repair not only means decentering the active design from creators to maintenance workers and users but also involves a shift in valuing the entire lifespan of technology and not just their innovation and renewal. This line of thought comes particularly from information studies scholars who have observed a tendency among their own to focus on design, innovation, and deployment, but rarely on decommission, decay, or recycling (Cohn, 2016). In this growing landscape of scholars investigating the role of maintenance practices as well as end-of-life of technologies, recent anthropological literature finds a resonance. Anna Tsing (2015) introduces the notion of "ruins" to capture landscapes and more-than-human entanglements beyond repair and aims to train an "art of noticing" relations that unfold when restoration is no longer an option.

The notion of fragility is employed to point to two connected inquiries: On the one hand, it shifts attention to the instability of information technology—in contrast to perceiving information technologies as instruments of stability (or immutability, in the words of ANT). Whereas often designed to achieve universal functionality, interoperability, and compatibility, technologies are subject to situated action (Suchman, 2006), articulation work (Star & Strauss, 1999), and re-appropriation

(De Laet & Mol, 2000). While their stable configuration—allowing transmission of data, interoperability of programs, etc.—is imperative, they are also "fluid" objects of multimodal relating (De Laet & Mol, 2000). Their success may not lie in them being stable agents of normalization, but in allowing adaptation (Mol & Law, 1994), or their work as stable tools comes into being through them being mendable to others, for example, repair workers (Denis & Pontille, 2015).

The second line through which fragility emerges in is that in digital security debates, fluid forms become problematized and morally charged. When turning into a security risks, adaptations are no longer welcome, they pose a danger. The "human factor" is often considered the "weakest link" in digital security debates (Adams & Sasse, 1999; Squires & Shade, 2015). Re-articulation, re-purposing, and situated action are considered a source of insecurity. When employing the notion of fragile in this book, my intention is not to expose adaptation as weakness, but rather to describe its virtues. What is fragile is not what is ready-to-be-fixed. The practices described in this book do not aim at rectifying insecure information technology, nor are they a source of fragility that must be fixed. Fragile computing includes developing ways of becoming watchful and involved with technologies. There lies a tension here, I want to unfold a bit: If what I said was useful, and fragility emphasizes where adaptations and articulation of information technology is no longer considered playful adaptation of technologies, but judged as problematic, it suggests that it had been unproblematic so far. This is, of course, only partially true as studies in post-ANT have argued. Being not the intended user of a system has always been a source of tension (Star, 1990), but now these tensions become more pertinent and shameful.

Another aspect of the tension is that in infrastructures, maintenance work is considered invisible and staying in the background, but in fragile computing, they become vocal and demanding. So far so that they begin to enroll users—those that were in the privilege of "just" enjoying the stability of the systems when they did not engage in repair work (Denis & Pontille, 2015). This unfurls the topologies of information technologies introduced by ANT and post-ANT further: immutable stability becomes trenched with demands of maintenance and mutable fluidity becomes risky. It is, thus, necessary to take fragility seriously: its reach and morality.

Part of this endeavor is to halt judgment for a moment. For example, judgment of users' articulation work. When divergence of designed purposes become a security risk, scholarship in actor-network-theory (ANT) suggests asking whether we should aim for utopian strength or try to understand more fluid forms (Law, 2000; Law & Mol, 2002a, 2002b). In such, security oscillates, is ambiguous and complicated. Halting judgment means not to avoid this complication, but to engage with it actively. I put forward an understanding of such fluid and uneasy digital security; or where computational practice becomes *fragile*.

The empirical chapters unfold how security is negotiated, partially achieved, postponed, distributed, etc. while staying responsive to the need to secure. We can neither overlook such situated fluid action, nor can we overlook security requirements. But commonly, security is alien to a fluid thinking: security requires discerning between areas of security and insecurity, building "parameters" (the military narration is obvious), or more recently "zero-trust"-relations (Spencer & Pizio, 2023), which, in turn, strengthens the imagination of technologies as being located "in" the social world (a company, a school, a car) with clear boundaries between the two (Sørensen, 2009). Topologies that are imperative to securing may be partially incommensurable to fluid forms of technological adoption as put forward in ANT. A sensitivity to this trouble of topologies is needed. Fragility includes this trouble: What is fragile is both fluid and contested, both precious and precarious.

Fragility has been discussed in relation to the temporality of infrastructure, for example, their decay over time (Ramakrishnan et al., 2021), or active tempering (Denis & Pontille, 2015). As a material condition, fragility points to the agency of objects, and trains abilities to recognize and attend to materiality (Denis & Pontille, 2023). This requires a shift in thinking from innovation and renewal toward repair and maintenance (Jackson, 2014). Fragility is not only a material condition but also a way of thinking about living together with decaying things and infrastructures. To Mol (2008), accepting fragility is part of the "logic of care" that is distinct from the logic of choice. In the logic of choice, informed rational subjects make decisions, separating them from the complications of the issue of hand. In the logic of care, it must be endured that not all things are rectifiable. Living with fragility then means engaging with mess—both

in the sense of maintenance work (where things get dirty), and in the sense of moral ambiguity (where things are not simply right or wrong). While as material condition, fragility can be the outcome of isolated incidents (vandalism or accidents), or gradually (over time), in the reading put forward here, it is also "normal", but uneasy to admit to (Perrow, 1999).

The book offers four situated enactments of digital security. In two, digital security is marginal, and secondary, epitomizing it as invisible and subversive work, while in the others, it is put on stage, rendered explicit in performances of testing and training. While each chapter presents socio-material practices through which digital security is enacted, taken together, they provide an impression of the multiplicity of the object of study and the need for not one but a variety of conceptual approaches to open digital security for studies in STS.

- **Testing** demonstrates how digital security is performed in different shapes or "patterns of relation" (Sørensen, 2009, p. 70). Applying such a topological lens inspired by STS literature allows us to specify how practitioners perform digital security in different forms, each producing a different outcome of what "good" security means and can be assessed. Testing practices do not solely aim at producing assurance but must also endure ambiguity and inconclusiveness.
- Following two developers while they write access control policy code, **Tinkering** offers an opportunity to learn how digital security is enacted as meticulous and situated practice that is engaged with conflicting moralities. Setting access control policy code is a material and moral practice. It requires practices of trying and failing, honing one's abilities of noticing, overflowing formal organizational roles and creating long-term relations. The chapter proposes to perceive of such handling of fragility as involving care. Caring is not aimed at solving the difficulties of setting access code once and for all, but about negotiating what is acceptable in a specific place and time. Care—drawing on the work of doctors and nurses—involves bending the rules and turning advice into livable or workable guidance for specific patients (in this case colleagues). Caring means handling fragility, where there is no light at the end of the tunnel.

- Reflecting upon my participation in an emergency **Training**, digital security in this chapter is discussed as both an event, and a long-term organizational practice. Before the training, many efforts go into creating a digital security emergency, for example, secrecy, warning texts, and measuring response times. During the training, participants, however, rely on knowledge they have built long-term and in attuning to each other. During the training, digital security becomes a matter of testing out options against previously acquired knowledge and attempts to limit harm. Instead of prevention, the training is aimed at preparedness for an emergency that reaches beyond its time-limited occurrence. In the ceremonial exercise, digital security includes creating an organizational stand-by—a state of attention to what is not to prevent.
- Finally, by looking at how digital security contributes to changing practices of **Performing**, the last chapter points to how digital security relates to practices of data innovation. The chapter follows the transition of the companies from a domain-specific to a centralized data storage and management, laying the foundation for new data science applications. In processes of innovation, digital security has an ambivalent function; both creating resilience and warning, supporting renewal while reminding to slow down. The chapter unfolds how digital security is pivotal in building trust in numbers and developing relevant inquiries for other's data.

By focusing on the four practices, the book offers accounts of enacting digital security—performing it locally, and often diverging from standard definitions. Each practice negotiates what security means in a particular setting, sometimes more obviously (by setting numeric standards of secure/insecure), sometimes less obvious (by trialing and testing until a security function is "good" enough).

Each chapter outlines different practices of doing digital security—some of which may lie in the realm of security experts, others in the area of other fields. I have made no difference between the two as my aim was to focus on the concrete material practices of enacting digital security, not on a judgment of whether such security was done "right" (according to regulation). What is fragile is prone to break down, it may not persist.

Developers, security officers, and data scientists deal with this possibility of breakdown and ending. This is not a nice and cozy world, you may think. It is a world where things go wrong, where people are blamed. But it is the world where digital security is configured in action.

The episodic approach taken here assumes that there is not one whole of digital security to be captured, and objective reality to elicit, but rather that "it" is enacted through situated practices. In "enactments"—the practicalities in which ontologies are bound up—Mol (2003) suggests, "there is no longer a single passive object in the middle, waiting to be seen from the point of view of seemingly endless series of perspectives. Instead, objects come into being—and disappear—with practices" (p. 5). The four practices portray digital security not as a matter of incompliance from a pre-set definition of security, but more precisely as sites where multiple securities emerge, meet and conflict.

Ontologies of digital security become "coordinated", conflate and may contradict (Mol, 2003). Digital security becomes *multiple*, yet not plural. Connections between the chapters are noted, yet many frictions remain (Tsing, 2004). The chapters are isolated but also connected—through the companies they are part of or through their common interests in securing. But the chapters are also in isolation and can be partially contradictory or antagonistic. Not all of them come together in a coherent way. To Mol, such valuing of practices demands the renaming ethnography into "praxiography" (Mol, 2003; Heuts & Mol, 2013).

A methodological question ensues: How should one describe digital security as fluid practice that is observable to praxiographic methods? Methodologically, this requires getting access to and staying with technological practice for such an ephemeral object like security to "appear" (and "disappear") or for interlocutors to point it out to us (or point out its absences). It requires attention to what is hidden away and rendered organizationally invisible. And it asks for the building of rapport and noticing of awkwardness and moral imperatives induced by the presence of a researcher who investigates security. After all, making visible in/security is risky; an ethnography of it could be itself "hacking" that exposes insecurities. Ethnography means recording, taking notes, and documenting what is often unspoken (Hirschauer, 2001). It requires gaining access to practices that are tediously concealed in order to be effective (Sundaramurthy et al., 2014).

To become part of a company, one has to follow its security guidelines, or put differently, following digital security guidelines makes you become part of the company. Throughout this journey (that requires deference to security rules), an ethnographer is able to trace why and for what reason workarounds or contentions are performed, which, in turn, improves our understanding of incompliance and "problematic" behavior. Ethnographic details can complement previously mentioned approaches because it emphasizes the situated and continuous efforts and troubles. Digital security lies in the everyday and is often approached in between or in addition to other things. These can only be observed when being present in person and feeling and going along with people's life and work.

My presence in the field, informants, scientific colleagues, and materials all co-created the research as I present it here. Taking the contingency of my ethnography as a starting point helps to describe my ethnographic journey, challenges, and moments of surprise. Paying attention to the practicalities of the ethnography endorses the situatedness of the researcher, where she comes from, what she intends, and also how intentions shift. Ethnographers are often confronted with complicated decisions and practical constraints that are rarely captured in Method handbooks. Attending to the "here-and-now practicalities" (Sørensen, 2009, p. 10) is important to present the ethnographic method as contingent and not simply resting on the ethnographer's choices. In my case, these practicalities included wrestling with my object of study occasionally: Gaining access as ethnographer while not becoming a hacker or "spy" (Boas, 1919) myself. While "co-laborative" research in STS and anthropology has been praised for moving ethnographic practice away from the armchair and into the direct collaboration with those being studied, studying corporations is rarely considered (Niewöhner, 2016). The insurance and energy industry, in particular, may be rather critiqued upon than allied up with by anthropologists or STS scholars. A "mutual skepticism" (Liburkina, 2021) may even exist. As the description of entering the field earlier in this chapter has proposed, however, I did become a collaborator to the field: they hoped I could mediate in a conflict between data scientists and security departments. And I attempted to live up to their expectations by presenting results of my study in both arenas, aiming to familiarize each with the other's work practices and incorporated logics (e.g., of playfulness and experimentation in data

science and of assurance and maintenance in digital security). The embodied presence of the ethnographer as a third party in this setting allowed for modes of co-laboration with industry actors that may not align with my own views or agendas. While collaborations with activists and even policy makers in STS and anthropology are more common (as political goals more often align), the willingness for situated co-laboration may be required to study fieldsites like mine, and I did not feel betraying my beliefs in moderating a looming friction in the field.

A second challenge emerged, however. While ethnographies of digital security are still scarce (Dourish et al., 2004; Squires & Shade, 2015; Kocksch et al., 2018), they have proven valuable to investigate individual's mental models (Sundaramurthy et al., 2014), group's opinions and perceptions of digital security (Palombo et al., 2020), or organizational responses to changed security policies (Poller et al., 2017). However, following debates in Human-Computer Interaction, anthropological ethnography is not solely a "tool" that can be added to existing methods of extracting information from a field (such as interviews or quantitative surveys) (Dourish, 2006).[3] Rather, ethnography has a commitment to develop "theoretical descriptions" (Hammersley, 1990): it aims to conceptualize through empirical stories, instead of fitting into theories off the shelf. Put differently, ethnographic engagement with digital security means unsettling its established preconceptions, and ontology. Instead of "applying" ethnography to pre-established understandings of digital

[3] Computer scientist Paul Dourish insists that computer science should take ethnography's conceptual contribution more seriously, for example, that there is not one "truth" to uncover about technological practices, that they are enacted in multiple ways (Dourish, 2004). Ethnographers are not "tape recorders" to bring the "reality" of technological use into engineering labs. Part of the debate is whether engineers can "simply" acquire the competencies of conducting the material work of ethnography without becoming familiar with the origins of ethnography in critical anthropological research (Forsythe, 1999). Reducing ethnography to a set of techniques may "underestimate, misstate, or misconstrue the goals and mechanisms of ethnographic investigation" (Dourish, 2006, 542). To Dourish, assessing ethnography by how well it develops "implications for design" falls into a fallacy as it underestimates ethnographer's abilities to uncover underlying assumptions and commitment that things could be different. As anthropologist Marilyn Strathern writes: We must understand ethnography's role "not as adding more of the same […] but as the intermeshing of different orders of phenomena, having to take certainties and uncertainties together" (Strathern, 2002, 312).

security, I understand ethnographic practice as a mode of theorizing digital security differently. This also means that it is not a sole method of data extraction from a field, but carefully engages with a field in moving along while also situatively juxtaposing oppositions of the field. It is a practice of both immersion into and alienation of the parties in a field (Emerson et al., 2011). This book is written as a series of practices that overflood the pre-set ontology of digital security. Instead of asking how well actors "perform" or "comply", these practices are "opening up" digital security (Liebetrau & Christensen, 2021).[4] What is secure/insecure becomes an empirical question. Other questions result from it: What is "good"/"bad" security in a specific practice? How to live with less-than-optimal security? and so on. The contribution of my ethnographic study of digital security does not lie in providing solutions, that is, by explaining human behavior, but in crafting stories that immerse us, and allow us to halt a moment, be surprised and even stumble.

Although it is imperative to understand that ethnography is not a tool that can be judged by how well it produces insights for existing digital security research, the book offers nine implications that should be both useful for readers in computer science and in STS or anthropology. By choosing the format of implications, the book aims to abstract from the practices described here and suggest that, although not aiming for representativeness, the empirical stories and the conceptual repertoires that are developed through them is relevant "elsewhere". Implications will have to be tested and trialed further.

Each of the empirical chapters puts the focus on one practice of digital security: testing, tinkering, training, and performing. Each empirical chapter develops terms and concepts in relation to the empirical material. This performs the work of theorizing digital security as practice, while staying partially inconclusive. Perceiving of concepts not as exclusive and

[4] Ethnographic writing, anthropologist Anand Pandian notes in reference to Kathleen Stewart, "tries to let the otherwise break through, to keep it alive, to tend it" (Pandian, 2019, 7). Ethnographies are exactly that: they tell different stories than other methods; they focus on what is not easily focused on. Or as Pandian puts it, they "rob the proud of their surety and amplifies voices otherwise inaudible" (ibid.). "Writing with care", he continues, is a form of "letting things be vulnerable and uncertain" (Pandian, 2019, 14).

convoluted, but as "companions" (Winthereik, 2020)[5] emphasizing some nuance (leaving aside others) creates a needed arena to theorize digital security. This can be understood as a playful engagement with theories, testing and trialing them in conversation with the empirical stories and interlocutors. This playfulness is intended: What does the "use" of concepts (for lack of better terminology) do to the field; to its relations and in/consistencies?

Conceptually, the four chapters offer (symmetrically) descriptions of practices that enact "expert" versions of digital security such as testing and trainings, as well as more subversive versions such as haggling over access control policies or negotiating data confidentiality.

I could have pointed to similar themes in each practice, but decided to give them more characteristic traits, while also provoking before-established terms and categories across them. Taken together, the chapters, however, do not convolute into a new theory of digital security. The goal is to open up digital security for STS and anthropology by offering some conceptual tools (others are possible and encouraged). This explores the additive value of thinking with tried and tested STS themes in connection with digital security. This does not attempt a critique per se on existing approaches in digital security (nor on STS concepts, for that matter) but aims to contribute new heuristics to the respective repertoires. This is not devaluation of existing approaches to digital security, such as usable security, mathematics, and engineering (in fact, those are imperative in many regards), but simply an opening of a new conversation about digital security based on the realization that the issue may be of increased complexity. The book equips us with examples, ethnographic anecdotes, and concepts to further our understanding of digital security in the current time. It argues for the purchase of multiple conceptual repertoires that are partially, but not fully, commensurable. Reiterating a commitment in STS and ethnography to opening seemingly settled definitions by rendering them as empirical objects, this book suggests new vocabulary and alternative modes of thinking and doing digital security.

[5] Brit Ross Winthereik suggests "concepts as companions" that travel with us through the field and become—like the ethnographer—changed through the encounter. "Concepts companions can help open worlds, but they can also be too loud and talkative to the already quite heavily populated places we visit during ethnographies" (Winthereik, 2020, 30). Concepts are not only companions to ethnographers but interlocutors as well. Ethnographers are sensitive to such concepts in the field, as well as their contradictions or hierarchies. This sensitivity allows for juxtaposition of concepts that are prevalent in the field (e.g., definitions of security) with concepts that we "bring".

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46. https://doi.org/10.1145/322796.322806

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cybersecurity. *European Journal of International Security, 1*(2), 176–198. https://doi.org/10.1017/eis.2016.8

Boas, F. (1919). Scientists as spies. *The Nation, 27*. https://doi.org/10.1111/j.0268-540X.2005.00359.x

Cohn, M. L. (2016). Convivial decay: Entangled lifetimes in a geriatric infrastructure. In *CSCW'16 Proceedings and companion of the ACM conference on computer-supported cooperative work and social computing*, San Francisco, CA, pp. 1511–1523.

Danyi, E. (2022). *Melancholy democracy: Politics beyond hope and despair*. Habilitation submitted, Institut für Soziologie, Goethe-Universität.

De Laet, M., & Mol, A. (2000). The Zimbabwe bush pump. *Social Studies of Science, 30*(2), 225–263. https://doi.org/10.1177/030631200030002002

Denis, J., & Pontille, D. (2015). Material ordering and the care of things. *Science, Technology, and Human Values, 40*(3), 338–367. https://doi.org/10.1177/0162243914553129

Denis, J., & Pontille, D. (2023). Cultivating attention to fragility: The sensible encounters of maintenance. In *Ecological reparation* (pp. 344–361). Bristol University Press.

Dourish, P. (2004). What we talk about when we talk about context. *Personal and Ubiquitous Computing, 8*(1), 19–30. https://doi.org/10.1007/s00779-003-0253-8

Dourish, P. (2006). Implications for design. In R. Grinter (Ed.), *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 541–550). ACM.

Dourish, P., Grinter, R. E., La Delgado Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing, 8*(6), 391–401. https://doi.org/10.1007/s00779-004-0308-5

Emerson, R. M., Fretz, R. I., & Shaw, L. L. (2011). *Writing ethnographic fieldnotes* (2nd ed.). The University of Chicago Press.

Forsythe, D. E. (1999). "It's just a matter of common sense": Ethnography as invisible work. *Computer Supported Cooperative Work, 8*(1–2), 127–145. https://doi.org/10.1023/A:1008692231284