Investigating the Sustainability-Cybersecurity Nexus in HCI as a Practical Problem

Presented at Workshop WS27: HCI for Climate Change: Imagining Sustainable Futures

CHI-2023, Hamburg 28 April 2023

Laura Kocksch*

The Techno-Anthropology Lab (TANTlab), Aalborg University, laurak@ikl.aau.dk
orchid-id: 0000-0003-4661-2638

Estrid Sørensen

Ruhr-University Bochum, estrid.sorensen@rub
orcid id: 0000-0002-3131-9415

When being explored as a practical problem, ecological sustainability concerns conflict, align and coalesce with other substantial interests of HCI. In our analysis, we focus on the entanglement of sustainability and cybersecurity, i.e., on the sustainability- cybersecurity nexus. The growing attention to sustainability in HCI interventions and recommendations has so far been outward facing; addressing policymakers, administrators or users. By exploring sustainability as a practical problem this paper invites a new audience to the sustainability debate: HCI itself as a community of designers, developers and socio-technical engineers. We seek to develop further the inward-facing gaze that has recently emerged in (S)HCI by asking: how can the design of technologies and the socio-material practices they enable be crafted in a more sustainable manner? And, more profoundly, what *is* sustainability in the design, deployment and discarding of IT systems? Based on ethnographic fieldwork, we discuss three ways in which sustainability and cybersecurity are entangled in practice: by design, by maintenance, and by hesitation.

Keywords: Ethnography, Climate Change, Digital Security, Practice, Hardware, Impact on environment, Security and privacy.

1 INTRODUCTION

In this short paper, we suggest sustainable HCI (SHCI) debates can benefit from investigating how practices of designing, maintaining and discarding IT systems entangle sustainability issues with other design matters. Our focus is on sustainability and cybersecurity, or, on the sustainability-cybersecurity nexus. Within this nexus, various tensions or partial alignments of sustainability and cybersecurity are practically negotiated. This offers an inward-facing gaze that addresses the practices of software and hardware engineers, user experience designers, IT admins and others contributing to the development and deployment of technologies in (academic) organizations. These have rarely been considered in SHCI, which has primarily focused on users and policymakers [1]. We concur that “we should question the amount of data and

* Place the footnote text for the author (if applicable) here.

energy that things we design currently consume, and that force others to consume in order to engage with us" [2]. We urge furthermore to include perspectives of everyday socio-material practices in the debate. Based on three ethnographic studies we describe practical negotiations that our fields were caught up in when attempting to design, deploy or discard technologies in sustainable ways. We uncover tensions between the demand for making technologies more secure and the will to make them more environmentally friendly. Desires to develop and deploy technologies as energy-efficient, resource-saving and without impact on biodiversity on the one hand, and on the other to make them secure and redundant to withstand security risks such as cyber-attacks co-exist, conflict or partially co-align in practice. Both cybersecurity and the environmental impacts of hardware and systems have gained importance in CHI and wider debates on the role of technology in society. Our contribution is to draw these concerns together and portray their entanglement and situated calibration.

According to recent studies, 40% of the internet's carbon footprint can be attributed to the design of websites, i.e., dynamic instead of static, high-resolution images or making use of a fanciful design [1]. Authors in HCI suggest a series of design instructions that can help reduce the energy footprint of websites such as employing a solar-powered server [1]. Such technological measures are key to reaching more sustainable HCI, yet they are not easily scalable and practically inefficient for large-scale organizations such as those of our studies. We thus suggest widening the scope of such in-ward-facing SCHI to include infrastructural-systemic and organizational-practical dimensions of (un)-sustainable IT.

It has been noted that commonly known design criteria may conflict with developing sustainable systems such as intermittence [1]. Intermittence is commonly considered a failure of a system that aims for maximal availability. However, as the authors argue, for a sustainable system in a certain organizational context a certain downtime may be acceptable. We conclude that aiming for more sustainable systems requires constant weighing, balancing, negotiation and prioritization, which is best observed in practice. Our approach engages with sustainability as a practical problem. Its complicated relationship to cybersecurity serves as a case in point: For example, although rigorous data backups are advisable from a security standpoint, filling servers with 'unused' data takes up additional energy and processing resources. Or while encryption protocols are essential to assure protection from eavesdropping attacks, they require enormous amounts of processing capacity. Our empirical studies indicate that the pursuit of sustainability in HCI is not a straightforward task but a practical negotiation and that a more nuanced understanding of the practices grappling with the sustainability-cybersecurity nexus is needed.

2 RELATED WORK

SHCI looks back at a more than 15-year history and incorporates various sub-streams. We focus this related work section on the question of how SHCI streams are particularly well-equipped to study the relationship between sustainability and cybersecurity (for a comprehensive review of SHCI, see [3]). We argue that attending to the practical tensions of a nexus of concerns, such as sustainability and cybersecurity, is particularly well placed in SHCI.

SHCI aims to limit environmental consequences related to computing technologies, on the one hand, and employing computing to help effect pro-environmental behaviors, on the other [3]. The latter stream has successfully developed tools and visualizations to persuade users to adopt sustainable behavior and engage in self-reflection, leading for example to more sustainable food choices [4]. This stream has received critique for its limited evidence of lasting and scalable effects and, perhaps more fundamentally, for its purporting of ecological responsibility as a matter of individual behavior [5]. Bremer et al. indicate a turn "beyond persuasion" in SHCI that has pivoted into a critical assessment of technological fixes in general [3]. We concur with their position that HCI should not fall into solely conceptual work, but harness influences from various fields. Instead, SHCI's unique attention to materiality (the first stream) is of particular value. Taking this

focus seriously requires investigating the practices that are related to devices and hardware. The ambiguous effects the sustainability agenda can have – for example when it stands in tensions with kindred concerns such as cybersecurity – are best observed in this socio-material space. We thus frame our approach as both inward-gazing (as it targets the material designs of HCI) and practice-oriented (as it analyses organizational tinkering with devices and hardware). Approaching sustainability as a practical problem portrays it as a matter of distributed responsibility and long-term commitments that are negotiated in everyday material encounters. This decenters sustainability from being either a matter of materiality or individual human action.

As a consequence of the turn described by Bremer et al. [3], SHCI has begun to invite broader debates of 'good' sustainability, prioritizing local practice as a source of ethics over abstract ideals [6]. A perspective we resonate here by stressing the practical rendering of IT, including ongoing efforts of maintenance [7, 8]. Jackson's work, in particular, urges us to find appreciation for the fragility of IT systems instead of their robustness, inviting in more ambiguous ethics. His proposal of "broken-world thinking" exemplifies a way of acting and thinking differently about IT than aiming for solutions and progressing forward – a thinking resounding with contemporary anthropology, most conspicuously with the works of Tsing [9]. Having undergone its own turn beyond persuasion, SHCI can have galvanizing effects in other sub-fields of HCI such as cybersecurity, where persuasion motives are still widely prevalent.

3 THREE EXAMPLES OF PRACTICAL TENSIONS IN THE SUSTAINABILITY-CYBERSECURITY NEXUS

This short paper is the result of conversations about SHCI from the perspectives of two different ethnographic studies. The first (discussed in 4.1. and 4.2. below) attends to the practices of planning, constructing, maintaining and using a data center at a German university. The second study (4.3. below) evolves around the IT systems of small and medium-sized enterprises (SMEs) in Denmark and takes their distributed socio-material tactics to withstand cyber-attacks into focus. Both studies attain the core principle of understanding the collective and situated work of their respective fields. The authors of this paper have done some of these studies together, some separately, and have been in regular exchange about their respective progress. It was in these conversations that we came to notice unexpected relations between sustainability and cybersecurity across the field sites, which motivated the combined analysis presented here. Our aim is not to point to a "best practice" of relationships between cybersecurity and sustainability, nor to offer solutions for this. Rather, as an alternative to always necessarily requiring "more" cybersecurity and "more" sustainability, we offer our observations as a platform for more ambitious reflections on and debates about how cybersecurity and sustainability are - and can be - problematized in various ways.

3.1 Sustainability by Design

"The university is planning the construction of a new and ***secure data center*** *with the aim of the goal of modular expandability of the building in order to be able to bundle large-scale consumers and thus achieve synergy effects in the* ***energy supply*** *and optimize it"*[1] (emphasis added). This is the first sentence of the 2014 feasibility study for the design of a university data center, which is our ethnographic field site. The sentence combines security and sustainability (here energy efficiency) as a core of the design process. Early on, the university decided to design a data center with the availability class TIER 3. This means that data are guaranteed available 99,9 - 99,99 % of the time, which is equivalent to a max downtime between 52,6 minutes and 8,8 hours per year. This came to be a design promise that any activity and any

[1] The quotes in this section stem from the feasibility report of the university whose data center is studied. In agreement with the participants the university is anonymized, and accordingly, we cannot disclose the reference to the feasibility study.

measure had to contribute to delivering. The risk of not keeping the promise became immanent in the design process, and a security issue was born: How to prevent risks of compromising the TIER 3 promise? The feasibility study states an abundance of security issues: flooding, groundwater rise, firefighting water; lightning, over-voltage, electro-smog, electromagnetic radiation; fire loads and corrosive fumes; unauthorized access (burglary, vandalism (e.g. by disgruntled students), plant espionage, theft, sabotage); explosions, terrorist attacks, airplane crashes; weaknesses in the construction; deficiencies in the safety concept; failure of the energy supply; and failure of air conditioning, among others.

Although considerably less than security the feasibility study also addresses environmental issues: "*The area has a steep slope and has an old, powerful tree population*", it is stated about a potential building site for the data center. However, the following sentence turns the matter into a security issue: "*The intervention in this 'green zone' could well be difficult from an environmental point of view since resistance to clearing seems very likely here*". Further, the matter is also pointed to as managerial and economical: "*As compensation for the interventions in the forest, extensive replacement reforestation or other additional ecological enhancement would have to be agreed upon"*. This reading of a few sentences of the feasibility study is exemplary of how sustainability came to matter – or not – in the design process. There was indeed attention to environmental sustainability, but sustainability issues were recurrently transformed into issues of other kinds, leaving the environmental focus behind. Issues of sustainability also recurrently came up in conversations with our interlocutors, such as ideas about renewable energy supply for the data center, the reuse of heat waste as well as emergency power generators operating without diesel.

However, the TIER 3 promise and the security mentality of the several data center norms guiding the design made security a more important issue than sustainability throughout the design process. Although security and sustainability seemed to be in conflict in the design of the data center, and although security issues routinely gained more priority than sustainability issues, it is wrong to conclude that the sustainability-cybersecurity nexus was a zero-sum game. Security issues were central in the design process, but the energy-saving potentials that came with centralizing the university's IT infrastructure were a substantial sustainability factor. The many small servers and server rooms scattered around campus required an extensive energy supply, and centralizing these into a data center already saves considerable energy.

3.2 Sustainability by Maintenance

In our interviews about storage practices with scientists involved in data-intensive research additional facets of the sustainability-cybersecurity nexus emerged: In the maintenance of technology lies both challenges and opportunities for sustainable and secure IT, and that different logics of security may also be entangled with different logics of sustainability. The scientist-users of the data center were meticulous about deleting data [10]. They abided by different deletion practices, such as rigorous deletion schedules (every Thursday) and tactics for sieving through data sets to sort out obsolete data or data as by-products of calibrating apparatus or algorithm testing. While storing data was supported by standard procedures, deleting was more improvisational and tedious. Data deletion was for many of our interlocutors a routine practice to maintain both data, long-living machines and energy efficiency, and as such we understand them as sustainable HCI.

For scientists, deletion practices were also about keeping machines lean and not overwhelming the capacity of fragile and older hard drives. They kept these close under desks, in the corner of offices, or locked cupboards. *"Listen... someone is making a complex calculation"*, an interlocutor noted, making us notice a monotonous purring in the background. Scientists were closely acquainted with the sound, feel and well-being of their data and servers. With the transfer of data to the university data center such intimate maintenance becomes obsolete. The data center was "autonomous," and scientists were not allowed access to servers. As one scientist remarked, his old machine *"may not make the move"* to the new data center, something that concerned him as he did not want to waste *"still good"* IT. The IT staff derogatively talked about this as

scientists' desire to *"cuddle their servers"*, and they pointed to the lack of security involved in this practice: Not only was the risk of losing data higher when servers were distributed across the campus' furniture, also theft was easier. The intimate relation to data and servers as a form of maintenance of local machines conflicted with the security goal of making data available, durable and reusable (a prevalent goal in contemporary sciences, [10]). The security logics of the remote data center conflicted with the security logics of being well-versed in the material components of IT systems and knowing how to maintain the integrity of data, e.g., keeping data sets clean. These were at the same time different sustainability practices. The servers that were kept local and "cuddled" by scientists were shut down when not needed – sometimes waiting on hard drives in cupboards for years for someone to reuse the data. This indeed saved energy compared to the data center's 99,99 % uptime. However, according to the data center staff, intermittence of services in the data center conflicts with the longevity of servers that are vulnerable to being booted on and off, and thus are rather kept running. A key issue of the sustainability-cybersecurity nexus is how technologies can be designed that combine the needs for security and backups with deletion and with keeping data lean to reduce energy use and the stress of machine occupancy. In the maintenance of technology lie both challenges and opportunities for sustainable and secure IT, and different logics of security may also be entangled with different logics of sustainability.

3.3 Sustainability by hesitance

The previous two examples have illustrated that sustainability and security emerge and are engaged with in concrete actions of designing or maintaining technologies. During the visit to a large industrial printing shop in Denmark, one of the authors encountered a different tactic that provokes further contemplation of how sustainability and security are intertwined.
While I sneak through a narrow path between two truck-size printing machines, my interview partner reports that "business has declined the last years". I am not surprised to hear this in a printing shop located in Denmark (which often paints itself as one of the most digital countries worldwide). The company has specialized in printing advertisement leaflets for grocery stores and lottery tickets, but most of their earnings derive from sending SIM cards. The SIM cards are shipped to them physically and stored in a secured room in the basement. Meanwhile, they have access to an sftp-server to download the respective customer data from the telecommunications company in order to match the right SIM card to the exact customer and merge both physically by attaching the SIM card to a printed A4 paper. *The interview partner interrupts his explanations to point to one of his most critical technologies for this purpose: 4 black floppy disks are neatly arranged on a desk next to an outdated-looking PC station that is connected to the printer we stand squeezed next to. The floppy disks are essential, he explains, to transfer data from this Windows NT machine to the next-door printer. The Windows NT machine is connected to a Windows XP machine that "translates" to a Windows 10 office laptop that can retrieve the data from the sftp-server. Such a complex arrangement is necessary because the old printers that are highly specialized, accurate and well-known by the workers were purchased in the 1990s and Windows NT is the last operating system compatible with them. And even if, the interlocutor speculates, one could replace the one printer, then the printer next door becomes inoperable as well as nothing can write the floppy disks anymore. He assures that the Windows NT and XP machines are secured by a firewall from the Windows 10 machine, but indicates that this is nothing to invest money or time in.* The episode reports a typical clumsy-seeming arrangement of legacy technology and more recent data storage techniques. The interlocutor is very concerned that his crucial technology may not be replaceable anymore as floppy disks and Windows NT machines are no longer produced. And while the large printers are energy intensive, the IT solutions connected are considerably low-maintenance. When attending to sustainability and security, the company does not design new features from scratch or is able to make meaningful maintenance or repair decisions. Rather they stick with what they have. This denotes a taint of *hopeful pessimism* where the printing business is precarious and possibly deemed to disappear

sooner or later anyway. The sustainability-cybersecurity nexus is attended to not by renewal, nor by repair but by hesitating and being patient with a clumsy solution that currently works. This does not mean that the company does nothing; they must hunt for floppy disks at yard sales and endure a complicated firewall arrangement.

4 DISCUSSION

The three analyses offer openings to ruminate about the intersections of sustainability and security:

Sustainability and cybersecurity oscillate. One being in the focus moves the other to the background. During the planning, construction and application of the data center, cybersecurity was the focus. Later, it moved to the background as energy costs and sustainable maintenance became more pressing. When saving data, security is of critical concern, but when data grows older or becomes obsolete, sustainability may prevail. Sustainability and cybersecurity ebb and flow. The examples above do not portray this oscillation as a simple matter of a shift in awareness or mental capacity, but rather as a practical necessity: Attending to cybersecurity complicates sustainability considerations as they are substantially divergent modes of action: saving data vs. saving storage, assuring data ownership vs. centralizing data, etc.

Neither sustainability nor cybersecurity are comprehensively solved. Rather than aiming for final solutions, all episodes above have portrayed sustainability and security as perpetual and ever-ongoing. Neither is achieved once and for all nor is there a definitive goal. We conclude from this for SHCI debates that sustainability and security alike are no simple features to be added to any given system. This summons a wider debate about whether climate change can at all be escaped or avoided. A narrative that may be misleading at best and potentially dangerous as it has the potential to neglect the real consequences already experienced by many. The three examples suggest a different mode of attending to pressing issues of HCI – the sustainability-cybersecurity nexus – by staying involved with and enduring uncomfortable knowledge.

Noticing ambiguities between conflicting goals contributes to a new understanding of sustainable HCI. Lastly, as scholars in contemporary anthropology and science and technology studies have suggested, it might require a more fundamental rethinking of progress narratives. Instead of escaping climate change by finding last-minute solutions, we might do good in appreciating other modes of action such as maintenance, care and hesitance. These aim for dealing with what is at hand, engaging in here-and-now practicalities and becoming honed to handle ambiguity. Living in "ruins" rather than progress, Tsing contends entails engaging in uneasy relation-making [9]. Rather than pursuing an abstract good, acting beyond progress requires constantly grappling with conflicting goods and engaging in practical perennial negotiations. What we might arrive at are local improvisations that make things *slightly* better or worse but are never complete.

5 CONCLUSION

Aiming to perceive of sustainability efforts in their complex intertwined effects, we have provided three examples of the sustainability-cybersecurity nexus as it plays out in our localized field sites. We have proposed these descriptions as an opening for a future debate about the tensions between sustainability and cybersecurity as well as a shift towards socio-material practice as a handle for SHCI. It takes an inward gaze at HCI to notice and trace how sustainability stands in conflict with other prevalent goals of HCI, such as cybersecurity. We have proposed that thinking of such tensions as practical problems purports a different narrative of sustainability: one that is more ambiguous, oscillating, and non-linear. We find this is emblematic of contemporary technological practices that are characterized by making local situations slightly better or worse instead of pursuing conclusive solutions.

ACKNOWLEDGMENTS

This work was funded by “Algorithms Data and Democracy”, a project of the VELUX Foundation, and the CRC “SFB1567 Virtual Life Worlds” funded by the German Research Foundation (DFG). We are indebted to our interlocutors who have so willingly shared their stories. We further acknowledge that conducting ethnographic studies and writing research manuscripts requires earthly resources.

REFERENCES

[1] Benedetta Piantella, Alex Nathanson, Tega Brain, and Keita Ohshiro. 2020. Solar-Powered Server: Designing for a More Energy Positive Internet. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20). Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3334480.3383155

[2] Max Willis, Julian Hanna, Enrique Encinas, and James Auger. 2020. Low Power Web: Legacy Design and the Path to Sustainable Net Futures. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20). Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3334480.3381829 Chelsea Finn. 2018. Learning to Learn with Gradients. PhD Thesis, EECS Department, University of Berkeley.

[3] Christina Bremer, Bran Knowles, and Adrian Friday. 2022. Have We Taken On Too Much?: A Critical Review of the Sustainable HCI Landscape. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22). Association for Computing Machinery, New York, NY, USA, Article 41, 1–11. https://doi.org/10.1145/3491102.3517609

[4] Janghee Cho, Laura Devendorf, and Stephen Voida. 2021. From The Art of Reflection to The Art of Noticing: A Shifting View of Self-Tracking Technologies’ Role in Supporting Sustainable Food Practices. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21). Association for Computing Machinery, New York, NY, USA, Article 298, 1–7. https://doi.org/10.1145/3411763.3451838

[5] Somya Joshi and Teresa Cerratto Pargman. 2015. In search of fairness: critical design alternatives for sustainability. In Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives (CA '15). Aarhus University Press, Aarhus N, 37–40. https://doi.org/10.7146/aahcc.v1i1.21301

[6] Puig de la Bellacasa, Maria. 2017. Matters of Care: Speculative Ethics in More than Human Worlds. University of Minnesota Press. http://www.jstor.org/stable/10.5749/j.ctt1mmfspt

[7] Jackson, Steven.J., 2014. Rethinking Repair. Media technologies: Essays on communication, materiality, and society, pp. 221-39.

[8] Denis, Jérôme, and David Pontille. 2011. Materiality, Maintenance and Fragility: The Care of Things. Available at SSRN 1947255 https://ssrn.com/abstract=1947255 or http://dx.doi.org/10.2139/ssrn.1947255

[9] Tsing, Anna Lowenhaupt., 2015. The Mushroom at the End of the World. In The Mushroom at the End of the World. Princeton University Press.

[10] Sørensen, Estrid and Laura Kocksch. 2021. Data Durabilities: Towards Conceptualizations of Scientific Long-Term Data Storage. Engaging Science, Technology, and Society, 7(1), pp.12-21.