Towards Safe and Just Work Environments for System Administrators

A Qualitative Sociotechnical Investigation into System Administration

Kaur, M.

DOI
10.4233/uuid:cb598569-af98-4cef-8115-9939fa5ed256

Publication date
2023

Document Version
Final published version

Citation (APA)
Kaur, M. (2023). *Towards Safe and Just Work Environments for System Administrators: A Qualitative Sociotechnical Investigation into System Administration*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:cb598569-af98-4cef-8115-9939fa5ed256

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

TOWARDS SAFE AND JUST WORK ENVIRONMENTS FOR SYSTEM ADMINISTRATORS

A Qualitative Sociotechnical Investigation into System Administration

MANNAT KAUR

Towards Safe and Just Work Environments for System Administrators

A qualitative sociotechnical investigation into system administration

Towards Safe and Just Work Environments for System Administrators

A QUALITATIVE SOCIOTECHNICAL INVESTIGATION INTO SYSTEM ADMINISTRATION

Dissertation

for the purpose of obtaining the degree of doctor
at Delft University of Technology,
by the authority of the Rector Magnificus, Prof.dr.ir. T.H.J.J. van der Hagen,
chair of the Board for Doctorates,
to be defended publicly on Tuesday 5th of December 2023 at 15:00 o'clock

by

Mannat KAUR

Master of Science in Aerospace Engineering,
Delft University of Technology, the Netherlands
born in Meerut, India.

This dissertation has been approved by the promotors.

Composition of the doctoral committee:

Rector Magnificus,	Chairperson
Prof.dr.ir. M.F.W.H.A. Janssen	TU Delft, promotor
Dr.-Ing. T. Fiebig	TU Delft & MPI-INF, Germany copromotor
Independent members:	
Prof.dr.ir. P.H.A.J.M. van Gelder	TU Delft
Prof.dr. M.E. Warnier	TU Delft
Prof.dr.ir. C.T.A.M. de Laat	Emeritus, Universiteit van Amsterdam
Prof. S. Zanero	Politecnico di Milano, Italy
Asst. Prof. Dipl.-Ing. Dr.techn. M. Lindorfer	TU Wien, Austria

Keywords: system administration, sysadmin, human factors, safety science, computer security, feminist research, just culture, sociotechnical system

Printed by: Proefschriftspecialist, Zaandam

Front & Back: M. KAUR

ISBN 978-94-6366-763-0

An electronic version of this dissertation is available at
http://repository.tudelft.nl/.

"Technologies only come to life and have meaning as people adopt and use them."

Judy Wajcman

Contents

Summary

Technological infrastructures and systems form the bedrock of modern society. Governments, organizations, communities and individuals are increasingly reliant on the proper functioning of IT systems to perform necessary tasks. This is even more relevant during times of crises, such as the COVID-19 global pandemic. But who is ensuring the proper functioning of system and network infrastructures? It is **system administrators (sysadmins)** or system operators who configure, maintain and operate these infrastructures and they do so, more often than not, behind the scenes.

The work of system administration tends to be unseen and, consequently, not well known. After all, do you think of your IT help-desk when everything is working fine? Usually, people reach out for help when something is not working as expected or when they need something. However, a lot of work and effort goes into ensuring that systems are working as expected most of the time and, paradoxically, this smooth functioning results in the invisibilization of the work and effort that went into it. On top of that, system administrators are often blamed for security misconfigurations that sometimes lead to large-scale computer security incidents (such as data breaches). This not only points to the crucial nature of sysadmin work but also the fact that sysadmins are given attention only when something isn't as required.

We employ a different perspective for this PhD research. Most existing research focuses on technical support for sysadmins, including automation in order to reduce the human factor as much as possible, and some on other social factors such as organizational changes. In this PhD research, we take a step back to better understand system administration work and what it entails with the aim of finding ways to enable sysadmins to do their work. Instead of proposing technical and social solutions for sysadmins, we try to better understand the "problem" that these proposed solutions are meant to solve. Instead of adding to the list of "solutions", we center the experiences of sysadmins and deep dive into what their day-to-day work is like.

Reviewing and systematising human factors research from 2008 to 2018 in the computer security domain (Chapter 3) reveals that system administrators are an understudied group of expert users. In addition, we find other scientific knowledge gaps such as lack of strong theoretical foundation and the centering of a U.S. and European perspective. We begin to address these scientific gaps by conducting empirical qualitative studies that focus on the work experiences of system administrators and have strong theoretical and methodological foundations. Specifically, the interview study relies on coordination theory from its inception and the focus group study is guided by a feminist research approach while being heavily rooted in previous related work.

Through the interview study (Chapter 4) we elaborately define what constitutes system administration work in terms of supporting others and the underlying coordination processes. Performed during COVID-19 global pandemic, this study has an additional focus on how sysadmins managed their work during the COVID-19 lockdown by performing extra tasks and dealing with the increased formalization of their work. We identify and explain coordination mechanisms used by sysadmins and propose that these can be used to better support sysadmin work and to be better prepared for crisis/unexpected events, such as COVID-19, in the future.

The focus group study (Chapter 5) is about the gendered experiences of sysadmins within the men-dominated field of system administration. This study highlights the extra care work done, gender considerations made and coping mechanisms used by sysadmins who belong to marginalized genders. We center the experiences of sysadmins who are not cis men in order to mitigate the limitations that we experienced during the literature review and the interview study (such as the lack of gender diversity in the participant sample). We show that equitable workplaces are an important step towards improving organizational computer security.

The two empirical studies, together, provide a deep look into the social aspects of sysadmins' work. We identify and explain the important factors that influence the work of system administrators and provide recommendations (Chapter 6) to help build safe and just work environments for system administrators where they are enabled to do their work. For future work we recommend to dive deeper into the social aspects of sysadmin work and do so using feminist lens. We recommend to do human factors research that has strong theoretical foundations, for example, in coordination theory and techno-feminist theory.

Samenvatting

Technologische infrastructuren en systemen vormen de basis van de moderne samenleving. Overheden, organisaties, gemeenschappen en individuen vertrouwen steeds meer op de goede werking van IT-systemen om de noodzakelijke taken uit te voeren. Dit is zelfs nog relevanter in tijden van crisis, zoals de wereldwijde pandemie van COVID-19. Maar wie zorgt voor het goed functioneren van systeem- en netwerkinfrastructuren? Het zijn **systeembeheerders (sysadmins)** die deze infrastructuren configureren, onderhouden en bedienen en dat doen ze vaker wel dan niet achter de schermen.

Het werk van systeembeheer is vaak onzichtbaar en daarom niet goed bekend. Denkt u immers aan uw IT-helpdesk als alles goed werkt? Meestal zoeken mensen hulp als iets niet werkt zoals verwacht of als ze iets nodig hebben. Er wordt echter veel werk en moeite gestoken om ervoor te zorgen dat systemen werken zoals verwacht, en paradoxaal genoeg resulteert deze soepele werking in de onzichtbaarheid van het werk en de moeite die erin is gestoken. Bovendien krijgen systeembeheerders vaak de schuld van verkeerde configuraties van de beveiliging die soms leiden tot grootschalige computerbeveiligingsincidenten (zoals datalekken). Dit wijst niet alleen op de cruciale aard van het werk van systeembeheerders, maar ook op het feit dat systeembeheerders alleen (negatieve) aandacht krijgen als er iets niet naar wens is.

Voor dit promotieonderzoek hanteren we een andere invalshoek. Het meeste bestaande onderzoek richt zich op technische ondersteuning voor systeembeheerders, inclusief automatisering om de menselijke factor zoveel mogelijk te verminderen, en sommige op andere sociale factoren zoals organisatorische veranderingen. In dit promotieonderzoek doen we een stap terug om systeembeheerwerk en wat het inhoudt beter te begrijpen, met als doel manieren te vinden om systeembeheerders in staat te stellen hun werk te doen. In plaats van technische en sociale oplossingen voor systeembeheerders voor te stellen, proberen we het "probleem" dat deze voorgestelde oplossingen moeten oplossen beter te begrijpen. In plaats van toe te voegen aan de lijst met "oplossingen", we centreren de ervaringen van systeembeheerders en duiken diep in hoe hun dagelijkse werk eruit ziet.

Het beoordelen en systematiseren van literatuur naar menselijke factoren van 2008 tot 2018 op het gebied van computerbeveiliging (Chapter 3) onthult dat systeembeheerders een onderbestudeerde groep deskundige gebruikers zijn. Daarnaast vinden we andere hiaten in de wetenschappelijke kennis, zoals een gebrek aan sterke theoretische onderbouwing en het centreren van een Amerikaans en Europees perspectief. We beginnen deze wetenschappelijke hiaten aan te pakken door empirische kwalitatieve studies uit te voeren die zich richten op de werkervaringen van sys-

teembeheerders en die een sterke theoretische en methodologische basis hebben. Met name de interviewstudie steunde vanaf het begin op de coördinatietheorie en de focusgroepstudie werd geleid door een feministische onderzoeksbenadering terwijl ze sterk geworteld was in eerder gerelateerd werk.

Door middel van de interviewstudie (Chapter 4) definiëren we uitvoerig wat systeembeheer inhoudt in termen van het ondersteunen van anderen en hun coördinatieprocessen. Deze studie, uitgevoerd tijdens de wereldwijde pandemie van COVID-19, heeft een extra focus op hoe systeembeheerders hun werk hebben uitgevoerd tijdens de COVID-19-lockdown door extra taken uit te voeren en om te gaan met de toegenomen formalisering van hun werk. We identificeren en leggen coördinatiemechanismen uit die worden gebruikt door systeembeheerders en stellen voor dat deze kunnen worden gebruikt om het werk van systeembeheerders beter te ondersteunen en om beter voorbereid te zijn op crisis/onverwachte gebeurtenissen, zoals COVID-19, in de toekomst.

De focusgroepstudie (Chapter 5) gaat over de gendergerelateerde ervaringen van systeembeheerders binnen het door mannen gedomineerde gebied van systeembeheer. Deze studie belicht het extra zorgwerk dat is gedaan, de gemaakte genderoverwegingen en de coping-mechanismen die worden gebruikt door systeembeheerders die tot gemarginaliseerde geslachten behoren. We centreren de ervaringen van systeembeheerders die geen cis-man zijn om de beperkingen die we in eerder werk ondervonden te verminderen (zoals het gebrek aan geografische en genderdiversiteit in de deelnemerssteekproef). We laten zien dat rechtvaardige werkplekken een belangrijke stap zijn om de computerbeveiliging binnen organisaties te verbeteren.

De twee empirische studies samen geven een diepgaand inzicht in de sociale aspecten van het werk van systeembeheerders. We identificeren en verklaren de belangrijke factoren die het werk van systeembeheerders beïnvloeden en doen aanbevelingen (Chapter 6) om te helpen bij het bouwen van veilige en rechtvaardige werkomgevingen voor systeembeheerders waar ze in staat worden gesteld hun werk te doen. Voor toekomstig onderzoek raden we aan om dieper in de sociale aspecten van systeembeheerderswerk te duiken en dit met een feministische lens te doen. We raden aan om onderzoek naar menselijke factoren te doen dat een sterke theoretische basis heeft, bijvoorbeeld in coördinatietheorie en techno-feministische theorie.

1

Introduction

"It might seem that security should gradually improve over time as security problems are discovered and corrected, but unfortunately this does not seem to be the case. System software is growing ever more complicated, hackers are becoming better and better organized, and computers are connecting more and more intimately on the Internet. Security is an ongoing battle that can never really be won."

Evi Nemeth, Unix and Linux System Administration Handbook (2010)

1

There is an increasing dependence of everyday life on the flawless functioning of IT infrastructure and systems. Organizations are reliant on IT systems as they are vital to daily functioning. For example, in the healthcare industry, healthcare workers are reliant on the IT infrastructure to have instant access to patients' medical records, to perform computer-assisted surgeries and even to provide remote care (for example, during the COVID-19 pandemic). The crucial task of operating these IT systems is known as system administration. People who design, run and maintain these human-computer communities are known as system administrators (sysadmins) or system operators [36]. They deploy and update software created by developers, configure network equipment, and provide services to users. In universities for example, the role of sysadmins would include ensuring that the university staff is able to deliver education to the students, the students are able to access this information as intended, students and staff are able to communicate as needed, educational tools and resources (such as recording of lectures, submission of assignments or software tools etc.) are available and users are able to ask for assistance when needed. Most organizations and industries, such as telecommunication and aviation, are similarly dependent on IT systems and therefore on sysadmins.

In order to ensure that successful operations continue day-after-day, system administrators' work involves a multitude of tasks. These tasks are both technical and social in nature. Technical tasks include installation and maintenance of (operations-critical) infrastructure and its compliance to required security standards. Social tasks include supporting the system users, and coordinating with team members and management staff. Previous related work around system administration has mostly focused on the technical tasks of sysadmins and the tools needed. For example the work of Haber et al. [108] who developed design guidelines for the tools of sysadmins. In recent years, more human-focused studies have emerged, such as the work of Dietrich et al. [70], which also take the social factors into account. Overall, there is a lack of understanding of these social aspects and, in turn, of the human factors that play a role in the work of system administrators.

Human factors applies to the understanding of interactions between a human and a (technological) system. The study of human factors is interdisciplinary and it brings together knowledge from the fields of social science, psychology, safety science etc. The modern understanding of human factors (see Section 1.2.1 and Figure 1.1) has overtime shifted away from individual responsibility towards organizational factors and societal perspectives. The focus currently is no longer on solely controlling the human factor (e.g. by preventing human errors), but instead, on how to facilitate proper resilient system operations. In the context of system administration work, it is about comprehending the technical work situated within specific social contexts, acknowledging that the social processes have a significant influence on this work and then accounting for the way in which the work is affected by the social factors. For instance, examining how the work of sysadmins is impacted by the organizational culture they're embedded within and how the societal norms influence this. We develop this knowledge by centering the experiences and expertise of system administrators, and in turn enable system administrators to perform their work in the way they feel is best.

We begin by introducing the background concepts which provide an essential starting point. Sections 1.1 introduces system administration and what this work entails in terms of coordination, gender and care. Section 1.2 defines human factors from different perspectives, what we can learn from other fields when studying human factors and why it is important to study human factors. Section 1.3 presents the research gap that we want to address and Section 1.4 presents the research objective along with the research questions. Finally, we describe the scientific and societal relevance (Sections 1.5 and 1.6) and present the thesis outline (Section 1.7).

1.1. What is System Administration?

In today's world, IT systems have become an integral part of how we work and live. Naturally, these IT systems have to be built and maintained, and this work is attributed to *system administrators*, or *'sysadmins'*[1]. These knowledge workers, for example, install and configure new hard- and software, update systems, create user accounts, and ensure that systems are backed up (and other security-related responsibilities). Formally, the U.S. National Institute of Standards and Technology (NIST) defines sysadmins as *"individuals responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures"* [50]. Less formally, Limoncelli et al. define a sysadmin as *"one who manages computer and network systems on behalf of another, such as an employer or a client."* [169, p. xli]. These definitions point not only to technical IT duties, but also to a requirement for sysadmins to coordinate in some way with those using the systems they prepare and provision, and whose work they enable.

DevOps

Since the early 2000s the concept of 'DevOps' has grown out of the concept of 'Site Reliability Engineers', first prominent at Google [22]. DevOps, a word-merger between development and operations, is often (mis)understood as something *different* than classical system administration [169]. However, instead of a fundamental change in the defining objective—providing a service—DevOps is a *cultural* change in the way system administration is done [54, 170]. Contrary to 'traditional' forms of system administration work, the DevOps concept aims to: include practices from software development (automation and repeatability, Infrastructure-as-Code (IaC), version control, test and production environments) [54, 169, 170]; formalize already existing practices (making outcomes and changes' impact measurable) [169], and; incorporate lessons learned from safety science on preventing errors (blameless post-mortems, for example) [54, 70, 170].

Given that DevOps is a cultural change instead of a change in the objective, it is also a *spectrum*. An organization does not start to do 'DevOps' by simply changing the name of the operations team—something often seen in practice [169]—but has to gradually change the culture of its operations. Hence, parts of how DevOps

[1] For brevity, from here on, we refer to System Administrators as 'sysadmins'.

becomes DevOps may be found in a company—such as repeatability in infrastructure deployments, version control—though other aspects might still be lacking, as for example, a restorative culture. In sum, we consider professionals working as DevOps to be within scope as sysadmins for the purpose of this research.

1.1.1. Coordination in System Administration Work

Several prior studies have highlighted the collaborative nature of system administration work [18, 109, 253, 282, 293]. Sysadmins have to constantly communicate with other sysadmins to coordinate tasks, i.e., *"work that needs to be done"* [282, p. 6]. Coordination—according to Malone and Crowston—is *"the act of managing interdependencies between activities performed to achieve a goal"* [177, p. 361]. Naturally, coordination also requires multiple actors to be involved for coordination to occur *between* them [177], where sysadmins coordinate their activities as a team [69]. Tasks can be discrete activities or consist of interdependent sub-tasks [223], toward a goal. Tasks are individual and executed by a single actor. A collaborative activity consists of several tasks, executed by multiple actors, to realize a common goal. To use a simple example, cooking dinner *together* with friends is a collaborative activity; chopping onions is a task.

Sysadmins also have to communicate and coordinate with *users* of the systems they manage. It is the task of sysadmins to coordinate their activities with users, so that users' work is not impacted by necessary changes to the IT system [169]. A common catalyst for this coordination is, for example, the rollout of software updates, which can necessitate computer restarts, which must not impact productive work [271].

There is both *implicit* and *explicit* coordination, with explicit coordination being the most commonly recognized form of coordination [78]. This manifests when actors in a team explicitly exchange information about their tasks in order to coordinate them [78]. This can happen via support tools (timetables, plans, written procedures), and by direct communication. Explicit communication can then be formal, as in (regularly) scheduled meetings, or informal, as in the case of 'water cooler chatting' or 'coffee talk' [78].

Implicit coordination occurs when teams exhibit coordinated behavior without any explicit exchange of information [78]. While difficult to formally describe, implicit coordination is best captured as instances of when 'everyone knew what they had to do.' Examples of implicit coordination are when a team appears to share a mental model, e.g., of how a process works [167], or similarly exhibit seemingly the same awareness of a situation [238]. Implicit coordination enables team members to assume future 'task states' and what the actions of others in the team will be, such that others can by that same mechanism anticipate their actions as well [78]. Naturally, implicit and explicit coordination can occur together. A team might explicitly coordinate a project through planned meetings, and coordinate implicitly as they then execute those plans, based on a shared situation awareness about the progress of the project.

1.1.2. Gender Roles in the Origins of System Administration Work

The technology workspace has been men-dominated for the past several decades [255] and remains so [10] despite proposals for making technology-related professions more equitably accessible [233]. However, *traditionally*, the field of computing was very much *not* dominated by a purely WEIRD (Western, Educated, Industrialized, Rich, and Democratic) [122] straight man's perspective. The idolized example for this is, most likely, Ada Lovelace, one of the first to work on algorithmic thinking. While the field of computer science was more of a niche of mathematics back then, work by Lovelace was fundamental and influences computing even today [9]. The first explosion of digital computing and algorithmics-related research occurred during the second world war, specifically around the necessity of breaking German cryptographic implementations. Efforts were centralized in Bletchley Park, where the British Government brought together a diverse set of bright minds to work on computing and breaking German codes [250]. Besides researchers, the (first) computers they built had to be *operated*. This task fell to the Wrens, the women in the "Women's Royal Navy Service" [251]. Overall, Bletchley Park was famed *"as a 'unique' institution, a conclusion derived from the eccentricities of its most celebrated staff members, its perceived egalitarian and collegiate working environment"* [250, p. 2].

Yet, after the war, the U.K. saw women return to patriarchal gender roles, while others fell to persecution because of their 'divergence' from the 'accepted' standard. The Wolfenden Report serves as a landmark for this shift, codifying such overcome perspectives with heavy support from the church of England [103]. Similarly, Alan Turing was ultimately pushed to suicide by the government due to being queer—for which the British Government only pardoned him in 2017 [72]—and the number of Wrens was reduced to 3,000 [303] from over 75,000 at the end of the war [283].

At the same time, on the other side of the Atlantic, it was also the Navy having a leading role in the development of computing. The most well-known is Rear Admiral Grace Hopper, who started working on the 'Harvard Mark I' and later developed 'FLOW-MATIC', the direct ancestor of 'COBOL' [243]. Similarly, Hedy Lamarr developed a technique for 'Frequency-hopping spread spectrum' [138, 149] communication to evade frequency jamming, which became an integral part of modern wireless protocols like Bluetooth and WiFi [267]. With the space race receiving increasing importance, National Aeronautics and Space Administration (NASA) was founded. Of course—even though still a manual effort—computations were a vital part of this, which saw women being employed en mass for this task [187]. This part of history is also deeply connected with the history of racism and segregation concerning women of color working as computers at NASA [74].

What both sides of the Atlantic had in common is that the general theme of *operating* computers was that of a clerk position: Not a prestigious position, but instead one akin to a secretary or assistant. With the rising importance of computing and hence system administration, significant funding, e.g., from DARPA, went into computing research. Along this development, more men moved into the profession of building and operating systems, ultimately leading to a change in the perception of the job as well as a change in the perceived gender coding of these roles [210]. This

is a well documented impact of a patriarchal system, studied in literature [210], and also known to occur in the opposite direction, i.e., professions being remunerated less and losing social status despite the *work itself not changing* when more women join the profession [165].

Hence, in summary, system administration, or IT work in general, is not a traditionally cis-men dominated field. Instead, this area of work was taken over when opportunities arose, while pioneers were forgotten or pushed out.

1.1.3. Care in System Administration Work

Care work is often understood in the context of healthcare and other similar fields of work. While care can be given to people, it can also be given to things in the form of maintenance (and sometimes to change things for the better) [156]. Care work *"is always ongoing, it never finds closure and hence demands affective commitment and dedication"* [156, p. 2]. It is often *"hands-on, piecemeal, badly accounted for, and feminized"* [156, p. 1]. Care work relies on improvisation and adaptation. The care aspect of work is usually invisibilized and is not considered to be a task in and of itself. It cannot easily be formalized, so it is not accounted for at an organizational level [156]. For example, quoting an interview participant from the study presented in Chapter 4: *"if you are not very careful with your time, you can go a whole week without having anything to account for because you are spending your time trying to help other team members."* [147, p. 13]

Sysadmins' work includes maintenance tasks, supporting others when needed and a commitment to ensuring continuous system operations. On the one hand, supporting systems' users is often a central part of sysadmins' work. On the other hand, users are often seen as lacking in IT literacy and hence, a burden to sysadmins' work. The series 'Bastard Operator from Hell' (BOfH) by Simon Travaglia [274] is about a rogue system administrator who takes out his anger and frustrations on the system end-users (lusers, a merger of loser and user) who constantly pester him for help. This series is popular in the sysadmin community, and the rogue 'BOfH' is often seen as a hero [54, 180]. While this series can be seen as a way to vent out the frustrations of a demanding profession, there can be negative consequences for the organization and for those who are embedded within this culture when similar attitudes are emulated in the real world [54, 180].

In summary, sysadmins' work includes care work by its very nature in terms of both caring for things and people. Care of things might not traditionally be seen as care work and hence rarely accounted for formally. Care of people is often seen as a burden, making it harder to do the "actual work".

1.2. What are Human Factors?

It is important to study human factors to better account for the role of people in sociotechnical systems and their role in ensuring system security. Research on human factors in the safety science domain has already spanned over a century whereas human factors studies in the computer security domain have been around for a couple of decades. This bears the question: What can we learn from safety

science? In this section, we first present the safety science perspective accompanied with a visual aid (Figure 1.1). We then present the computer security perspective on human factors. Finally, we discuss what we can learn from other domains and also insights that cannot be directly applied.

1.2.1. Safety Science Perspective

Initially, the term *human factors* described the application of scientific knowledge, concepts, models, and theories derived from social science disciplines, such as psychology, towards improving operational efficiency and reducing the human errors that led to accidents [6, 62]. Early literature on human factors and human error has since gone through five major stages of development in the past century (Figure 1.1).

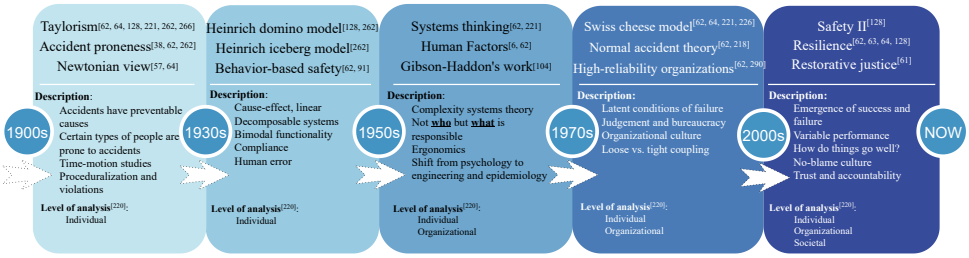


Figure 1.1: Overview of the development of human factors research in safety science [62]. Note how over time, the perspective shifted away from individual responsibility to, first, organizational factors, and finally to a societal perspective. Ultimately, the focus is no longer solely on how to prevent human error, but also on how to facilitate proper resilient operations.

For the first half of the 20$^{\text{th}}$ century, the core ideas were that certain people are prone to accidents and accidents are preventable by taking away the causes, for example, enforcing compliance with rules. These ideas developed further and gave rise to the concepts of decomposable systems (a linear model where cause and effect is visible and wherein the system can be decomposed meaningfully into its parts and rearranged again into a whole) and bi-modal functionality (the components of the system can be in one of two modes of operation - either functioning correctly or not). These two concepts led to the assumption that every failure has a root-cause and if we can find this root-cause, we can fix it and ensure safety. In this case, the analysis is centered around the individual responsible for "human error" or failure.

During the second half of the century, the systems perspective emerged, as did the label of "human-factors" research. This changed the narrative from *who* is responsible to *what* is responsible, shifting the focus on the latent conditions behind failure. The analysis now included both individual and organizational aspects.

Since the 2000s, the safety science domain has witnessed another shift in paradigm. The new perspective on safety is known as Safety-II. The Safety-II approach takes into account that what is responsible for success. Instead of creating the best way for people to comply, researchers take a step back to understand people and their variable performance in safety or security-critical operational environments. The Safety-II approach does not replace the traditional approach to safety that has de-

veloped over the decades. It is a complementary approach with a focus on proactive safety management. In addition, we also see a shift in the way in which we deal with human error. Restorative justice is an approach that focuses on repairing the harm through accountability and learning instead of responsibility and blame. Also included now are the societal parameters in the analysis of human factors.

A key take-away from the contemporary perspective is that trying to *eliminate* the human factor to build safe and secure systems is not the only way to improve safety. It is also important to understand *why systems do not fail*, in daily operations as well as in the presence of human error, and understand how the human factor contributes to *success*.

1.2.2. Computer Security Perspective

Computer security work often addresses intentional harm that manifests in the form of malware, data breaches etc. However, computer security has grown to include protection from other non-intentional types of harm such as vulnerable code or faulty system operations. In much of scientific literature, people are considered the weakest-link in computer security and many large-scale incidents/breaches are often blamed on (unintentional) human error. Currently, the most common solutions to this human problem are to eliminate the human-in-the-loop, training and education, compliance via policies and root-cause analysis (reactive security) [311]. When mistakes occur, the route to security is to eliminate these mistakes by adding automation, protocols or standards [70].

In the computer security domain, human factors research is relatively new. Traditionally, computer security concerned itself with understanding the technical properties of systems and networks in order to guarantee confidentiality, integrity, and availability. With the rapid societal adoption of computer systems over the past decades, researchers identified new security and privacy issues, stemming from the interaction between users and systems. This gave rise to the study of human factors in the computer security domain. In this context, most research emerged as part of either (a) designing secure and usable systems or (b) empirical studies of problems around how users interact with systems and services.

The first approach is design-oriented. Data on users is collected as part of a design process or an evaluation of an existing system. Think of eliciting user requirements or validating the performance of the designed system with actual users. Organized around the concepts of usability and human-computer-interaction, researchers have worked on creating secure *and* usable systems. A classic example is Whitten and Tygar's usability analysis of GPG's user interface [298].

The second approach to human factor research is descriptive, i.e., focuses on soliciting empirical data on users' *behavior*. Users are studied in various security-relevant contexts, to learn more about their behavior in general, not directly tied to the design process of a specific system or service. This work typically relies on experiments, surveys, and observational data. For example, Krombholz et al. conducted experiments to see if system operators are able to properly deploy HTTPS [160] and Golla et al. collected behavioral data around password reuse notifications from a production system [98].

1.2.3. What lessons can computer security learn from safety science?

Despite all our efforts, serious security breaches and hacks continue to happen. Some contemporary research has emphasized the need to rethink the status quo, challenge the core assumptions underlying our current approach and learn from other fields [123]. As discussed earlier, the traditional safety science approach sees people as the problem and assumes that systems are decomposable and bimodal. Human factors research in the computer security domain is interdisciplinary. We are studying sociotechnical systems that are complex, unpredictable and emergent. Due to this, the traditional assumptions (human-as-problem, bimodal functionality or system decomposability) do not work well.

Zimmerman and Renaud propose the *cybersecurity, differently* approach [311]. Drawing learnings from other fields such as military, management and safety, they present some key principles of this new approach. These are system emergence (vs. system decomposability), human-as-solution (vs. the more common view: human-as-problem), deference to expertise (vs. policy compliance), encourage learning and communication (vs. constrain and control), focus on success (instead of solely preventing errors) and finally, balancing resistance and resilience [311].

As explained before, the Safety-II approach does not replace the traditional approaches to safety but is complementary. Similarly, the *cybersecurity, differently* approach is not about radically changing the way in which we manage computer security. It is about recognizing the sociotechnical aspects of computer security when addressing the human factors. We must broaden our perspective on the management of human factors and explore modern principles along with traditional ones.

Finally, are there some learnings that cannot transcend from another domain to the computer security domain? The human problem in the safety domain focuses on unintentional mistakes by well-intended humans. The case of intentional harm and sabotage is not addressed in this approach and is seen as a separate security concern. However, the computer security domain deals with both malicious actors and non-malicious human error. Therefore, we need to remember this knowledge transfer does not address dealing with malicious actors.

1.3. Research Gap

System operators and administrators are an understudied population of users in the computer security domain (discussed further in Chapter 3). Much of the existing research investigates the average (non-expert) end user. This is concerning because even though expert users (such as sysadmins) are relatively a smaller group, their behaviour and work practices have a much larger impact on overall system security as compared to the average end-user.

There exists a scientific knowledge gap in the understanding of human factors in system administration work. This knowledge gap pertains to the extent of social and technical work that is being done to perform successful system operations, and the social factors that affect this work. Furthermore, there is space for research that

employs the human-as-solution approach by centering the experiences of expert users such as sysadmins and enabling them to do what they do in a way that they see fit.

1.4. Research Objective

The purpose of this PhD research is to determine the important human factors and processes underlying system administration work, to better understand how these factors operate and find ways to be able to support them. The factors which are considered as 'important' are those which influence the work of sysadmins on a regular day-to-day basis and can require sysadmins to take them into consideration when performing their work. We generate descriptive knowledge about system administration work via archival research, one-on-one interviews and focus groups. The main research question is:

What are the human factors that affect system administration work and in what ways can we enable this work?

To answer this, the following sub research questions were addressed:

1. What is the state of knowledge of human factors research in the computer security domain? (Chapter 3)

   The first step is to understand the state of the art of human factors (user-related) research in the field of computer security. To do this, we analyse the studies published in top security-conference venues over the past decade. We distinguish between non-expert users and expert (e.g. sysadmins) users. The findings show that while human factors research in generally on the rise, expert-user related studies are infrequent. Expert users such as sysadmins remain an understudied population despite their crucial role with regard to system security.

2. What does the day-to-day work of system administrators look like and how did this work change due to the COVID-19 lockdowns? (Chapter 4)

   To fill this research gap, we perform empirical research to better understand sysadmins' work from the perspective of those doing it. As the COVID-19 pandemic was ongoing during this study, we utilize the unique opportunity to investigate the impact of the global pandemic and remote working on the work of sysadmins. Via one-on-one online interviews, we talk to sysadmins about their day-to-day work and how it is impacted by the COVID-19 imposed lockdowns. In addition to the effects of the pandemic on work coordination and formalization, we identify *care* aspects as part of sysadmins' work.

3. In what ways do sysadmins manage to work in the cis-men-dominated field of system administration? (Chapter 5)

   Care work is often feminized and system administration is currently a men-dominated field. The literature review showed that previous research around system administration work rarely accounts for gender of the participants and

what role it might play in their work. While we did not consider gender as a factor in the previous study (Chapter 4), we faced difficulties in finding a diverse group of participants to talk to. Hence, we wanted to study the role of personal and individual factors (e.g. gender) in sysadmins' work. We take a feminist approach for this study to highlight the invisibilized aspects of sysadmins' work such as the extra care work performed by sysadmins who are not cis men and extra work done due to gender considerations.

4. In what ways can we enable system administrators' work to be more safe and equitable? (Chapter 6)

   We synthesize our findings and insights gained from the empirical work done to answer the previous sub research questions in order to develop recommendations for enabling sysadmins' work. We draw on lessons both from the safety science domain and from the feminist research approach. In general, when sysamdins' work is better supported by organizations, it will also contribute to improving computer security by fostering a safe and equitable environment that ultimately contributes to positive operational outcomes.

1.5. Scientific Relevance

The scientific relevance lies in the novel empirical work that we carried out by a) interviewing sysadmins about their work during a global pandemic and b) talking to sysadmins who are not cis men to investigate sysadmins' work through a feminist lens. We formulated empirical studies in response to scientific knowledge gaps that we identified during the literature review of computer security research and also based on our insights during each study. We draw on concepts from the field of safety science and feminist research methods, and apply it to the computer security domain. This work is interdisciplinary as knowledge and research methods from different disciplines are integrated and applied to answer the research questions.

1.6. Societal Relevance

With a deeper qualitative understanding of system administration work, we can develop recommendations for enabling this work. This is important, first and foremost, for creating safe and equitable work spaces for *all* system administrators. Furthermore, system administration work is crucial to the functioning of our societies with all the technological infrastructure that supports it. Due to its fundamental nature system administration work can often have a widespread effect across organizations and users, potentially affecting system security and thus, organizational and individual security, privacy and safety. The operations-critical nature of system administration work can become even more vital during times of crises (such as the COVID-19 global pandemic) when certain infrastructures (such as those supporting connectivity or knowledge-dissemination) become absolutely necessary. Recommendations for enabling and supporting system administration work are therefore relevant for society as a whole.

1.7. Thesis Outline

This thesis is structured as follows: Chapter 1 has introduced the background concepts, and the research objective. Chapter 2 lays out the research design for the entire project. Chapter 3 investigates the state of knowledge (SoK) of human factors research in the computer security domain and highlights knowledge gaps. These knowledge gaps informed our subsequent projects. Chapter 4 describes the day-to-day work of system administrators. This chapter also includes the effect of the pandemic and shift to remote work on the work of system administrators. In addition, this project reveals aspects of (often feminized) care work in system administration. Combining this with the fact that system administration is a men-dominated field and most existing scientific literature does not take gender into account, we identified the need to study personal factors, specifically gender, and investigate system administration work from a feminist perspective. Therefore, Chapter 5 describes the role of gender in the work of system administration. This project sheds light on the gendered experiences of system administrators in terms of the care work being done, and also identifies ways in which sysadmins manage their work in men-dominated inequitable work environments. Finally, we reflect on the work done and present practical recommendations for enabling this work in Chapter 6 along with the limitations and future research outlook. We conclude by recapping our research questions and how they were addressed in Chapter 7.

2

Research Design

2

This PhD research project is exploratory in nature where the main aim is to develop a deeper understanding of system administration work. In Section 1.3, the identified scientific research gap is presented and in Section 1.4, the research objectives (including the research questions) are developed accordingly. In order to answer these research questions, in this chapter, we present our research design for the development of knowledge of the human factors in system administration work.

We start with our research philosophy in Section 2.1 where we briefly discuss our ontological, epistemological, axiological and methodological beliefs. The following Section 2.2 presents our synthesis on the research philosophy. Based on these, we chose qualitative research approaches, introduced in Section 2.3, to address the research questions. Reflecting on these beliefs puts us in a better position to conduct empirical research, which includes not only collecting and analysing data but also understanding the role of the researcher in relation to the data (Section 2.4) and what we hope to achieve with the knowledge gained from our research project. Our research strategy is depicted in a research flow diagram in Section 2.5.

2.1. Research Philosophy

Reflecting on the research paradigm is important so as to understand one's position as a researcher and to make explicit the implicit assumptions that one is working with when performing scientific research. Here we briefly discuss our ontological (nature of reality), epistemological (nature of knowledge), axiological (value and use of the research) and methodological (appropriate research methods) beliefs.

Ontology refers to the nature of reality and what can be known about it [105]. There are four main ontological beliefs: (a) positivism, which maintains that objective reality exists and can be known through the use of appropriate scientific methods [112] (b) postpositivism, which maintains that an objective reality exists (similar to positivism) but recognizes that it cannot be known perfectly as it is influenced by the human interpreter; (c) critical theory, which focuses on social critique of the status quo and ingrained structural issues which influence our social reality [214] and (d) constructivism, which maintains that reality cannot be objectively known and it is the people (including researchers) who create their realities [276]. Our ontological belief is constructivism as we aim to understand how people interact in their social context and make sense of their own reality. We assume that an objective reality does not exist and strive to account for our role as researchers when trying to interpret social phenomenon.

Epistemology refers to the nature of knowledge in terms of the relationship between what can be known and the knower [105]. Both positivism and postpositivism strive to capture an "objective reality", however, postpositivism (in contrast to positivism) acknowledges that objectivity remains an unattainable ideal [105]. Critical theory belief is about instigating social change by interacting with the people in the study [214]. Constructivism here is about interpreting social reality and the processes with which people create meanings and act [276]. Hence, interpretivism is our epistemological belief as we see our roles as researchers to interpret the interactions between people, technology and organizations, and then describe/document these interpretations.

Axiological belief is about the intentions of the researchers and what they intend to achieve with their work [214]. Positivist and postpositivist researchers both strive for a value free role in their search for an objective reality. A critical theory researcher aims to effect social change through social critique. Constructivism is about creating an understanding and a constructivist researcher interprets the process with which people create meaning. Here we can understand constructivism as weak and strong [214]. Weak constructivism is when the researcher interprets the social reality by using empirical data and strong constructivism is when the research is living and immersed in this social reality. We take the weak constructivist perspective as we want to understand the interactions between different aspects of a sociotechnical system and the strong constructivist approach of immersion might draw our analysis away from the sociotechnical aspects towards individual aspects.

Methodological belief and assumptions consider the appropriateness of research methods in gathering relevant empirical data [214]. Positivist researchers aim to test and verify hypotheses, and generalize their research findings. They rely largely on quantitative research methods and data. Postpositivist researchers instead aim to falsify the hypothesis and use both quantitative and qualitative research methods to do so [105]. Researchers who take the critical theory approach want to understand social constructions and the underlying factors by interacting with people situated in certain social contexts in order to bring about change. Hence, they employ interviews, participatory observations and similar qualitative methods for their work [105]. Constructivist research also engages with the people involved in specific contexts to understand their perspective in order to interpret dynamic social processes. This is done via archival research, interviews, observations and similar qualitative methods which also allow for a comprehensive analysis as is needed for interpretation [153]. Our methodological belief is rooted in constructivism as we believe that qualitative research methods are best suited for researching social processes and interactions.

2.2. Synthesis on Research Philosophy

Our research philosophy is rooted in constructivism and interpretivism as we believe that objective reality does not exist. Reality and what can be known about it is meaning that people create based on their lived experiences in a constructed social reality. This also includes reflecting on and accounting for our role as researchers when comprehending this social reality (Section 2.4). Our intentions as researchers situates us in a weak contructivist paradigm where we attempt to interpret reality via empirical data as opposed to immersion within the social reality itself. Based on these beliefs, we choose qualitative methods for data collection, namely archival research (Section 2.3.1), one-on-one interviews (Section 2.3.2) and focus groups (Section 2.3.3). We employ the reflexive thematic analysis (TA) approach for analyzing empirical data which is well suited for exploring, interpreting and finding patterned meaning in qualitative data (Section 2.3.4).

2.3. Overview of Qualitative Research Methods

Our philosophical assumptions lead us to qualitative inquiry. Qualitative data collection methods include naturalistic field observations and interaction with the participants such as via interviews and focus groups. The researcher plays a key role in collecting and interpreting the data, and then reporting the findings [49]. Qualitative data analysis methods are interpretive, for e.g. grounded theory and thematic analysis. In this section, we introduce and provide an overview of the different approaches that guided our qualitative research to answer the main research question.

2.3.1. Archival Research - Literature Review

Archival research refers to the obtaining of data from documents, typically those in archives and repositories (such as manuscripts, documents, audio & visual materials etc.) [49]. The pros of this method are ease of availability and accessibility of historical open-data, which makes for a rich data source that was compiled with attention and it saves the researchers' time and effort for transcribing [49]. The cons include unavailability of private/protected data, outdated or incorrect data, time-consuming process of searching for the right documents and intensive manual work of reading and understanding the archival data [49].

We conduct an extensive literature review of the computer security domain to first understand the state of knowledge. We followed the Systematic Literature Review (SLR) process laid out by Kitchenham et al. [150] and reviewed peer-reviewed publications from 14 top-tier venues in the field stretching over a period of 11 years. We scoped the review by developing a strict selection criteria (Section 3.1), thereby saving some time in the search process. However, the process of reading the archives was highly time- and effort-consuming but worthwhile in creating a strong foundation for this project. We analyzed the selected literature on six aspects (Subsection 3.1.4): perspective on human factors (rooted in safety science), population sample, recruitment methods, research objective, research method and use of theories. This review and the findings are presented in Chapter 3.

2.3.2. Interviews

Interviews involve talking to the study participants one-on-one in a structured or semi-structured way [49]. The advantages of this method are that we can gather the participants' lived experience and perspectives in their own words (specially if it is difficult to observe them in natural settings) and it also allows the researcher to direct the line of questioning [49]. There are also several cons such as participant bias (e.g. social desirability bias) and researcher bias (e.g. confirmation bias).

We choose interviews as our data collection method because we wanted to better understand day-to-day system administration work from the perspective of sysadmins. To truly center the perspectives of sysadmins, we thought it best for them to tell their own story in their own words. We mitigated the limitations by using only open-ended semi-structured questions and steering clear of leading questions, by doing online interviews when participants were in their place of work and also giving them the option to choose between a video or an audio interview. We also strove

hard to be as unbiased in the analysis as possible by including several collaborators and a diverse research team. This interview study is presented in Chapter 4.

2.3.3. Focus Groups

Focus groups entails talking to multiple (6-8) participants in a group and deep-diving into a selected topic [49]. Usually a few open-ended questions are asked so as to give enough room for the participants to share their own opinions [49]. The advantages of this data collection method are similar to those of an interview. The disadvantages of this data collection approach are also similar to those of an interview study but having more than one participant in a session helps to mitigate the participants' bias.

We conduct a focus group study where multiple sysadmins (who are not cis men) could freely and safely share their experiences. We do this to dive deeper into their experiences by focusing on the social dynamics within which their work is situated. This way the participants could find commonality with other professionals in the group and discuss experiences that the PhD facilitators could not easily think of. Furthermore, having two facilitators for the focus group helps to mitigate the researchers' bias and a diverse research team helps in doing a minimally-biased analysis. This focus group study is presented in Chapter 5.

2.3.4. Thematic Analysis

For the empirical work presented in Chapters 4 and 5, we used inductive reflexive thematic analysis (TA). TA is used to *"develop patterns of meanings ('themes') across a dataset"* through a reflexive and recursive engagement with the data [34]. It is an interpretive, emergent and flexible process that is useful in centering the participants' perspective while also critically examining the researchers' role. Reflexive TA consists of six analyses phases [34], namely: a) Familiarising yourself with the dataset; b) coding; c) generating initial themes; d) developing and reviewing themes; e) refining, defining and naming themes and f) writing up. We elaborate on how we performed these steps in further detail in Chapters 4 and 5.

2.3.5. Feminist Research

Feminist research is motivated by social justice and looks beyond privileged viewpoints. It encourages us to challenge the positivist notion of objective knowledge and understands that all knowledge is contextual [120]. Furthermore, it roots itself in the observation that *participants* have expert knowledge about *their own* experiences. Feminist research is also about self-reflection of our role as researchers and identifying and understanding the biases we bring to our research. In addition, we must acknowledge the power we hold as researchers and strive to remove this power imbalance. Finally, feminist research advocates for intersectionality [48] (how gender intersects with all other forms of oppression such as race, ethnicity, sexual orientation, ability, class or age), slow scholarship [195], open access [186], and feminist citation [8]. While we do not claim that this entire PhD project has followed a feminist approach, each project has been more feminist than the last, with the final project (Chapter 5) employing an explicitly feminist lens throughout.

Parallels to the Safety Science perspective

Feminist research is motivated by social justice and hence tries to center the voices / perspectives of those that have been historically marginalized [1]. Safety science (the Safety-II perspective [128]) teaches us to better account for the real work-in-practice (what is already working well) to support operational safety and resilience (discussed earlier in Section 1.2.1). Both approaches are "bottom-up" - they look at what the situation actually is (from the point of view of those living it) as opposed to what it is imagined/supposed to be (perhaps based on policies, rules, etc., or from the perspective of the management). Both approaches realize that participants have expert knowledge and center the experiences of those people who are commonly overlooked in scientific research.

In our final empirical study (Chapter 5), we uniquely combine these two approaches. Feminist ideals drive us to imagine and build something new instead of trying to fix existing systems that are fundamentally broken and unjust. Safety-II teaches us to develop our understanding in a "bottom-up" way, and to support the work as it is done in practice. Such a people-centered approach to understanding what works and what is needed is essential to building something new that is more just and equitable.

2.4. Researcher's Role

The PhD researcher comes from an engineering background specialized in human factors and safety science topics, and is therefore an outsider in the sysadmin community. This is helpful when bringing in perspectives from other research domains but can be limiting when interpreting social processes in the specific context of system administration work. Fortunately, this PhD project was supervised by Dr.-Ing. Tobias Fiebig who has considerable practical sysadmin experience and helped in interpreting, contextualizing and directing the empirical work. We further discuss researchers' reflexivity and positionality in Chapter 5 (Section 5.2.1) in line with the feminist approach used in that particular study.

We strove to acknowledge and eliminate the researcher-participant power imbalance wherever possible. One way we did this was by following the institutional ethics requirements and obtaining approval from the ethics board (HREC) for all human-participants research. This included obtaining informed consent from the participants after sharing with them the honest project descriptions and data management plans. Next, the interpretive nature of this project makes it important to reflect on researcher bias and participant bias [49]. Researcher bias can occur when the researchers' perspectives or beliefs influence the research design or methods, and can manifest in various ways such as selection bias, confirmation bias, implicit bias, leading question bias [131]. We mitigated these by including multiple perspectives in the research team from the beginning, performing exploratory studies without looking to confirm any hypothesis and designing theoretically-rooted open-ended interview questions. Participant bias can occur most commonly in the form of social desirability bias and also in other ways such as friendliness bias or habituation

[1] to relegate to an unimportant or powerless position within a society or group [189]

bias [242]. To address these, we encouraged the participants to share their stories and took the responsibility of preserving their anonymity in the process. We aimed to keep the questions as open-ended and neutral as possible while also striving for an engaging talk with the participants where our main goal was to have a meaningful conversations and steer clear of "experimenter-subject" dynamics.

2.5. Research Flow

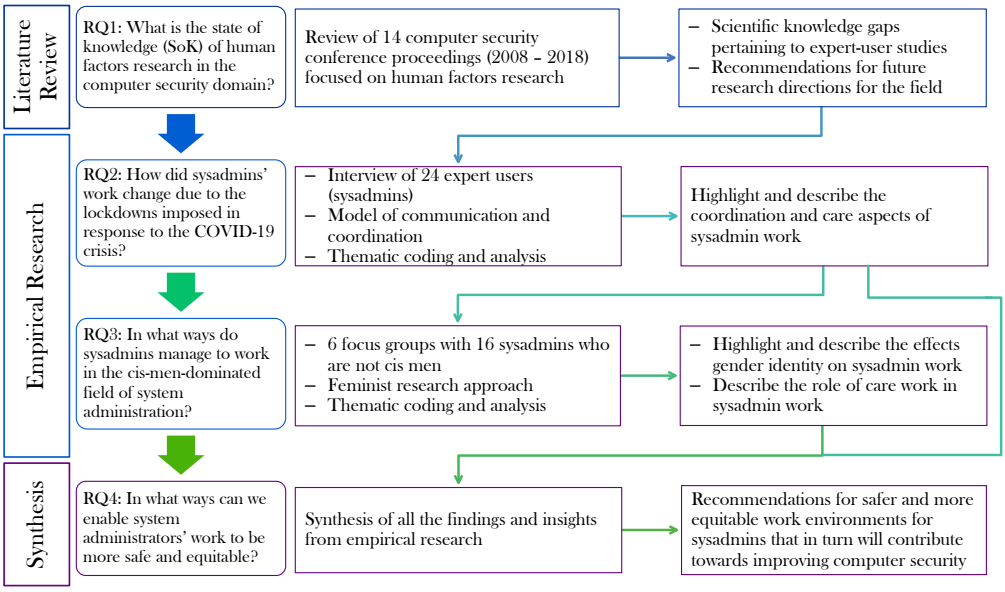


Figure 2.1: Research flow diagram

Figure 2.1 illustrates how the research process was carried out. The PhD journey began with the first question that inquired about the state of knowledge (SoK) of human factors research in the computer security domain. We performed an extensive literature review (Chapter 3) to answer this question which brought to light the knowledge gaps pertaining to expert users in the field of computer security. This then led us to focus on a specific group of understudied expert users, i.e. system administrators (sysadmins), and better understand their day-to-day work. We performed an interview study with 24 sysadmins (Chapter 4) which highlighted the coordination and care aspects of system administration work. Wanting to further focus on the care aspects, we employed a feminist lens for our next study. We conducted 6 focus groups with 16 sysadmins who belonged to marginalized genders (Chapter 5) and were able to highlight the role of gender in sysadmins work. Finally, using insights gained from the empirical work, we devised practical recommendations towards more safe and just work environments for sysadmins (Chapter 6).

2.6. Thesis Structure

Chapters	Research Questions	Methods
Chapter 1 Introduction	-	-
Chapter 2 Research Design	-	-
Chapter 3 SoK: Human Factors Research in Computer Security Domain	1. What is the state of art of human factors research in the computer security domain and what lessons can we learn for future research? a. What insights from the safety science domain can be applied to the computer security domain? b. What sample populations are being investigated and in what ways are they recruited? c. What is the objective of the research? d. What are the research methods that the researchers are using to study users? e. What kind of theories, if any, are the researchers using and how?	Systematic Literature Review of user studies in the computer security domain - (14 conference venues) between 2008- 2018
Chapter 4 System Administration during COVID-19	2. How did system administrators' work change due to the lockdowns imposed in response to the COVID-19 crisis?	Online one-on-one interviews with sysadmins Thematic Analysis
Chapter 5 Gendered System Administration	3. In what ways do (non cis-men) sysadmins manage to work in the cis-men-dominated field of system administration?	Online focus groups with sysadmins who are not cis men Thematic Analysis
Chapter 6 Discussion	4. In what ways can we enable system administrators' work to be more safe and equitable?	Synthesis
Chapter 7 Conclusions	-	-

3

State of Knowledge: Human Factors Research in Computer Security

The first step in our research strategy (as laid out in Section 2.5) is to assess the current state of knowledge of human factors research in the domain of computer security. Instead of solely considering technology, computer security research now strives to also take into account the human factor by studying regular users and, to a lesser extent, experts like operators and developers of systems.

Large-scale security incidents are often traced back to human error, like mistakes or forgetfulness [30, 125, 208, 224, 284]. The status quo approach to managing the human factors in cybersecurity says that humans are the weakest-link in security. Numerous efforts are made to eliminate, control or train the human factor in order to improve security [311]. Such human-factors studies have been a steady presence in the main security and privacy venues in the recent past. In fact, the portion of published work that includes user research has more than doubled over the past years. But what all constitutes human factor research? How has the field evolved in the recent past and what are the research gaps that still exist?

In this chapter, we focus our analysis of the state of the art on one critical population in human factors research: **experts**. By experts we mean the people who develop, build and run systems (a more precise taxonomy is developed in Section 3.1). Their errors can be highly consequential, as they can impact many systems at once or impact critical systems, on which many users and organizations rely. To better locate the studies on experts in the overall field of human-factors research, we also analyze a sample of end-user studies and compare both types of research throughout.

Investigating human factors is not one of our community's traditional areas of expertise and other disciplines have been studying human factors since much longer. Research in these domains have shown that the "weakest-link" approach is not the only way to manage the human factor [57]. This provides an opportunity for our community to learn from more mature areas which have investigated human behavior for many decades. Valuable lessons can be gained from safety science (discussed earlier in Chapter 1), which is an engineering-dominated discipline that aims at preventing adverse outcomes, similar to security, but with a substantially longer track record of incorporating human factors (discussed further in Section 3.2 and Figure 3.2).

Research that crosses over from computer security to these other fields is still rare. Examples include Egelman and Peer, who developed a Security Behaviour Intentions Scale (SeBIS) that measures users' attitudes towards various computer security tasks [76], and, Hámornik and Krasznay, who developed a research framework linking computer-supported collaborative-work (CSCW) and team cognition in high risk situations to better understand teamwork in security operation centers (SOCs) [115]. However, our community can build more systematically upon the work in social and safety sciences to leverage their theories and methods and to increase scientific rigor and generalizability, which are issues plaguing "security as a science" as pointed out by Herley et al. [123].

Our research question for the review is: **What is the state of the art of human factors research on experts in the computer security domain and what lessons can we learn for future research?** We analyze the current state

of human factor research in computer security to serve as a point of reference for new and established researchers alike. We review the literature on six aspects and answer the following sub questions:

1. What insights from the safety science domain can be applied to the computer security domain?
2. What sample populations are being investigated and in what ways are they recruited?
3. What is the objective of the research?
4. What are the research methods that the researchers are using to study users?
5. What kind of theories, if any, are the researchers using and how?
6. How did the researchers evaluate the ethics of their work?

Whether it be design-oriented or descriptive work, we first want to account for all the human factors research and create an overview of the state of the art. We scope our work by identifying papers that directly involve people in the main computer security venues from the past ten years. We end up with 557 publications in total. Then we group these papers based on the population they investigate, i.e., whether the paper deals with end users or expert users. End users are the focus of 91.4% of the papers, while expert user studies make up a mere 8.6% of the publications. We systematize the state of the art for the expert user group and analyze all of the 48 papers in depth. For comparison, we also review a sample of end user papers. Since we cannot analyze all the 509 papers in depth, we have chosen a stratified random sample of 48 end user publications. Subsequently, for each category, we provide recommendations on how the field can further mature. The contributions of this study are:

1. We find that expert users, different from end users, are an understudied population in terms of human factors in computer security, even though their behaviors and mistakes have higher stakes and more severe consequences.

2. We also find that papers on expert users commonly treat human error as a root cause to be removed from the system. This is an opportunity to learn from safety science research where the focus is to better understand the human factor and in turn build resilient systems that produce the desired outcome despite human error.

3. Similar to other fields, we find that the recruitment of study participants is dominated by convenience sampling and has a geographical bias towards the US and Europe, which threatens international generalizability.

4. Most human factors research (78.12%) lacks theory to inform research design and causal reasoning. Even research that utilizes Grounded Theory regularly stops before the step of building a theory from the empirical findings. The absence of theory limits the generalizability of the findings beyond the context of the study itself.

In this chapter we first detail the paper search and selection process in Section 3.1. Following that we structure our investigation as follows: (i) The perspective

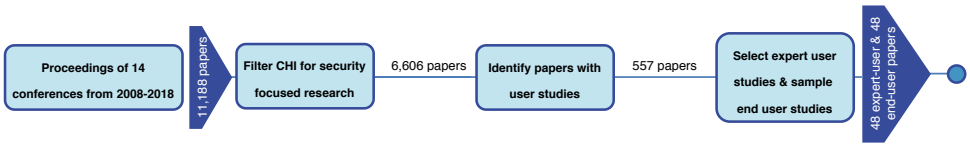


Figure 3.1: Visual overview of the search process.

on human factors (Section 3.2), and how we can learn from safety science; (ii) How and who are the participants recruited (Section 3.3), and how this—as we find—creates a western-centric perspective; (iii) Research objectives (Section 3.4), and how to align these with the chosen research methods (Section 3.5); (iv) How theories can be used to increase rigor in the communities scientific work (Section 3.6), including limitations to the use of Grounded Theory, which is often incompletely applied; and (v) How researchers handle ethical implications (Section 3.7), and what we can do to account for them more consistently.

3.1. Paper Search and Selection Process

In this section, we present our approach to building a representative corpus of human-factor studies and present the analysis criteria for our subsequent analysis.

3.1.1. Search Process

We perform a systematic literature review (SLR), inspired by Kitchenham et al. [150], to identify publications on human factors in computer security. Figure 3.1 presents an overview of the major steps of our selection and filtering process.

Inclusion and exclusion criteria

First, we perform an comprehensive search across the most prominent computer security venues. Specifically, we selected all top-tier (Tier 1 and 2) computer security and network operations venues, based on a common ranking.[1] We consider venues that purely focus on cryptography, like Crypto or TCC, as out of scope. Furthermore, we did not include workshops, as for example USEC, as our goal is comprehensiveness, not completeness, even though they also publish a sizeable number of human factors related security work. We do, however, add the Symposium on Usable Privacy and Security (SOUPS, Tier 3) to this list, as it is a major venue for usable security. We also add ACM CHI, the Conference on Human Factors in Computing Systems, which is the "premier international conference of Human-Computer Interaction". Overall, we reviewed the proceedings of 14 conferences from 2008 to 2018, resulting in an initial set of 11,188 papers. We specifically chose to limit our search scope to this period because we want to investigate the current development of the field. Also, we do not present search keywords because all the papers were

[1] See http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm. The list was updated after we had finished our search and now has 18 venues in Tier 1 and 2, instead of 17. We acknowledge that this list does not constitute an 'official' ranking, yet is commonly used within the community, even though it is critically acclaimed by some for its selection of venues.

selected from these venues. Next, we reduce the set of papers to 6,606 papers, by only including papers from ACM CHI that are presented in sessions related to security, privacy, passwords, and authentication. We acknowledge that this might lead to individual papers within CHI being omitted. However, to set a reasonable scope for the literature review, this limitation was necessary. We read the title and abstracts of all 6,606 papers to identify those that investigate human factors. The key criterion is the direct involvement of humans in the research, both online and offline, to study *behavior* or *actions*. This means we exclude papers that only perform large-scale internet measurements to understand user behavior. Furthermore, we also exclude papers that do not contain full-fledged user studies, for example Czyz et al., who perform an unstructured inquiry via email to identify root causes of IPv4/IPv6 security misconfigurations [51]. Ultimately, this selection process took over 1,300 working hours. We identified 557 papers on human factors in security (see Tables 3.2 and 3.3 for an overview). Finally, we discuss the limitations of our search process in Section 3.8.

3.1.2. End Users and Expert Users: A Taxonomy

Here, we developed a taxonomy of what users are being studied to explain how we arrive at the distinction between "expert users" and "end users" which we use for segmenting and sampling the literature in the next section. This categorization is based on the task that is being studied, rather than on inherent properties of the user who participates in the study. If the task is part of expert work, then we include the study as an expert study. This means that even when a person which could be classified as a "security professional", if this person is participating in a study of an email user interface, this participation would not make the study an "expert-user" study. Similarly, studies that subject "non-experts" to expert tasks, like vulnerability discovery in the case of Votipka et al. [286], do not become "end user" studies because of the utilized population.

- **Expert Users (Building Systems):** Expert users are those that build and run systems. Contrary to end users, they directly influence the security of systems *used by someone else*. Studies in this category deal with tools exclusively used in this context, that is, the process of providing a system for a third party (end users), and the processes and behaviors associated with the process of running these systems.
  - **Developers:** Developers write the code for end user visible applications as well as the back-end systems that make these tools function. A common sub-distinction for developers is frontend vs. backend developers.
    - **Frontend Developers:** Developers who work on the user interface of applications.
    - **Backend Developers:** Developers who work on the backend, that is, they create application programming interfaces (APIs) that can be used by the frontend to handle database interactions and business logic.

- **Fullstack Developers:** Developers versed in frontend and backend tasks.

– **Operators:** Operators are those running systems (also discussed earlier in Section 1.1). They deploy and update software created by developers, configure network equipment, and provide *services* to users. We note, that this distinction is difficult. On the one hand, we see that the community often utilizes "developers" as a covering term for everything that involves building and running a service or application, thereby covering operators. On the other hand, recent developments in how we run systems more and more merge the concept of operations and development, that is, DevOps [269]. Below, we provide a non-exhaustive set of examples of operators.

- **System Operators:** System operators operate systems in general, akin to fullstack developers, that is, they take care of systems from several of the following categories.
- **Network Operators:** Network operators deal with network infrastructure, that is, they configure network switches and routers, and are usually also in charge of designing the physical network.
- **Client Operators:** Client operators are among the most visible operators of an organization, as they deal with provisioning and providing patches to workstations, which are the most user-visible activities.
- **Help Desk Personnel:** Help desk personnel is commonly the first point of contact for users. Although help desk staff does not fall into the "traditional" operator categories, they often receive some operational permissions to handle common user requests.

– **Security Experts:** While security professionals constitute their own class, they often overlap with other roles from development or operations. However, due to the context of our work, we detail them as a dedicated class.

- **CSIRT/SOC Workers:** Computer Security Incident Response Teams (CSIRTs) and Security Operations Center (SOC) workers handle threat intelligence feeds and incident reports received by an organization and follow up on potential threats.
- **Red/Blue Team Members:** Red and blue team members conduct assessments of an organization. While red teams attempt to gain access to systems as "attackers," blue teams audit infrastructures to identify security issues and "defend."
- **Residential Security Experts:** Residential security experts often overlap with blue team work, and they are members of an organization who are in charge of assessing and reviewing security sensitive changes in code bases or concerning infrastructure.

  - **Researchers:** Some papers study computer-security researchers as their sample population. These studies account for the researchers' perspective in the computer security domain.
  - **Computer Science (CS) students:** Many of the studies recruit computer science students as a proxy for expert users. These students have a technical background and are a convenient sample in academic research.
  - **Others:** The remaining studies are categorized as 'other'. These include experts from various organizations such as those that develop cryptographic products [118], studies that perform participant observation inside the organization [261], studies that include hackers [196] etc.

- **End Users (Using Systems):** This group contains *users* of systems. This means that this group is not involved with *running* or *changing* the systems they use, and they use these systems for personal—in a private and professional context—activities, such as reading or encrypting one's emails.

  - **Applicable Subgroups:** For end users, various population slices are applicable. This ranges from studies of the elderly and their security behavior [92] to children [163], and it includes classifications of profession related subgroups, like journalists or aid workers. We identified the following sub-groups for our study, namely: the general public, university students/staff, specific users groups like journalists or air workers and children.

Improving human factors clearly requires different approaches and solutions for expert tasks compared to regular end-user tasks. One can design very different solutions given the stark contrast in training and competencies of experts compared to end users. Furthermore, the stakes of individual human errors of experts are often higher. A simple error during the operation of a system of the development of software can easily affect hundreds to thousands to even millions of users. This, in turn, may have a significant impact on how human factors need to be treated for these two different populations.

3.1.3. Dataset Overview and Sampling

The first observation we can make is that human factors research is on the rise, both in an absolute and a relative sense. Starting at 21 papers in 2008 (3.4% of all studies in the selected venues), the number of human factors papers rose to a total of 88 in 2018 (6.1%). Naturally, most of these papers appeared in SOUPS (198) and ACM CHI (133). We do not consider all SOUPS papers because not all include user studies, that is, users were not directly involved in the research, for example, in the case of literature surveys and position papers.

From a human factors perspective, different user populations present different challenges, which also implies the need for different theories and methods. The most important distinction we encountered across the corpus of papers is between *expert users* and end users, see Section 3.1.2. End user studies typically concern themselves with topics like interfaces used by the general population, or user behavior

Conference	2008		2009		2010		2011		2012		2013		2014		2015		2016		2017		2018		Total	
	HFS	All	HFS	All	HFS	All	HFS	All	HFS	All	HFS	All	HFS	All	HFS	All	HFS	All	HFS	All	HFS	All	HFS	All
ACM AsiaCCS	-	40	1	40	1	37	2	61	3	47	3	61	5	50	-	71	5	83	4	72	3	62	27	624
ACM CCS	-	52	1	58	1	55	1	61	3	81	6	96	5	138	4	131	6	146	9	159	9	140	45	1,117
ACSAC	1	45	1	48	1	42	2	41	3	45	1	40	2	47	4	47	3	47	4	47	8	60	30	509
IEEE DSN	1	58	-	64	-	65	1	52	-	51	-	68	-	57	-	50	1	58	-	55	-	62	3	640
ESORICS	1	37	-	42	-	42	2	36	-	50	-	43	-	58	1	57	-	59	-	56	1	55	5	535
IEEE CSF	-	22	-	22	-	23	-	21	-	25	-	19	2	29	-	35	-	33	-	34	-	27	2	290
IEEE S&P	-	28	1	26	1	34	2	34	2	40	-	38	1	44	1	55	6	55	8	60	5	63	27	477
ACM IMC	-	31	-	41	-	47	1	42	-	45	-	42	-	42	1	44	-	46	-	42	-	43	2	465
ISOC NDSS	-	21	1	20	-	24	1	28	1	46	5	50	2	55	3	50	-	60	2	68	5	71	20	493
PETS	-	13	1	14	-	16	1	15	2	16	1	13	4	16	-	23	9	51	5	52	3	35	26	264
RAID	-	20	1	17	-	24	-	20	-	18	-	22	-	22	1	28	1	21	-	21	-	32	3	245
SOUPS	10	12	14	15	14	16	15	15	14	14	15	15	21	21	21	22	22	22	26	26	26	28	198	206
USENIX Security	-	27	1	26	2	30	1	35	4	43	2	45	4	67	5	67	1	72	5	85	11	100	36	597
ACM CHI	8	218	7	277	10	302	15	409	7	369	5	392	10	465	18	484	21	545	15	600	17	665	133	4,726
HFS papers (%):	21 (3.4%)		29 (4.1%)		30 (4.0%)		44 (5.1%)		39 (4.4%)		38 (4.0%)		56 (5.0%)		59 (5.1%)		75 (5.8%)		78 (5.7%)		88 (6.1%)		557	(5.0%)
End Users	19		26		29		42		38		36		53		54		71		70		70		509	
Experts	2		3		1		2		1		2		3		5		4		8		18		48	

Table 3.1: Literature on human factors in security (HFS) vs. all papers, for major security venues between 2008 and 2018. For each year we list the number and share of HFS papers for that year, and how they are distributed over end users and expert users.

around widely-used technology. In contrast to end users, expert users do have prior knowledge, training, or experience in software or hardware engineering, networks, or systems operations, which they use to build systems.

Overall, we find that end user studies considerably outweigh expert user studies: 509 of 557 papers deal with end user (91.4%), while only 48 papers (8.6%) concern themselves with expert users. The lack of human factor research on expert users is alarming. While numerically clearly a smaller group, the behavior of expert users typically affects more systems than just their own, thus having a comparatively larger impact on security than individual end users. For example, system administrators making security misconfigurations can affect thousands or more regular users. For our study, we review all the 48 expert user studied in depth. To gain additional insights, we have also reviewed a group of end user papers. Since we cannot analyze all the 509 papers in depth, and the two groups are imbalanced, we have chosen a stratified random sample of 48 end-user publications. Stratification was done by publication year, that is, we matched the distribution of expert user papers over time by randomly choosing papers from the end user group corresponding to the number of expert user papers per year. To illustrate: since two papers on expert users appeared in 2008, we randomly selected 2 out of 19 end user publications in 2008. We acknowledge that this might limit our view on the literature on end users. However, given the vast body of existing literature, an exhaustive analysis is infeasible, and a stratified sample based on the temporal distribution of the expert user sample provides a reasonable trade-off between reliability and feasibility.

3.1.4. Analysis Criteria

We analyze the literature on six aspects: The general perspective on human factors, the sample used in the study, how this sample has been recruited, the research objective, how the authors utilized existing theory or methodology to inform their research design, and, ethical considerations.

Perspective on Human Factors: In safety science, decades of research has fundamentally changed the understanding of human factors and human error. The current perspective of safety science sees human error not as avoidable, but as a property of human work, which systems have to account for to ensure safe operations in the presence of error. This evolution is summarized in five major stages, which we discuss in the next Section (see also Figure 3.2). We analyze how research on human factors in computer security compares to this understanding from safety science.

Study Population: Naturally, we also investigate the samples used in contemporary research. We identify the major types of populations based on how authors describe their samples. This taxonomy is discussed in Section 3.1.2. For end users, these groups are "children" (minors), the general public, university-affiliated users (like staff and students), and other specific user groups. For example, some studies focus on users with social disorders [204], South Asian women [239], or users in relationships [164, 215]. If no information about the sample population is available, then we mark the population as "N/A."

For expert users, we broadly differentiate between developers, operators, security professionals, researchers and computer science students. Each of these categories is explained, along with the subdivisions, in Section 3.1.2. When studies compare expert users to end users, a confusing edge case, we classify them as "end users" among the expert-user publications. The remaining studies on expert users we categorize as "other". This includes studies where a set of different experts from a specific organization or set of organizations are involved [118, 260, 261], technical experts and end-users are recruited for a comparison study and their expertise is not specified [248], or a study with hackers and testers [286]. As an additional point of reference, we also identify the geographic region from where samples are collected, and where the authors themselves are located.

For our analysis, we only consider the broad categories and not the subdivisions. For example, we talk about frontend, backend and fullstack developers in our taxonomy. During the analysis however, we broadly classify all these under the developer category.

Recruitment: We analyze how researchers recruited participants. For end users, we consider recruitment via crowd-sourcing platforms (like Amazon Mechanical Turk, or other crowdsourcing platforms like CrowdFlower [12, 42]), recruitment in the local city, at the local university, via personal contacts, a recruitment agency, social media, or "other" online channels. For example, these online channels can be Craigslist [95, 278, 312], Sampling Survey International [229], or simply using other non-crowdsourcing platforms online, like message boards.

Similarly, for expert users, we distinguish between crowd-sourcing platforms, GitHub, the local university, personal contacts, industry contacts or industry organizations, social media, and "other" methods. Other recruitment methods include recruitment at a conference [118, 160], public bug bounty data [286], or establishing an online brand [70]. In case the authors fail to provide sufficient recruitment information, we mark it as "N/A."

Research Objective: Concerning the research objective, we distinguish between studies that (a) evaluate an artifact, (b) test hypotheses, (c) perform general exploratory research and (c) focus on gathering users' perspective on specific issues. Moreover, if authors evaluate an artifact, we check if they used an existing research framework for building and evaluating the artifacts, such as design science, and whether they include user feedback or evaluation results in the design of their artifact.

Research Method: We systematize *how* researchers conduct their studies by distinguishing between studies performed in a local laboratory, online, using interviews, surveys (including questionnaires), focus groups, or using observations. One study can have multiple research methods.

Theory/Framework: Regarding the use of theories and frameworks, we scrutinize how authors use existing scientific theories. Specifically, we investigate if they

1. use an existing theory to inform their research design or set out to validate and improve upon an existing theory
2. mention an existing theory in the context of their results and observations
3. neither use or mention a theory

In our analysis, we identified three major theories (Mental Models, Sensemaking, and the Theory of Reasoned Action). Furthermore, we closely study work that claims to use grounded theory, which is a methodology that creates theory through a systematic process of data gathering and interpretation. Correspondingly, we do not mix it with the use of existing theories, but add an additional category, in which we explore whether authors

1. focus on the methodological parts of grounded theory to obtain observational results and generally inform their qualitative data analysis
2. use a "middle ground" approach [241], in which they contrast their findings with existing theories
3. perform grounded theory to construct a new theory or model

Ethics: Finally, we study whether the authors considered the ethical implications of their work. We distinguish between

1. authors that obtained full clearance from their ethical review board
2. those who discuss the ethical implications but did not or could not obtain a clearance from a review board, e.g., because their institution does not have one,
3. authors who do not discuss the ethical implications of their work

3.2. Perspective on Human Factors in the Reviewed Papers

As discussed earlier in Chapter 1, research on human factors has emerged in safety science decades earlier than in computer security. In this section, we briefly reiterate the safety science perspective with a visual aid (Figure 3.2). We then present the computer security perspective on human factors research and what we observed in

our literature review. Finally, we present our key observations and recommendations at the end of the section.

3.2.1. Safety Science Perspective

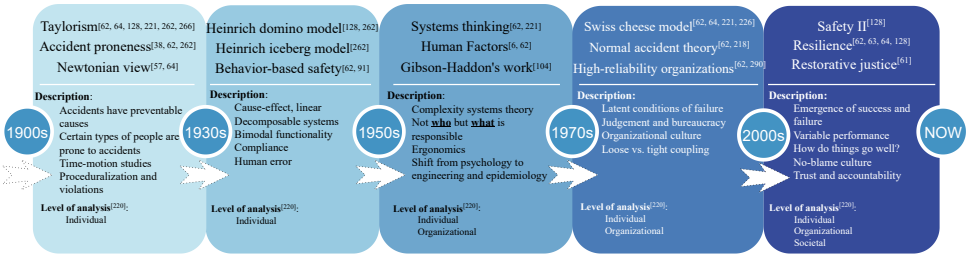


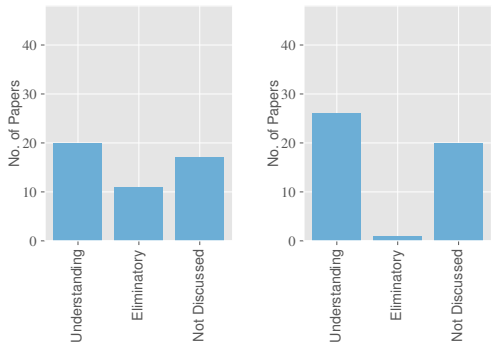
Figure 3.2: Overview of the development of human factors research in safety science [62]. Note how over time, the perspective shifted away from individual responsibility to, first, organizational factors, and finally to a societal perspective. Ultimately, the focus is no longer on how to prevent human error, but instead, on how to facilitate proper resilient operations (This figure is also presented in Chapter 1 as Figure 1.1).

The contemporary perspective on human factors shifts away from elimination towards understanding. We find that trying to *eliminate* the human factor is not the only (main) way to build safe and secure systems. It is also essential to understand *why systems do not fail* in daily operations as well as in the presence of human error. In other words, we must understand how the human factor contributes to *success* (see Figure 3.2).

3.2.2. Computer Security Perspective

We have discussed the computer security perspective on the human factor in detail in Chapter 1, Section 1.2.2. The current understanding is that many serious computer security incidents occur due to simple errors – or security misconfigurations - which are often attributed to human errors made by system administrators [70]. In fact, most of the issues in computer security are related to the human actors [311]. Hence, "human error" is considered to be a serious security concern. Examples of large-scale computer security incidents attributed to human error include the Equifax data breach (2017) where personal information of 148 million users was compromised using an application vulnerability on their website and the Facebook data breach (2019) when multiple unprotected Facebook databases were exploited to leak sensitive account information (such as phone number, location, gender) of 540 million users [273]. Such incidents are often declared as preventable.

To be able to classify human factors in computer security literature more easily, we condense the perspective of safety science in the following way: a) eliminating the human factor, that is, preventing errors, b) investigating the human factor to understand what makes things go the way they go and c) neither of these perspectives is identified. We marked papers trying to "eliminate" the human factors in column "HF Persp." with a ● and those that are trying to understand the real-world



(a) Expert Users (b) End Users

Figure 3.3: Overview of the perspective taken on the human factor in expert-user and end-user papers. We see that the eliminatory perspective is still more prevalent in papers dealing with experts.

phenomenon with a ○ under "Theory/Framework" in Tables 3.2 and 3.3. If neither of this perspectives is identified, the paper is unmarked.

We find that eleven papers in the expert-user sample take the elimination perspective, as opposed to one paper from the end-user studies, These papers set the premise of error elimination by proposing complete or partial automation [81, 82, 99, 160, 205, 305], emphasizing the role of policies, systems and frameworks [97, 140] or focusing on "human error" as the root cause [80, 200]. We connect this observation to how we, in general, perceive experts and end users. Professionals are expected to be knowledgeable and trained enough to not make mistakes. Researchers, especially from the engineering field, implicitly assume experts should know better than to make certain mistakes in the operation and creation of systems.

In end-user studies, on the other hand, we often encountered the somewhat condescending notion that end users are "the weakest link" in systems' security. While this notion initially points towards a similar elimination of the human factor, we observe that in practice that it is implicitly accepted that mistakes are unavoidable and that systems and environments should perform well in the face of these mistakes. It seems that, here, the field has embraced another perspective.

We find that about half of the papers (20 for experts and 26 for end users) take the perspective of understanding the human factors. For expert users, this mostly consists of researching the perspectives of users [13, 19, 20, 70, 94, 117, 135, 201, 212, 248, 268, 286, 294], organizational factors [77, 118, 308] or both [260, 261]. They investigate the perceptions and attitudes of experts, such as operators, security experts, or developers, and they provide important insights into the real-life practices and processes of complex operations. Studies on the organizational aspects are researching interactions among different stakeholders and the role of other factors such as culture. These approaches are important because accounting for the sociotechnical factors creates a more realistic description and better equips us to deal with the operational uncertainties.

The end-user studies look at user perspectives around the security and privacy challenges of emerging AR technologies [164], layman's understanding of privacy [209], user behavior and opinions on the adoption of two-factor authentication [46] and whether social disorders influence social engineering [204], to name some examples. Just as expert-user studies, these papers provide important insights into users' perspective and real-world concerns.

3.2.3. Observations and Recommendations

Key Observations: We find that past research on expert users mainly took an eliminatory stance. That is, the research tried to remove the human factor from systems, for example, by introducing automation. This approach is losing steam in safety science research, mostly based on the insight that the human factor cannot be ultimately eliminated, and, therefore, systems rooting their safety and security in this are ultimately never really safe. Fortunately, the situation is better for end-user related work, which hardly takes the traditional perspective of eliminating the human factor and focuses on usability studies and learning the users' perspective.
Key Recommendations: Given how often human error is considered to be the root cause of security vulnerabilities, we encourage the field to rethink the perspective that we take concerning human factors in computer security, especially when studying expert users. One key takeaway is that in addition to preventing human error, we should also try to understand which behavior leads to secure outcomes, and how we can facilitate that behavior. To accomplish this, we will have to investigate—especially expert users—in their daily interactions with the tools and issues we focus on, something that is hardly done at the moment (see 3.5).

3.3. Sample Population and Recruitment in the Reviewed Papers

Next, we look at the population samples, that is, *who* researchers investigate and how they recruit the participants. Our results are summarized in columns "Sample" and "Recruitment" in Tables 3.2 and 3.3, and we visualize the geographic distribution of authors in Figure 3.4.

3.3.1. Population Selection and Recruitment

In the expert-user studies sample, we discover that Computer Science students and security experts are the most utilized populations. This holds true even for end-user studies. In other words, university students are the most popular population sample being studied for both expert and end-user studies. This is to be expected: members of the (local) university are easily accessible for university researchers, that is, they constitute a convenience sample. Interestingly, only one of the papers is specifically studying college students as their intended research subject [225], while the remainder used them as a convenient proxy for end-user and expert-user populations.

Regarding recruiting participants from these populations, we identified eight categories for both expert and end-user samples, though not exactly the same cat-

Year	Idx.	Ref.	Sample: Developers	Operators	Other	Researchers	Sec. Exp.	CS Students	End-Users	Sample Loc.	Author Loc.	Ext. Validity	Recruitment: MTurk	GitHub	Univ.	Personal	Industry	Social M.	Other	N/A	Res. Obj.: Eval.	Hyp. Test	Exploratory	Perspective	Research Method: Lab	Online	Interview	Survey	Focus Groups	Observations	Theory / Framework: Mental Models	Sensemaking	TRA	Other	GT	Design Eval.	HF Persp.	Ethics
2008	E1	[292]					●				○	◐							●		●			●			◑		◑		○			○		◑	○	○
	E2	[203]		●							○	◐								●	●			●	◐									○		◑	○	○
2009	E3	[77]			●						○	○				●	●							●				◑				○				○	○
	E4	[19]		●							○	○				●								●		◑					○	○				○	○
	E5	[85]					●			○	○	○							●		●				◑		◑								◑		○
2010	E6	[136]			●						○	○							●		●				◑		◑	◑		◑					◑		○
2011	E7	[129]		●						○	○	○			●						●				◐										◑		●
	E8	[134]				●	●			○	○	◐			●				●		●				●		●		●					●	◑	◑		●
2012	E9	[305]	●					●		○	○	◐			●	●					●				●		●					○				◑	●	○
2013	E10	[81]	●								○	○							●		●						●						○		●	●	○
	E11	[20]			●			●			○	○				●		●			●	●			◐							○	○		●	○	○
2014	E12	[135]					●		●		○	◐	●						●		●		●	●		●	●						●	◑	●	○	○
	E13	[211]	●							○	○	○			●		●					●		●				●					●			○	●
	E14	[80]		●							○	○							●					●				◑				○	○			●	◑
2015	E15	[260]			●					○	○	●								●			●	●			◑		◑				●	●		○	●
	E16	[133]					●		●	●	○	◐	●			●		●	●					●			◑	●			○	○					○
	E17	[140]			●			●	●	○	○	◐			●	●			●					●			◑				●			○		●	○
	E18	[97]		●						○	○	◐			●		●		●					●				●				○				●	○
	E19	[82]	●								○	○				●			●		●					◑							○		◑	●	●
2016	E20	[56]					●		●	○	○	◐							●	●			●	●			●	●					○	○			○
	E21	[261]			●					○	○	◐								●			●	●					◑					●	◑		○	●
	E22	[306]					●		●	○	○	○			●		●				●			●		◐		◐				○			◑			○
	E23	[3]	●						●	○	○	◐			●			●	●					●	●		●		●			○	○					●
2017	E24	[93]			●				●	○	○	◐			●				●	●				●			●				●				○			●
	E25	[4]	●								○	◐		●								●	●			◐		◐				○		○				●
	E26	[160]					●		●	○	○	●			●		●		●					●	●		●	●				○				●	◑
	E27	[200]							●	○	○	◐			●									●	◑		◑	◑			○			○		●	◑
	E28	[205]	●						●	○	○	●			●		●				●	●				◐		◐							●	●	●
	E29	[68]	●								○	◐					●							●				◐			○	○					●
	E30	[94]				●				○	○	○							●	●		●		●				◐				○		○			●
	E31	[2]	●								○	●		●								●	●			◐		◐			○				◑		●
2018	E32	[117]					●				○	○				●			●					●	●		◑						◑	○		○	●
	E33	[196]			●	●	●	●			●	●			●		●				●			●	●			●	●			○	○		◐		●
	E34	[256]		●							○	◐							●					●				◐			○	○					◑
	E35	[70]		●						○	○	○							●					●			●	●			○	○		○		○	◑
	E36	[248]			●				●		○	◐	●			●		●	●					●				●					◑				○
	E37	[286]	●		●						○	◐				●	●		●					●			◑					○	○	●			●
	E38	[99]	●								○	●		●		●		●	●		●			●	◐								○		◑	●	◑
	E39	[190]	●								○	○				●							●	●		◑					○		○				●
	E40	[294]	●								○	●						●			●			●	◐		◐				○		○	○	◐	○	●
	E41	[7]	●						●		○	◐									●		●	●	◑		◑						◑				●
	E42	[201]						●		○	○	◐			●							●		●	◐			◐				○	○		○		◑
	E43	[13]	●							○	○	◐				●		●					●	●		◑						○		○			●
	E44	[212]	●					●		●	○	○			●	●		●						●	◐		◐					○	○				●
	E45	[268]					●				○	◐				●								●		◑					○	○				○	●
	E46	[247]	●		●			●			○	○								●	●				●										◐	●	●
	E47	[119]						●		○	○	◐			●							●			◐			◐				○					●
	E48	[118]			●					●	○	◐				●			●					●			◑					○		○	○		●
Σ			17	7	12	3	11	13	7				3	3	17	15	11	8	20	9	18	8	12	29	14	10	24	25	2	4	12	19	2	29		31		

Legend:
Location: ○: Western (Europe, North America); ◐: Non-Western; ●: International (Multiple Regions); No Marker: Unknown;
External Validity: ●: Considered and addressed; ◐: Mentioned as a limitation; ○: Not discussed;
Methods: ●: Mixed Methods; ◐: Quantiative; ◑: Qualitative;
Theories: ●: Used; ◑: Mentioned; ○: Suggested;
Grounded Theory: ●: Full; ◑: Middleground; ○: Analytical;
Evaluation of Artifact: ●: Before and After; ◐: Before; ◑: After;
HF Perspective: ●: Eliminatory; ○: Understanding;
Ethics: ●: Review with HREC; ◑: Review without HREC; ○: Not discussed;

Table 3.2: Overview of expert related human factors in security research

egories. For expert-user research, the most popular recruitment method is via personal contacts and university channels. We note that it seems to be convenient to find experts through one's personal networks, specially for researchers working in the same field of expertise. For end users, university channels, like local (physical) message boards and on-campus recruitment, are the most popular recruitment method, followed by Amazon MTurk. Similar to the reason why university students are most studied, this is probably due to the fact that university channels are a convenient recruitment method.

3.3.2. Population Location

We find that in a large number of the studies, the population sample is based in North America or Europe. Only four end-user and expert-user studies each report

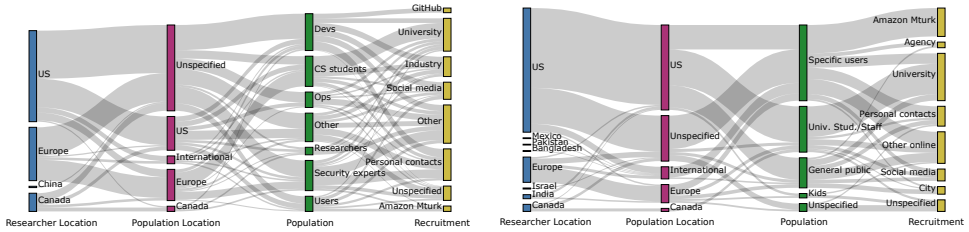
Year	Idx.	Ref.	Sample: Children	Sample: N/A	Sample: Gen. Pub.	Sample: Univ.	Sample: Spec. Users	Sample Loc.	Author Loc.	Ext. Validity	Recruitment: MTurk	Recruitment: City	Recruitment: Univ.	Recruitment: Personal	Recruitment: Soc. Media	Recruitment: Oth. Online	Recruitment: Agency	Recruitment: N/A	Res. Obj.: Eval.	Res. Obj.: Hyp. Test	Res. Obj.: Exploratory	Res. Obj.: Perspective	Research Method: Lab	Research Method: Online	Research Method: Interview	Research Method: Survey	Research Method: Focus Groups	Research Method: Observations	Theory / Framework: Mental Models	Theory / Framework: Sensemaking	Theory / Framework: TRA	Theory / Framework: Other	Theory / Framework: GT	Theory / Framework: Design Eval.	Theory / Framework: HF Persp.	Ethics
2008	NE1	[89]				●		○	○	●			●						●				◐			◑					○				●
	NE2	[75]			●			○	○	●		●				●							●						◑						○	○
2009	NE3	[184]			●				○	○				●		●				●	●			◐								○				○
	NE4	[151]			●		●	○	○	○							●				●	●		●	●							◑	○		○	○
	NE5	[141]				●		○	○	●			●						●	●				●								●		◑		●
2010	NE6	[132]			●		●	○	●	◐			●			●			●					◑					◑					◑	○	○
2011	NE7	[310]				●		○	○	●			●						●		●		◐			◐						●				●
	NE8	[244]				●		○	○	◐			●						●	●			◐			◐								◑		●
2012	NE9	[237]		●					○	○								●	●				◐			◐						◑		◑		○
2013	NE10	[235]				●		○	○	◐			●						●				◐									○		◑		●
	NE11	[67]			●		●	●	○	○			●			●			●			●	◑			◑						○		◑		●
2014	NE12	[289]				●		○	○	◐			●									●			●	●			○						○	●
	NE13	[14]					●		○	○	●										●	●				◐						●				●
	NE14	[192]				●		○	●	○								●	●	●			◐			◐						●		◑		◑
2015	NE15	[278]			●	●		○	○	◐		●	●			●					●	●	◑		◑				○		○				○	●
	NE16	[12]					●	●	◐	●				●		●					●	●			●	●						◑			○	○
	NE17	[42]				●			○	○						●					●	●		◐					○	○				○	●
	NE18	[24]				●			○	○	●								●					◐									◑		●
	NE19	[130]				●	●		○	◐			●	●		●			●							◐								◑		◑
2016	NE20	[79]					●		○	◐	●										●					●						●	◑		○	○
	NE21	[182]				●	●	○	○	◐			●		●				●		●		◑		◑							●		●	○	●
	NE22	[229]			●			○	○	●			●	●	●						●				◑				○		○		○		○	●
	NE23	[272]				●		○	○	○			●								●	●				●				○	○					●
2017	NE24	[163]	●					○	○	◐								●	●		●		◐								○		◑			●
	NE25	[236]			●			○	○	◐		●										●			◑							◑	●		○	●
	NE26	[270]					●	○	○	◐	●		●						●			●	●			●			●					◑		●
	NE27	[171]		●					○	○								●	●				◐										◑			●
	NE28	[245]					●		○	◐	●								●					◐										◑	●	●
	NE29	[309]				●		○	○	◐			●						●				◐										◑			●
	NE30	[43]				●			◐	◐	●			●					●					◐										●		●
	NE31	[1]				●	●	○	○	◐			●			●						●			◑				●				○		○	●
2018	NE32	[198]			●		●	○	○	◐				●			●				●	●			◑		◑		◑						○	○
	NE33	[225]				●		○	○	◐			●								●				◑						●		○		○	●
	NE34	[239]					●	●	●	◐				●			●				●	●					◑		○		○				○	◑
	NE35	[110]					●	○	○	◐	●					●					●	●				●			○		○				○	●
	NE36	[111]					●	○	○	◐	●											●				●			○	○					○	●
	NE37	[312]			●	●		○	○	◐			●		●	●						●			◑				●						○	●
	NE38	[142]					●	●	○	◐	●					●						●				●			○			○			○	○
	NE39	[215]					●	○	○	◐	●										●	●				●			○		○				○	○
	NE40	[204]					●	○	○	◐			●		●					●			●			●						◑			○	●
	NE41	[95]			●	●		○	○	◐			●		●	●				●	●			●		●						●			○	●
	NE42	[240]		●		●		○	○	○				●					●				◐			●							◑			○
	NE43	[46]				●		○	○	◐			●								●					●						◑			○	●
	NE44	[53]					●	○	○	◐	●											●				●						●				●
	NE45	[231]					●		○	●	●						●					●				●						○			○	●
	NE46	[209]	●		●			○	○	◐						●					●			◐				●				●			○	●
	NE47	[230]					●	○	●	●	●								●							◐			○		○			◐		○
	NE48	[164]					●		○	○	◐				●	●					●	●	◑		◑				○			○			○	●
Σ			2	3	12	18	25				13	3	21	9	6	16	3	4	19	7	16	25	18	9	12	23	2	0	18	2	6	26			27	

Legend:
Location: ○: Western (Europe, North America); ◐: Non-Western; ●: International (Multiple Regions); No Marker: Unknown;
External Validity: ●: Considered and addressed; ◐: Mentioned as a limitation; ○: Not discussed;
Methods: ●: Mixed Methods; ◐: Quantiative; ◑: Qualitative;
Theories: ●: Used; ◑: Mentioned; ○: Suggested;
Grounded Theory: ●: Full; ◑: Middleground; ○: Analytical;
Evaluation of Artifact: ●: Before and After; ◐: Before; ◑: After;
HF Perspective: ●: Eliminatory; ○: Understanding;
Ethics: ●: Review with HREC; ◑: Review without HREC; ○: Not discussed;

Table 3.3: Overview of end user related human factors in security research.

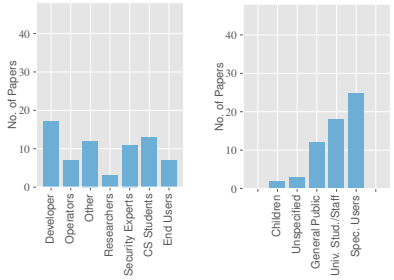
an international population sample. Hence, overall, the western user population is the most represented. This follows from our observation on convenience sampling, as we also see that most research itself is contributed by authors from the U.S. and, to a lesser degree, Europe. In Tables 3.2 and 3.3, we mark western authors and populations with ○, authors and populations from other regions with ◐, and international collaborations and populations with ●.

In our analysis of the end-user studies, we find that the majority of the eleven papers where the location of the population is not reported, are studying "specific users" (see Figure 3.4). Specific users, as explained earlier, refer to users of specific online channels, such as MTurk or the Security Behaviour Observatory, or other specific groups, like users with social disorders. For expert users, the group of papers not specifying the location of the studied population is even larger (24/48).



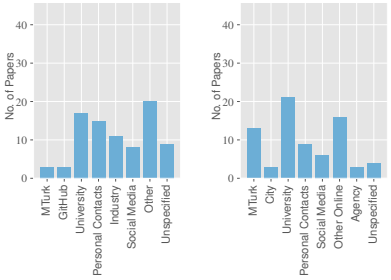
(a) Expert Users (b) End Users

Figure 3.4: Overview of Authors' location in comparison to the population types, recruitment methods, and population locations. The figure depicts how the share of publications across properties, for example, US, Europe, etc., for each category (Researcher Location, Population Location, Population, and Recruitment) connects to the other categories. For example, in 3.4a, we see that the majority of studies on US populations is contributed by researchers located in the United States. Similarly, the authors' location in 3.4b predetermines the populations' location, apart from studies using a population of *specific users* where the population's location usually is not disclosed. This is similar to 3.4a in so far, that Expert Users are predominantly recruited as a population of *specific users*.



(a) Expert Users (b) End Users

Figure 3.5: Overview of the studied populations for expert users (3.5a) and end users (3.5b). Note that for end users the focus is on specific users, such as users using a *specific* software, while for expert users the perspective is more on general observations tied to the function of the study participants (developers, operators, etc.).



(a) Expert Users (b) End Users

Figure 3.6: Overview of recruitment channels for expert users (3.6a) and end users (3.6b). For both samples, we see convenience samples being prevalent, that is, recruitment at the local university, or via personal contacts. Naturally, university sampling is more common for end-user studies, as the local university corresponds closer to the target population.

A likely explanation for this imbalance is that "expert users" are a form of "specific users." We conjecture that it is difficult to report the location of the population when people are recruited through online channels, which is the case in a large number of the expert-user studies. Similarly, when selecting for a specific type of users, expert or end-user alike, it may seem reasonable to not focus on the users' location. However, even when investigating specific users using an online service, the authors' location may predetermine the recruited population's location, for example, due to the language used for recruitment, or due to the service used being biased towards a population, like Amazon MTurk [228].

3.3.3. Challenges in Recruitment

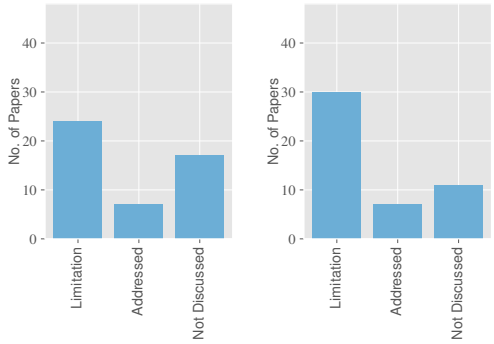
In end-user studies, recruiting a representative sample is difficult, as the use of technology is inherently global and cultural differences may influence the effectiveness of security measures [98]. In this case, it is better to acknowledge the limitations of one's population sample and report on the resulting restrictions on the generalizability of the results. For expert-user studies, representativeness is even more challenging. Recruitment channels are more limited and willingness to participate is often reduced due to the high workload of experts [70].

In their work on exploring a convenience sample, Acar et al. [4] further discuss the challenges in recruiting participants for expert-user studies. Different from end-user studies, where recruitment is fairly straightforward (MTurk, posting flyers, classifieds etc.), no well established recruiting processes exist for expert-user studies [4]. This is because it can be difficult to contact and invite professionals for in-lab studies, to find professionals locally, find free time in the experts' schedule or simply to provide enough incentives [70]. These observations close the loop to our earlier remarks on convenience samples, such as from a local university or via personal contacts: It is simply easier. However, when following this path, it is imperative to account for the limitations this introduces for the external validity of the obtained results.

3.3.4. External Validity

The limitations in study populations connect to the matter of external or rather global validity. External validity is an important parameter to be evaluated to understand the generalizability of results. To ensure external validity in quantitative studies, the researchers must restrict claims which cannot be generalized to all end or expert users. This can be due to the interaction of several factors, like participant selection, experimental setting or temporal factors [49]. For qualitative research, generalization has a different meaning. This is because the intent of qualitative inquiry is not to generalize the findings but to understand a phenomenon in its specific context. To ensure replicability in such cases, it is crucial to properly document the data collection and interpretation procedures used.

During our evaluation, we find that a majority of studies in both our samples do mention or discuss the generalizability of their findings (30 for end-user studies and 24 for expert-user studies), usually in the form of stated limitations (marked ◐). However, only seven end-user studies and seven expert-user studies take steps to address threats to external validity (marked ●). Examples of the steps taken include not using a laboratory setting and employing deception [141], assuring theoretical saturation of the sample [229], experience sampling in a wider population [231], and the global recruitment of specific developer groups (e.g., Google Play or Python developers) [99, 294]. However, this leaves eleven end-user and eleven expert-user studies that do not address the generalizability of their findings or mention the limitations thereof, which we mark with a ○. In general, there seems to be a trend to acknowledge limitations, as we find an increasing number of recent papers discuss their generalizability limitations compared to older work. This still leaves the issue that generalization often means generalization to a U.S. or western population



(a) Expert Users (b) End Users

Figure 3.7: Overview of how studies address the external validity of their results for expert users (3.7a) and end users (3.7b). Note that only a fraction of papers try to actively address this limitation, instead of simply stating it. Furthermore, in expert-user studies, this limitation is more frequently not even mentioned or discussed.

instead of a global population, see, for example, Redmiles et al. from 2019 [228] without explicitly stating this limitation. Given that *"Most People are not WEIRD [(Western, educated, industrialized, rich and democratic)]"* [122], this means that human factors work for expert and end users alike in our community has so far neglected the concerns of the majority of earth's population. It is imperative to fill this gap in the future.

3.3.5. Observations and Recommendations

Key Observations: We find that population samples are dominated by convenience sampling, that is, in the local environment of the researchers or via their personal contacts. In some cases, we observe Computer Science students being substituted for operators with operational experience [160]. Such limitations are regularly not discussed, or only mentioned as a limitation, while general conclusions are drawn. We tried to be representative by surveying the top security research venues on a global stage. We found that samples are nearly exclusively sourced from western countries (the U.S., Europe, Australia), without researchers acknowledging that the specific socio-economic background of their population might influence their results.

Key Recommendations: In future research, we, the community, must investigate more diverse population samples in terms of where the sample is located in the world to avoid selection bias. We acknowledge, that this is a hard problem. However, it is important to have a varied population represented in the top-tier computer security venues. Removing systemic bias within the field is a lengthy process, which cannot be paraphrased in a paragraph. As a point of reference, we recommend a paper by Guillory [106], who takes a stance on systemic racism in AI. Addressing this problem entails a cultural change in hiring researchers, mentoring early career researchers, and international collaboration. Indeed, looking at the surveyed papers,

we find that international collaboration with researchers from non-western regions, for example, Sambasivan et al. [239], holds promise for research which allows us to explore and understand the impact of one's socio-economic background on security behavior. The main point here is not "utilizing" researchers from the global south in the classical post-colonial western modus operandi to "get access to samples otherwise inaccessible," but instead collaborating with researchers as the peers they are to allow the wider community a better understanding of differences, and shaping technology in a way that enables secure behavior for humans taking their diverse backgrounds into account. This equally pertains to the perspective of hiring and mentoring, or as Guillory phrased it: *"While substantial research has shown that diverse teams achieve better performance* [...]*, we reject this predatory view of diversity in which the worth of underrepresented people is tied to their value add to in-group members"* [106]. Especially given the dominance of western economies not only in research, but also the development of tools and technologies, these steps are imperative to build a securely usable digital and global world.

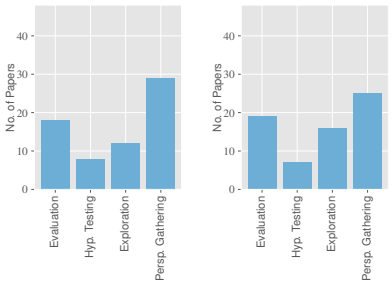
Nevertheless, research on a population from a specific region has independent scientific value. However, if we focus our research on a specific region or socio-economic background, we must report the location of the population along with recruitment method, sample size, demographics and discuss the generalizability of the findings to a specific population. While we see more work acknowledging limitations with regard to their sample population, simply acknowledging the current U.S./western bias is a limitation which we, as a community, must overcome. Furthermore, convenience sampling, which is currently common, must receive more scrutiny to ensure that results generalize outside its narrow scope, for example, beyond the university-attending population (see WEIRD [122]). It is important to place the research in the global context and work towards reducing biased data which can have serious real-world consequences [246]. If this is not feasible due to the constraints of the research project, the researchers must strive to discuss these limitations in terms of the cultural context and generalizability. Finally, to help the generalizability of the results, we suggest the use of theoretical frameworks. These can be used to inform the research design as well as aid the external validity of the findings. We discuss the use of theories in detail in Section 3.6.

3.4. Research Objectives in the Reviewed Papers

Following, we investigate the research objective of human factors in security research, that is, *what* researchers are investigating. For an overview of our findings, please see column "Res. Obj." in Tables 3.2 and 3.3.

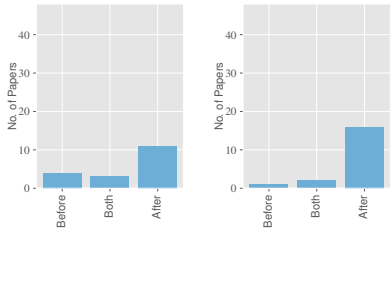
3.4.1. User Perspective and Exploration

Investigating the perspective of the user is the most common research goal across both expert and end users (see 3.8). For example, Dietrich et al. investigate system operators' perspective on security misconfigurations [70]. However, exploratory research is more prevalent for end-user studies, while a stronger emphasis is put on perspective gathering in expert related studies. Note the distinction between ex-



(a) Expert Users (b) End Users

Figure 3.8: Overview of research objectives in expert-user (3.8a) and end-user papers (3.8b). We find no fundamental differences in this parameter, apart from a slightly higher number of perspective gathering work in the expert-user sample. We conjecture that this is due to work on expert users only now becoming more prevalent.



(a) Expert Users (b) End Users

Figure 3.9: Overview when artifacts are evaluated and whether user perspectives/requirements are collected before the artifact is being developed in expert-user (3.9a) and end-user papers (3.9b). We find a very classical approach of *first* building a system and *then* evaluating it, instead of first collecting users' requirements and perspectives.

ploratory research and research trying to understand users' perspective: While the former tries explore a new area from an external point of view, the latter strives to describe how a specific user group *perceives* an issue. Interestingly, earlier work on expert users is dominated by work that evaluates artifacts, while more recent work shifted towards looking at their perspective on specific issues. This is in line with a mechanic in very early research focusing on end users, for example Whitten and Tygar [298], which also started out by evaluating artifacts, and then matured into considering users' perspectives.

For expert-user literature, a majority of it is concerned with gathering the user perspective and twelve publications are exploratory research. For end-user publications, there is a similar distribution between papers that are gathering the users' perspective and those that are exploratory. Gathering users' perspective is common for issues that are prevalent and understudied. Hence, in these cases, perspective gathering research is exploratory by nature.

Compared to expert-user research, slightly more end-user studies are exploratory. This might be the case because end-user research has been more prevalent and expert-user research is only slowly getting traction in the last few years. For both user categories, however, exploration itself is not the sole aim of most research.

3.4.2. Evaluation and Rigorous Design

Artifact evaluation is similarly common between end-user and expert-user studies, including the overlap with other research objectives. In both cases, about half of the existing research is solely performing an evaluation study and the remainder overlaps with the other aims.

Most evaluation studies evaluate an existing or new artifact, but not all of them directly evaluate the *usability* of an artifact. For example, Wermke et al. performed

a (non-user) evaluation of a tool to study obfuscation in Android applications [294]. For all evaluation studies, we identify under "Design Eval." as part of the "Theory/Framework" columns whether the evaluation was purely done to test something *after* (◑) it has been built, if they first collect users' input to then design an artifact (◐), or if they combine both approaches (●). Only two end-user studies and three expert-user studies gather requirements and input before designing an artifact, and later evaluate their artifact against the users again, see 3.9. A further one end-user study and four expert-user studies gather input from users before designing the artifact without validating the created artifact afterwards, again, see 3.9. This approach has the disadvantage that users' requirements are not incorporated in the design process of the artifact, which is problematic because the users' actual requirements may be different from the imagined user requirements, thus leading to poor artifacts. In industry, most development processes incorporate a user-driven design component, hoping to prevent a requirements mismatch [287].

The information systems community has already recognized the missing rigor in their artifact design and evaluation. To counteract this limitation, they formalized a processes known as "Design Science Research" (e.g., see March and Smith [178] or Hevner et al. [124, 285]). We suggest that studies in computer security that are in fact designing and evaluating an artifact also leverage the Design Science framework [124, 285]. Unfortunately, we could not identify any paper in our sample that explicitly uses the Design Science framework to inform their research.

3.4.3. Hypothesis Testing

Other fields, like the social sciences and safety science, regularly use theories as a guiding concept in their research. They employ a body of existing theories to formulate hypothesis that they can then test using appropriate research designs. Of course, there are other ways to create a hypothesis, such as through previous work or through anecdotal evidence. Only eight expert-user studies test a hypothesis, of which only one also uses an existing theory or framework. The remaining ones build hypotheses based on informal observations and related work. For end-user studies, seven papers test hypotheses. In general, work testing hypotheses often overlaps with evaluation and exploratory studies, and only few papers solely focus on testing a hypothesis.

3.4.4. Observations and Recommendations

Key Observations: At the moment, research is dominated by exploratory and perspective work, focusing on instances of problems instead of generalizing to a wider societal and organizational setting. Especially considering our earlier observations on recruitment and a geographic bias in current work, this poses a challenge for our field. As a field, we have to move beyond purely observing, and conduct work that systematizes, understands, and proposes solutions to the effects we observe.

Key Recommendations: To accomplish the further maturation of our field, we suggest that researchers who investigate human factors in computer security adopt the concept of theories (see Section 3.6). Furthermore, we recommend that researchers adopt the formal process of design science [124, 178, 285]. While, tech-

nically, some work already follows (parts) of this framework, diligently following it can increase the rigor and reproducibility in our work. This will allow us to build and refine our understanding, and derive and test solutions from this body of understanding in a structured way.

3.5. Research Methods in the Reviewed Papers

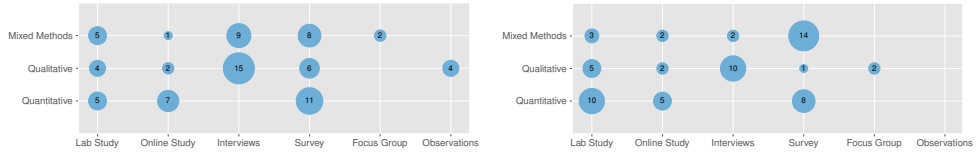
In this section, we analyze the research methods that are used to perform user studies, that is, *which research methods* are used to investigate users? Research methodologies are usually quantitative (statistical evaluation of large datasets), qualitative (extraction of qualitative insights from data not statistically analyzable), or both (mixed methods). According to Creswell [49], a quantitative approach tests theories by developing hypotheses and collecting data to support or refute the hypotheses. This is done using an experimental design and instrument-based data collection (like a survey) followed by a statistical analysis. The qualitative approach, however, seeks to understand the meaning of certain phenomenon from the views of the participants situated in specific contexts. For mixed methods research, both approaches are combined, either sequentially (elaborate the findings of one method with another method), concurrent (merging data from both to provide a comprehensive analysis), or transformative (an overarching theoretical lens within a design using both data types) [49].

The column labeled "Research Method" in Tables 3.2 and 3.3 holds a summary of our findings. We mark studies using a quantitative approaches (◐), those following a qualitative approach (◑), and those using mixed methods (●).

In our sample, we find all three research approaches are being used across six common research tools. However, we notice that quantitative methods are sometimes used for qualitative research and vice-versa, for example, by collecting data for statistic analyses in interviews, or by collecting free-text responses in surveys. We also find that there is no consistency in explicitly mentioning the methodology used to inform the research design and select an appropriate research tool.

For expert users, interviews and surveys are the most used research method, while focus groups and naturalistic observations are least used. Intriguingly, especially naturalistic observations do not suffer from a self-reporting bias, as can usually be found in surveys and interviews [227]. For end users, surveys are the most used method, followed by laboratory studies. While only two studies conducted focus groups, none of the end-user studies in our sample have employed naturalistic observation as a research method.

In our analysis, we find that the expert-user research has a slightly and not significantly higher number of qualitative research compared to mixed methods research and quantitative research (15 mixed methods, 15 quantitative, 18 qualitative) while the end-user research has a high number of quantitative research (17 mixed methods, 18 quantitative, 13 qualitative). The research methods used are also dependent on the identified research objectives (see Section 3.4). Research gathering users' perspectives is mostly qualitative or mixed methods research. Evaluation studies, on the other hand, are mostly quantitative or mixed methods. Studies that test a



(a) Expert Users (b) End Users

Figure 3.10: Overview of research methods in expert-user (3.10a) and end-user papers (3.10b). We find a classical distribution of methods (Surveys more quantitative/mixed methods and Interviews more qualitative/mixed methods). In expert-user related research we find focus groups as a common instrument to generate the foundation of a questionnaire.

hypotheses are almost entirely quantitative, as to be expected. Finally, exploratory studies are mostly qualitative or mixed methods.

Hence, our results are in line with our earlier observations on research objectives. With an emphasis on exploratory and perspective gathering research, qualitative methods are common. Quantitative methods are more prevalent in evaluation studies and hypotheses testing. Where as understanding user perspective or performing exploratory research requires qualitative methods, as they are applicable when studying novel phenomenon or explaining social factors and dynamics.

3.5.1. Observations and Recommendations

Key Observations: At the moment, the choice of research tools is commonly driven by the ultimate goal of a study, instead of being a result of a reflection on these goals. We also find that naturalistic observations, which, as we mentioned earlier, would be instrumental in understanding secure behavior especially in the day-to-day workings of expert users are not commonly used.

Key Recommendations: We suggest that future research considers the trade-off between a study's objective and the available tools more carefully. Especially for exploratory work, researchers should consider naturalistic observations and technical measurements of behavior [65] more closely, instead of relying on interviews and surveys, which potentially suffer from a self-reporting bias.

3.6. Theories in the Reviewed Papers

The use of theories is a common practice in the social sciences. According to Van de Ven [280], theories explain why something is happening by describing and explaining causal relationships. They help us to see the findings of a particular study as special cases of a more general set of relationships, rather than as isolated pieces of empirical knowledge. These relationships can then be tested and revised by others. Gregor [102] claims that a good theory consists of three elements:

1. *Generalization:* Abstraction and generalization from one situation to another are key aspects of any theory
2. *Causality:* Causality is the relation between cause and effect

3. *Explanation and Prediction:* Explanation is closely linked to human understanding, while predictions allow the theory to be tested and used to guide action

In summary, theories (should) explain *why* something happens and from this starting point, can be used for prescriptive or design purposes. Theorizing can bring together different understandings of the problem, thereby ensuring that research contributes to a general class of problems and to a broad variety of organizational and societal settings, instead of a single problem instance. Especially the last step is instrumental to generalize results and provide a scientific foundation.

3.6.1. Theory Use

We investigate if and how human factors researchers in computer security have used theories. In case the authors did not use an established theory, we survey a list of existing theories to identify applicable ones [279], marked with a ○ in the tables. The list of theories was compiled by the Communication Science department at the University of Twente in 2003/2004 for students to better understand theoretical frameworks and aid them in choosing one.

We find 20 papers, seven expert-user papers and thirteen end-user papers that actively use a theory to inform their research, which we mark with ● under the theories section. A further three papers on expert users and nine on end users mention theories in the context of their findings, which we mark with ◑.

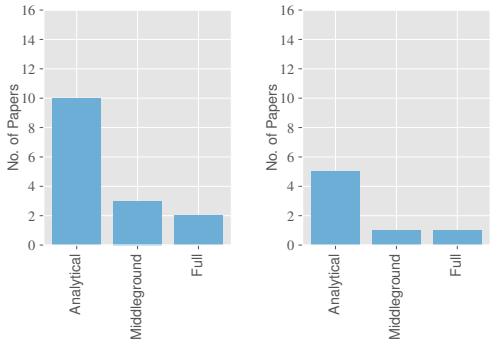
The most commonly used theory is that of mental models, which is being used in six (two expert and four end-user papers) and mentioned in a further three end-user papers. Mental models are used as a tool to study the ways in which users understand and interact with their environments. Furthermore, we find a cluster of three papers focusing on activity theory. Activity Theory is based on the idea that activity is primary [121]. It holds that doing precedes thinking and that goals, images, cognitive models, intentions and abstract notions like "definition" emerge out of people doing things. Apart from these clusters, we find a diverse set of individual theories being used or mentioned in the remaining 26 papers from both samples that use or mention a theory.

We also evaluated the papers to see which theories might have been applicable, based on their research topic. Mental Models are the most commonly applicable theory, applicable to a further 21 papers, ten for expert users and eleven for end users. Sensemaking theory [291] is promising as well, as it would be applicable to 19 expert-user papers, and two more end-user studies. The theory of reasoned action [87] holds promise for two expert-user papers and six end-user papers.

Apart from these three theories, the other theories are only applicable to a limited set of papers, as, for example, activity theory is only applicable to the three papers where it is also being used. There is no one-size-fits-all approach of a set of "best" theories to inform human factors in security research. Instead, we suggest that researchers do not only focus on selecting specific "heavy hitter" theories, but instead refer to a more comprehensive list, such as the one by the University of Twente [279], at the beginning of their research projects.

3.6.2. Grounded Theory

Grounded Theory (GT), first developed by Corbin and Strauss [47], is a structured method to derive a theory from data, instead of utilizing an existing theory. It is a common method for exploratory research, especially in new and emerging fields, and when using qualitative data sources. We surveyed all papers in our sample on their use of GT, independent from their use of other established theories.



(a) Expert Users (b) End Users

Figure 3.11: Overview of how Grounded Theory is being used in expert-user (3.11a) and end-user papers (3.11b). In both samples, the majority of papers claiming to use GT do so analytically, i.e., skip the theory generation step. Note, that GT is far more prominent in explorative research with expert users, but the distribution between papers fully using GT and those only using it for analytical purposes is comparable.

We find that more than twice as many (15 compared to 7) papers investigating expert users, rather than end users, leverage grounded theory. This is in line with our earlier observation that expert studies primarily focus on exploratory research, such as investigating user perspectives on issues or their work environment, or trying to get a first look at a specific issue. These approaches usually rely on qualitative data and, hence, are amenable to a GT-based methodology.

However, when investigating *how* GT is being used in the literature, we find that the majority of papers do not use GT to develop a new theory (see column "GT" under "Theory/Framework"). Instead, most studies (10/15 for experts and 5/7 for end-user studies) reference GT only for the sake of the coding process, including the calculation of Cohen's kappa for inter-rater reliability, and rules for establishing saturation. This means that the authors do not follow the full four-step process for GT (open coding, axial coding, selective coding, theory generation) by omitting the last stage. Instead, these publications provide conclusions around an overview of the discovered codes, often connected to specific quotes from the interviews. This form of incompletely applying grounded theory as a method to present raw data and enrich it with statistical information to seemingly reach a higher level of validity is also known issue in other fields, for example, management sciences [259]. We mark these ○ in the tables.

A further three papers on expert users, and one paper for end-users use a middle-ground approach [241]. Instead of generating their own theory from the collected

data, they utilize an existing theory to explain their findings obtained by the first three steps of GT, or they adapt an existing theory to synthesize their findings. We mark these ◑ in the tables. Ultimately, in our sample, only two papers on expert users and one on end users execute all four steps of GT to contribute to the theory corpus in the field, which we mark ●. In general, these findings align with observations of McDonald et al. [185], who found uncertainty in the HCI community on when and how to use indicators like inter-rater reliability and a tendency to "expect" numeric measures to underline a study's reliability.

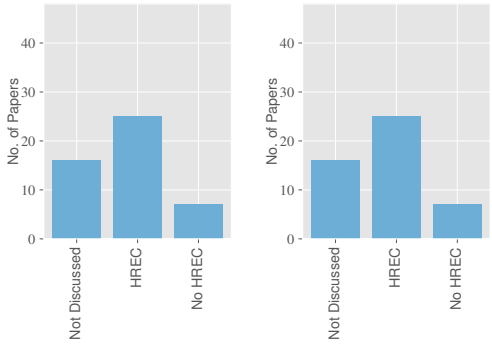
3.6.3. Observations and Recommendations

Key Observations: At the moment, only a quarter of surveyed human factor papers use theories to guide their research design and result interpretation. While mental models are a common tool to inform research design, we find no other theory that is consistently *used* across several papers. Theories that are applicable to a wide range of studies, still go unused (Theory of Reasoned Action, Sensemaking Theory). This lack of theory is, from a scientific perspective, concerning. Other authors, for example Muthukrishna and Henrich [199] see one of the causes for the replication crisis in psychology in an inconsistent and not overarching use of theories in the field. Grounded Theory, a technique for generating new theories from data is commonly claimed to be used, yet authors do not leverage its potential to generate theories. Instead, they focus on the analytical aspects of grounded theory to present their data.

Key Recommendations: To mature from this state, we encourage the field to adopt the concept of using and improving existing theories, as well as forming new ones. As already mentioned in 3.4, theories can help the field to generalize findings in specific situations and use these generalizations to implement and test improvements to the handling of the human factor in IT security. Given the state of the field, we might indeed be already in a situation similar to the replication crisis of psychology [199]. *Grounded Theory*, which can be used for this, is already commonly being used, yet not executed fully. Hence, we recommend authors adopt the full four-step approach of GT and start to formulate theories. Given the emerging nature of the field, theories do not yet have to be refined. Instead, we should start into a process of iteratively testing, validating, and improving findings from earlier work. We recommend as further research more replication studies, as well as studies replicating findings in diverging socio-economical backgrounds (see Section 3.3).

3.7. Ethics in the Reviewed Papers

In this section we assess the implementation of ethical considerations in research involving human subjects. Traditionally, this includes whether the study is ethically justifiable, especially in the context of deception studies and whether participants were exposed to unreasonable harm. However, this point usually also includes whether informed consent was correctly obtained, and the general handling of research data, i.e., whether applicable local privacy laws are followed, and if the authors anonymized the data as soon as feasible during the research project.



(a) Expert Users (b) End Users

Figure 3.12: Overview of how ethical considerations are handled in expert-user (3.12a) and end-user papers (3.12b). We find that the share of papers not discussing ethical implications of their work (informed consent, handling of data etc.) is higher for the expert-user portion of our dataset. Similarly, the number of papers where no suitable HREC was available is higher in the expert-user sample.

Hence, for each paper we identify whether ethical considerations were properly discussed *and* the study has been submitted to an ethics review board[2] for approval (●), whether the authors evaluate the ethics of their research themselves and discuss their review in the paper (◑), or if ethics are not discussed in the publication (○).

Even in 2018, individual publications still do not involve an ethics committee, but the general trend is towards a thorough consideration of ethical requirements. Despite this positive trend, it appears that papers investigating expert users initially discussed the ethics of their work less consistently. A common issue, leading to authors not involving an ethics committee, are cases where the authors' ethics committee is not sufficiently equipped to deal with the specific research plan. A classical case of this is the 2015 study of Burnett and Feamster [37], which measures censorship, but does so raising ethical concerns [202]. However, the ethics committee of the researchers' institution signed off on this work, most likely due to the board being unfamiliar with the ethical implications of research at the intersection of human factors and computer science. Other studies, for example, Dietrich et al. [70], did not involve an ethics committee because their host institutions does not have such an entity.

3.7.1. Observations and Recommendations

Key Observations: While the field made significant progress in the inclusion of ethical considerations, some institutions still lack the appropriate research infrastructure. Furthermore, especially for expert-user related work, authors even in 2018, still do not always discuss their work's ethical implications.

[2]We call this HREC (Human Research Ethics Committee). A common, yet US centric implementation is the well-known Institutional Review Board (IRB)

Key Recommendations: Authors should adopt the habit of evaluating the ethical implications of their work. In case no ethics board is available, the Menlo report can provide guidance on how to evaluate the ethical implications of one's work [71]. When considered for publication, authors should be held to these standards, that is, documenting their efforts in handling ethical implications and subjects data rights should be mandatory. Furthermore, we suggest to address the issue of no capable ethics board being available by introducing a community driven ethics board, capable of reviewing human factors in security studies, for example, by the IEEE and ACM extending their existing bodies.

3.8. Limitations

Our literature survey has several limitations. Firstly, we do not take into account the research before 2008. While a historical perspective going back to the earliest papers nearly 30 years ago might prove useful to understand the origins of the field, a more recent scope is better suited to provide an overview of the state of the art and comprehensive recommendations on how the field can improve further today.

Secondly, instead of searching the standard databases like SCOPUS or Web of Science using particular keywords to find relevant publications, we chose to search all the top-tier computer security venues. We didn't use any keywords for search but included all the publications from the top-tier venues after 2008. We made this choice so as to showcase the work of top-tier computer security venues in regards to human factor research. We understand that this may exclude notable human factors research from outside these top-tier computer venues but we consider those out of scope as we want to learn what the leading security venues are doing.

Thirdly, after an in-depth review of the 48 expert user publications, we were interested in comparing these publications with the end-user publications. Therefore, in order to have a reasonable number of papers to review, we opted for balancing the two user groups. For this, we used a random sample of 48 papers from the end-user group. These papers were chosen so as to match the number of expert user papers per year. We understand that this is a random selection but we believe it serves our purpose in answering our research question. While we do not review all the end-user papers, we review enough to gather the overall gist of end-user research and to be able to provide an overview of the research in both user groups.

Overall, we systematize a significantly larger body of literature than related surveys, for example, Hamm et al., who cover three conferences over five years [114], or Tahei and Vaniea, who focus only on developers [263].

3.9. Conclusion

This chapter presented the systematization of how research of the past ten years in the emerging field of human factors in computer security is conducted, with a special focus on expert versus non-expert users. Although the field is growing, we find that there is an opportunity for the community to adopt methods, rigor, and practices from other fields in which human factors research has matured over the past years. Most notably, we can learn from safety science in terms of how we treat

the human factor, and the social sciences in terms of utilizing theories to streamline our research work, and their experience in the ongoing struggle with WEIRD study populations, which we share.

Moreover, we find that expert users are under-represented in human factors research. Only around 9% of all papers have focused on this group, even though their choices and mistakes typically have more impact than those of regular end users. For the critical population of expert users, our field can benefit from safety science's perspective on human error (see Section 3.2). In this field, human error is a "normal" probabilistic outcome of a set of organizational and institutional conditions under which users interact with the technology, rather than the failure of an individual. Systems have to be build in a way that handles and accounts for the occurrence of these errors. "Fixing the (expert) user" is not the path to better security and privacy [73].

In terms of methodology, population selection and recruitment we find that currently most work is biased towards samples that are locally accessible to researchers. This means that current work is heavily dominated by a U.S. and Europe-centric view (see 3.3). This current focus of samples may lead to a biased perspective of the work we do, only focusing on the needs, expectations, and behavior of citizens of the global north. In the pursuit of diversifying the populations that our field studies, for example, utilizing Cultural Dimensions Theory might prove useful. Similarly, Design Science is a promising framework to formalize the process of designing and evaluating an artifact, that is, starting with requirements gathering from a population, designing it while considering best practices from the literature, and properly evaluating the final artifact.

At the moment human factors research in computer security is still dominated by exploratory and perspective-gathering research (see Section 3.4). Hence, to further advance the field, we suggest to adopt the concept of theorizing from the social sciences and psychology (see Section 3.6). Only a fraction of the published work leverages theories (see Section 3.6.1), even though many of these studies could have benefited from including theories, like Mental Models, Sensemaking Theory or the Theory of Reasoned Action.

Current use of theories is either observational, that is, to improve experimental design in case of Mental Models, or fragmented, not consistently focusing on a specific set of theories. While several recent publications claim to utilize Grounded Theory, we find that work typically does not execute the full process of Grounded Theory, which should culminate in true theorizing. Instead, it is used as an analytical framework to formalize experimental design and the qualitative data analysis process authors conduct (see Section 3.6.2).

Future Work

Considering our research question and sub questions, we can make the following recommendations for future research. Firstly, in addition to preventing human error, we should also try to understand which behavior leads to secure outcomes, and how we can facilitate that behavior. For this, we recommend investigating expert users and their interactions with their environment from different qualitative per-

spectives. On top of interviews and surveys, we recommend employing different research methods (e.g. naturalistic observations) to study human factors. Secondly, we recommend investigating more diverse population samples and also better discussing the external validity and limitations of the findings with regards to the samples studied. Thirdly, we recommend exploring and using existing theoretical frameworks to inform the research design. Fourthly, we suggest using and improving upon existing theories as well as forming new ones. This will help in generalizing the results. We also recommend more replication studies, specially replicating findings in different socio-economic backgrounds. Lastly, we suggest that researchers should try to evaluate the ethical considerations of their work in human factors research. We also suggest the possibility of creating a community-driven ethics board which can help researchers that do not have an ethics committee available to them.

Our literature review has has several limitations, as discussed earlier. We do not claim to have represented the totality of several decades of human factors research, assuming that would even be possible. We do claim to provide a thorough overview of the research on experts in the past decade and a representative view on work on non-expert user populations for the purpose of making a comparison. We suggest extending the scope of the review by diving deeper into various user categories to gather specific insights and by investigating other security venues that were excluded in this study.

Over the past decade, human factors research has been increasingly recognized as a key contribution to the field of computer security. Now, it is time to learn from its own successes and failures as well as observations and experiences from other fields to further mature it. In the following chapter, we present an interview study where we applied the lessons we learnt from our extensive literature review. We did so by centering the perspectives of sysadmins to understand their work experiences in the context of day-to-day operations. We informed our study by coordination theory and used a theoretical framework to formalize sysadmins' coordination during the COVID-19 crisis.

4

System Administration during COVID-19

This chapter is based on an article published as: Mannat Kaur, Simon Parkin, Marijn Janssen, and Tobias Fiebig. 2022. "I needed to solve their overwhelmness": How System Administration Work was Affected by COVID-19. In Proceedings of the ACM on Human-Computer Interaction 6, CSCW2, Article 390 (November 2022), 30 pages. [147].

In Chapter 3 we presented an extensive literature review to understand the state of knowledge of human factors research in the computer security domain. The research gaps and future research directions for future work are presented in Section 3.9. One of the main gaps we found was that expert users, such as system administrators (sysadmins), are an understudied population despite their crucial role with regard to computer security. After examining 14 computer security conference venues (proceedings from 2008 – 2018), we identified 557 papers with user studies. These papers included only 48 expert user studies out of which a mere 7 studies were pertaining to system administrators.

To begin to address this scientific knowledge gap, in this study we dive deeper into system administration work. During the time of this study (July – December 2020), the global COVID-19 pandemic was ongoing and presented a unique opportunity to investigate system administrators' work during a crisis situation. When the World Health Organization declared the COVID-19 outbreak as a pandemic on 11th March 2020 [299], many countries – if they had not already begun to do so – imposed various forms of lockdown to reduce the virus' spread. These measures, depending on the country, were in place for several months, and – after being lifted – often were followed by further similar measures in subsequent waves. Essentially, since March 2020, the world finds itself in a situation that transformed working from home from an optional feature leveraged by a minority of office workers, to the quasi standard where possible. Hence, the *way* office workers conducted their work had to be adapted in a similarly swift manner as well. In turn, the IT infrastructure used to work remotely had to keep pace with, and anticipate, these changes.

While the onset of COVID-19 was a disruptive event for everyone, we investigate how this challenge affected system administrators in their work. We focus on sysadmins, as these knowledge workers are generally those *running* and *adapting* digital infrastructure for users and customers. Within their duties, sysadmins configure firewalls, set up network connections, and install operating systems and software on servers and client machines, such as laptops needed by employees to work from home. Sysadmins often also provide support to users directly by, for instance, acting as an additional technical support desk.

When working from home became the new default, sysadmins not only faced changes to their own way of working—as many did—but they also had to ensure that the IT infrastructure they manage was adapted to enable users to cope with working from home. This included providing laptops for users who had previously used fixed workstations, and configuring phone lines and VPNs (Virtual Private Networks) and making them accessible to users. Perhaps most prominently, video communications tools were rolled out within countless organizations.

In this chapter we investigate: **How did system administrators' work change due to the lockdowns imposed in response to the COVID-19 crisis?** Our investigation includes how sysadmins saw their work fundamentally changing as a consequence of the crisis, and how they responded to the immediate challenges of keeping infrastructure running under those changing circumstances. Our goal is understanding how sysadmins' tasks and coordination with others changed when reacting to this crisis. This will allow us to identify which of the changes in the

way they work point to adaptations worth keeping, and which lessons we can learn to be more prepared for future crises. To this end, we conducted semi-structured interviews with a globally diverse sample of 24 system administrators, which we analyzed using thematic analysis [33].

We found that sysadmins faced a two-sided crisis (Section 4.3): While sysadmins' own work environment changed and they had to react to the new situation and facilitate stable options to work online for themselves (Section 4.3.1), they also had to do so for their colleagues and support their users in adapting to the crisis (Section 4.3.2). This finding embeds into earlier work (Section 4.4) on the connection between IT (security) work and the notion of 'care', where we substantiate these earlier findings with results from a repeatable method grounded in coordination theory (Section 4.3.3). Furthermore, while we found that sysadmins perceived no major changes in the way they work, a deeper investigation revealed that they did experience several counter-intuitive effects on their work. This included that while day-to-day communication became inherently more difficult, other tasks were streamlined by the remote working format and were seen as having become easier. Finally, by structuring our results according to a model of coordination and communication (Section 4.5.1), we identified changes in sysadmins' coordination patterns, from which we derived recommendations (Section 4.5.2) for how system administration work can be coordinated, ranging beyond the immediate pandemic response and the transition to any 'new normal' way of working.

This study makes the following contributions:

1. Our study is the first to address how COVID-19 uniquely impacted the ability of sysadmins to adjust their own practices through this unprecedented crisis, while also enabling the work of others. We apply a coordination and communication model for response and replanning [44], providing evidence of the connection between IT (security) work and notions of care and responsibility [156], notably within a time of crisis and turbulence;

2. By rooting our investigation in crisis management and coordination literature, we create an empirical lens that expands beyond the (intuitive) effects of lockdowns related to COVID-19, as identified in the literature. Though similar lockdown-related effects also manifest in the work of sysadmins, sysadmins also exhibit effects not found in other populations of employees, due to the nature of their roles. This includes additional costs to existing tasks due to increased effort in coordinating their actions with others;

3. We outline coordination of various sysadmin tasks and their adaptations in the circumstances of the COVID-19 pandemic as a large-scale disruptive event. These adaptations include a shift from trust-based informal procedures to assurance-driven formal processes, as a means to maintain predictability and stability in the view of external parties. With attention to how these additional coordination costs are borne by sysadmins themselves, we identify potential benefits of carefully applied and organically developed formalizations, as detailed in our recommendations.

The remainder of the chapter is arranged as follows: We first introduce background literature on sysadmins' work, coordination, and existing frameworks for handling crisis situations in Section 4.1. Informed by existing approaches, we next present our methodology in Section 4.2, where we also detail our analysis approach and ethical considerations. We then present the results of our analysis in Section 4.3, going on to frame our study alongside related work (Section 4.4), before a discussion of the implications of our results (Section 4.5); this includes lessons learned and subsequent steps for both addressing challenges and leveraging opportunities in sysadmins' work. Finally, we conclude and discuss future work in Section 4.6.

4.1. Background

Here we describe system administration work during a crisis situation and introduce the model of coordination and communication for distributed anomaly response.

4.1.1. System Administration in a Crisis

As discussed earlier in Chapter 1, system administration is the crucial task of designing, operating and maintain IT systems. Those who use their "technical, social, and organizational skills to architect, configure, administer, and maintain computer systems, including operating systems, networks, security systems, infrastructure, databases, web servers, and application" are known as system administrators (or sysadmins) [18].

In addition to the technical IT duties, system administration work also requires coordination with their colleagues and the users they support. In a crisis, sysadmins must facilitate other employees' adaptations by adapting the IT systems available to them. In doing so, they not only have to *adjust* their work to the crisis like everyone else, but at the same time act to *mitigate* the impact of the crisis on others through that work. The ability of sysadmins to adapt to a crisis then has a cascading effect on other workers' ability to adapt.

If there is a sudden *shift* in *how* people conduct IT-enabled work—as seen with the myriad work-from-home orders during the COVID-19 related lockdowns—peoples' technological needs change. Countless users who used to work on desktop machines may now use laptops. Remote workers will need increased capacity for Virtual Private Network (VPN) access to company resources [25]. A policy and support framework may be necessary to enable Bring-Your-Own-Device (BYOD) practices.

In light of these considerations, we regard sysadmins not only with reference to their specific tasks and activities, but also their role in providing and maintaining digital infrastructure *used* and *needed* by others.

4.1.2. Modelling Coordination in a Crisis

Within an organizational context, we refer to a crisis—such as the emergence of the COVID-19 pandemic—as *"an event perceived by managers and stakeholders as highly salient, unexpected, and potentially disruptive"* [35, p. 1662]. Under disruptive conditions, coordination is essential for an appropriate response to an adverse

event, with insufficient coordination often being cited as a major contributor to unsuccessful crisis response [27].

To navigate the complex space of system administration work during the unprecedented COVID-19 pandemic and associated lockdown measures, we utilize the model of communication and coordination for distributed anomaly response and replanning created and applied by Chow et al. [44]. This model is also called the co-ladder model, because of its shape of (multiple) ladders placed next to each other, see Figure 4.2. We regard an anomaly in planning as an event that is both *abnormal* and *unexpected* [101]. In Chow et al.'s model, distributed work refers to *"multiple human agents who must coordinate across functions, time and physical distance to achieve their shared high-level goals"* [44, p. 1].

The co-ladder model was derived from several studies of human-to-human coordination in a complex, high-performance environment of space mission control. Specifically, the model was created to help find communication patterns and coordination processes among practitioners working in complex domains in a distributed way. The model was used to analyze anomalous activities in technical systems during critical missions, specifically leaks from hydraulic systems used for space shuttle missions. Of pivotal importance is that the model also considered how system anomalies were managed by flight controllers and engineers. Members of the operations team were represented as one agent in the model, and the members of the engineering team as another. Chow et al.'s model can accommodate individual human agents, teams that act as one agent, and interactions among agents at both an inter- and intra-organizational level. The model has also been applied to assess coordination between distributed agents in the lead up to an airplane incident [144]. In this case, agents needed to work together to ensure continuous flight operations.

We select the co-ladder model as it provides a task level perspective on coordination, and the objective for which the model was designed aligns with the objective of our study of sysadmins. In the above cases, processes must be maintained in a complex and distributed technical environment, to ensure continuous and secure use of provisioned systems by employees. Further to this, system operations must be maintained—as phrased by Chow et al. for their use case as well—*"while modifying plans in action in the face of time pressure, uncertainty, high consequences of failure and multiple interacting goals"* [44, p. 1].

We chose the co-ladder model for our analysis as opposed to the 4-phase model by Boin and Bynander [27] or the theoretical coordination framework by Christensen and Ma [45]. We did not select the 4-phase model by Boin and Bynander as it has been created to explain the effectiveness of collaboration in the aftermath of a temporarily limited disaster–for example a major accident or plane crash–and how this is impacted by formal authorities. Similarly, the theoretical coordination framework by Christensen and Ma examines coordination from vertical dimensions (that refer to the labor division across intra- and inter-organizational perspectives) and horizontal dimensions (referring to the linking and de-coupling between different issues and policy areas). We consider this to be too broad for analyzing sysadmins' coordination in response to the COVID-19 pandemic. The Chow et al. model allows us to examine crisis response and coordination from the standpoint of individual actors

rather than a higher-level organizational perspective. Other models as, for example, that by Wolbers et al. [301], usually deal with concrete fast-response emergency scenarios (similar to the model of Boin and Bynander [27]), and as such are not as suitable for analyzing a repeating or long-term crisis such as the ongoing COVID-19 pandemic, for which we collected retrospective reflective data from sysadmins in interviews.

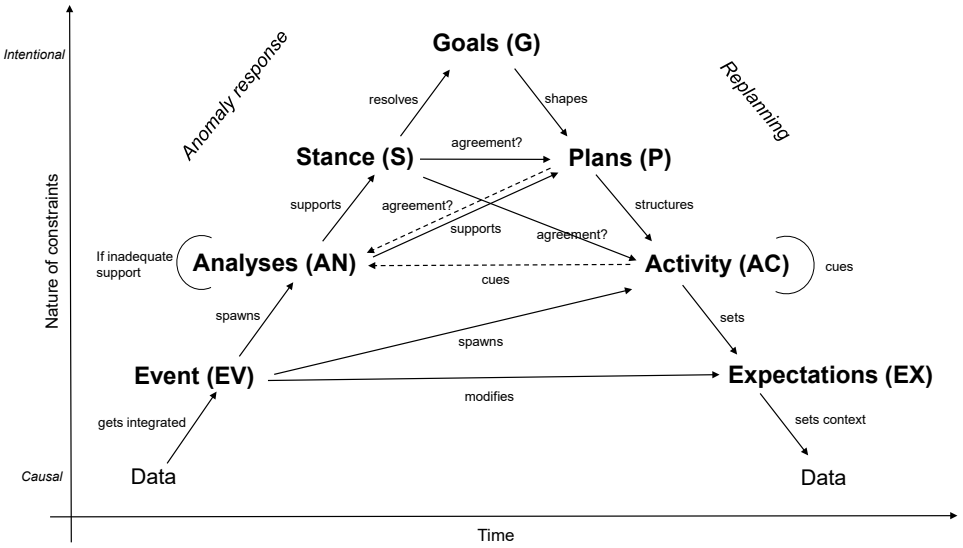


Figure 4.1: Model of coordination and communication for distributed anomaly response and replanning (Co-Ladder Model), reproduced from Chow et al. [44].

We provide an overview of the Chow et al. model in Figure 4.1. From this point on, we refer to the model as the 'co-ladder model' for convenience. The co-ladder model consists of information types (represented as "nodes") and transitions between these (represented as "links"). The different information types are: i) Data: observable data values that suggest an abnormal occurrence; ii) Event (EV): the operator integrates the observed data and recognizes it as an anomalous event; iii) Analysis (AN): once identified, the event will lead to a diagnostic and evaluation phase; iv) Stance (S): the result of the analyses will develop or modify the team's agreed-upon rationale; v) Goals (G): high-level objectives held by all members of the team; vi) Plans (P): goals shape actionable plans; vii) Activities (AC): plans structure individual tasks and activities which the practitioners coordinate to perform; viii) Expectations (EX): activities performed and the awareness of these activities among team members set expectations. These expectations need to be monitored against the observable data.

The left side of the model is driven by data, and focused on anomaly response. The right side of the model is goal-driven and informs replanning. The processing of various information types can be influenced by causal constraints (facts and constraints of the system) and/or intentional constraints (of the human practitioner making choices), as seen along the y-axis. The different coordination processes take place over time, as seen along the x-axis. In addition to the linear transitions explained above, the anomaly response (left) and replanning (right) nodes can influence each other. Walking through the common path of the model, an event is identified when the data does not meet the expectation, which is detected as an anomalous event. Detection of an event will alter the expectations towards observed data, spawn activities and trigger analyses to determine the cause of the event. Depending on the results of an analysis, the stance may change, resolving to changes or creation of a goal. Based on a goal, a plan is crafted, which results in activities that may raise an expectation with regard to the outcome of the activity, ideally the resolution of the issue. During the resolution phase, there is interaction between analyses and the stance, thereby affecting the current resolution plan and resolution activities. Figure 4.1 visualizes how an activity triggers analysis as an arrow against the unidirectional time arrow (x-axis).

When applied, e.g., as by Chow et al. [44] to anomaly response in space missions, the model expands to the right, with an activity node receiving a new arrow towards the analysis node of a *new* ladder towards its right instead of creating a loop in a single ladder. Figure 4.2 illustrates how an example process might be represented using the model. We consider a simple example, specifically of users reporting degraded performance on VPN connections into the company, and monitoring indications of a reduction in average bandwidth per VPN user. This would represent unexpected data values. For the sysadmin(s), this data indicates an issues with the VPN service and will be identified as an event (EV). This event (EV) may trigger new activities (AC), such as contacting users for more information, and checking the utilization of the VPN gateways. The activities (AC) then cue an analysis (AN) phase, where the sysadmin will evaluate what the problem is and how it can be solved, potentially through discussions with other sysadmins. During this analysis, the sysadmins may realize that the number of users currently active on the system exceeds its capacity. This analysis (AN) leads to an updated plan (P) – most likely deploying additional VPN gateways or upgrading the current one – while the overall goal (G) of providing a sufficient service to their users does not change. The new plan (P) restructures the activities (AC) to be performed, such as buying and deploying a new VPN gateway, and also modifies future expectations (EX) regarding how the system should function, i.e., which load patterns should be observed on the VPN gateway(s) with the current number of users.

In the next section, we detail adaptations to the co-ladder model, to facilitate qualitative research with sysadmins holding active roles in a variety of organizations, in the period immediately after the enactment of work-from-home mandates as a response to COVID-19.

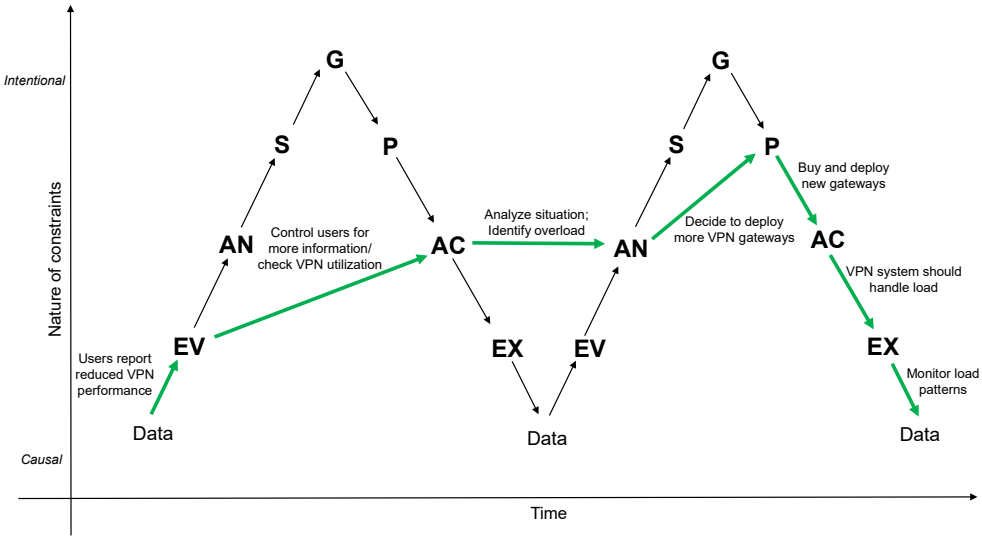


Figure 4.2: Example illustration of a coordination process where sysadmins address reduced VPN performance. An event (EV) triggers new activities (AC) which then cue an analysis phase (AN). This leads to an updated plan (P) which restructures the activities (AC) and also modifies future expectations (EX).

4.2. Methodology

In this section we describe our research methodology, including preliminary work conducted with our target population and approach for creating the interview script.

4.2.1. Modelling Coordination Within System Administration

The Chow et al. / 'co-ladder' model [44], and other studies based on it, have up to now used log entries and transcripts to analyze coordination. This provides structured data relating to explicit communication, whereas the reasoning behind the communication and coordination, and with this the role of implicit coordination, are not known. We seek to capture aspects of both explicit and implicit coordination. Collection of data logs would be unreliable, as sysadmins are creating new processes in conditions of crisis, for which there may not yet be logs. We instead rely on qualitative data collection, informed by in-situ observation (Section 4.2.2). We structured the engagements accordingly, as described in Section 4.2.3.

Using this model enriches our qualitative analysis as it helps to identify the coordination and communication processes underlying system administrators' work in a structured way during complex and unusual operational situations, such as

in COVID-19 lockdown conditions. This way, we can develop a comprehensive description of sysadmins' coordination, have a starting point for formalizing this human-human coordination, provide the capability of prediction of similar coordination in the future, and finally, add to the existing body of knowledge regarding human-centered design recommendations for sysadmins' tools.

4.2.2. Pre-Study

In early 2020, before COVID-19 emerged as a global crisis, the PhD researcher began an observational study in a team of six Linux administrators, similar to the work of Barrett et al. [18]. In total, they spent 30 hours over 20 days with the team. The aim of this process was to develop a practical understanding of day-to-day system administration work, in terms of explicit (observable) coordination, using naturalistic observations and informal discussions with the team. With the introduction of COVID-19 countermeasures, the objective of the study shifted to understanding the impact of the lockdown measures in sysadmins' work, while also switching the methodology to an interview-based one; the latter was necessary as the host institution introduced a policy prohibiting in-situ data collection for human studies. This pre-study enabled us to prepare for engagement with sysadmins' work in interviews and also highlighted the importance of coordination in sysadmins' work, underlining the necessity to utilize a coordination-focused framework for analyzing interview data.

4.2.3. Interview Protocol

For the interview questions, our main focus is on the day-to-day tasks of sysadmins, following our description in Section 4.1.1. Given the diverse nature of system administration work, we utilize a similarly broad interview protocol within a semi-structured interview structure, flexible enough to accommodate this diversity of topics. Within this structure, we employed follow-up probes based on our experience from the earlier naturalistic observations and the co-ladder model, to further investigate participants' responses regarding coordination.

In line with the co-ladder model, which captures the impact of events on tasks (or activities, as in the model), questions first build a base understanding of sysadmins' tasks before the first lockdown, during the first weeks of the lockdown, and 'now', i.e., in late 2020 when the data collection took place. These are questions 1-3 in Appendix A. Note that we consider the lockdown to begin in mid-March 2020 in the sample script. In the beginning, lockdown measures differed widely across the world; we asked each participant when the first lockdown began for them, and then framed the questions accordingly.

Where the co-ladder model emphasises those changes to tasks requiring coordination, we ask participants about changes they experienced regarding their tasks, carefully probing for the triggers of those changes (such as events, stance, or plan changes, as in Section 4.1.2). Here it is important to relate to the terminology used by participants [5], and rather than introduce these terms from the co-ladder model, instead be careful not to introduce the researchers' terms into the interviews themselves [159]. Finally, we ask participants whether they perceived an impact of

the task changes they have discussed specifically in relation to the security of the systems they manage. Security is not only an aspect of system administration work, but can emerge as an imperative which must be balanced with other priorities, although for sysadmins it is part of the goal of their work. This then opens up the possibility to discuss the coordination of potential goal-changes and their impact on tasks with participants.

The interviews took place as 1-on-1 sessions over a period of four months, between 31st July 2020 and 2nd December 2020, and lasted an average of 48 minutes. We used our university's self-hosted video communications platform for this purpose, which also created recordings as indicated in the consent form. While we did not analyze visual cues, we did activate cameras depending on the participants' individual preferences (where accommodating a naturalistic setting is important [5]). Prior to working through the interview questions we collected general demographic information to validate our participants' employment as sysadmins: the job title, years of experience, job location (country), type and size of the organization, and the educational background of the participants.

4.2.4. Ethics

This research project was approved by TU Delft's Human Research Ethics Council (HREC) under ID number 1215. In this process, the HREC audited our data management plan and data storage procedures, and compliance with applicable privacy legislation. They furthermore verified that we only collect aggregate data, i.e., that we delete all PII (names, places of work, etc.) during the transcription process. The HREC also audited the informed consent forms we used for our study, with which we collect participants' consent for the interviews (alongside oral consent before proceeding) and inform them about the study and their subject data rights. The HREC also required in-person human research activities to move online in response to local lockdown mandates, hence our shift in research circumstances between the pre-study and main set of interviews described here.

4.2.5. Recruitment and Participants

We recruited participants via our personal networks as convenience sampling, given that our target population is an instance of 'poor reachability' of highly experienced and busy professionals, a challenge also noted by Reinfelder et al. [232] and Dietrich et al. [70]. Additionally, we recruited via social media posts (Twitter, LinkedIn) to attract self-described sysadmins. See Figure A.1 in the Appendix for the flyer we used for this purpose. No compensation was offered to participants given the nature of the target population, in line with findings by Dietrich et al. [70]. In total, we recruited 22 participants for interviews, see Table 4.1.

We received a written response to the interview script from a further two sysadmins, who were unable to allocate a fixed time for an interview, P23a and P24a. While written responses are not ideal, as they do not allow us to apply our probing-based approach, these responses still add qualitative perspectives, hence why we consider them as *additional* input to our dataset.

ID	Sector	Experience	Location	ID	Sector	Experience	Location
P1	IT	2 years	Netherlands	P13	Telecom	7 months	Ireland
P2	Education	10 years	Italy	P14	Education	8 years	Netherlands
P3	Education	22 years	Netherlands	P15	Education	10 years	Netherlands
P4	Education	24 years	Netherlands	P16	IT	10 years	India
P5	Healthcare	19 years	Norway	P17	Education	9 years	United States
P6	IT	10 years	Netherlands	P18	NGO	6 years	Norway
P7	Research	25 years	Germany	P19	IT	5 years	Ghana
P8	IT	7 years	Germany	P20	Finance	8 years	Sweden
P9	IT	20 years	Netherlands	P21	Finance	6 years	India
P10	Research	20 years	Austria	P22	IT	18 years	UK
P11	Education	5 years	Netherlands	P23a	Manufacturing	16 years	Germany
P12	Education	10 years	Austria	P24a	IT	4 years	Canada

Table 4.1: Overview of participants' working location, work experience, and their employers business sector.

Work experience of our participants ranges from entry-level employees with less than a year (7 months) of experience, up to senior operators with up to 25 years of experience in the industry. Furthermore, we were able to recruit participants from organizations who have their core business in IT services, as well as organizations that focus on other sectors, e.g., research, healthcare, manufacturing, and finance. Recruiting from a diverse set of organizations is crucial for our qualitative sample, as organizational factors may influence the work of sysadmins based on their sector, as discussed by Dietrich et al. [70]. We do not list our participants' specific job titles. We found, in line with existing understanding in Section 4.1, that sysadmins' job descriptions are highly diverse, up to the point that they might make the specific employer or even specific participant identifiable. Nevertheless, we were able to relate roles and responsibilities in line with our definition of a sysadmin as in Section 4.1, and further consider roles during our result analysis.

4.2.6. Data Analysis

Due to the qualitative and explorative nature of our work, we chose the inductive, reflexive thematic analysis (TA) approach described by Braun and Clarke for our data analysis [33]. Note that *"data are not coded in an epistemological vacuum"* [31, p. 84], and we inform our work with existing theory (Section 4.1) to place our work within the existing research in the field (Section 4.5). TA is a recursive process that consists of six phases: *"1) data familiarisation; 2) systematic data coding; 3) generating initial themes from coded and collated data; 4) developing and reviewing themes; 5) refining, defining and naming themes; and 6) writing the report."* [33,

p. 4]. Again, given the exploratory nature of our work, and following the recommendations of Braun and Clarke on the number of codes for the application of TA [31], the PhD researcher acted as coder and conducted this activity using Atlas.TI. Furthermore, instead of using multiple coders, we opted to involve regular codebook discussions at intervals, including all authors, in the coding process, in order to discuss and refine the codes and ensure the reliability of the process. Given the recommendations of Braun and Clarke, and the feedback loop between researchers during our coding process, we consider this method sufficient to capture the richness of the phenomenon under observation; see also McDonald et al. [185]. In total we developed 93 codes split over four main themes and 15 subgroups, as in Table A.1.

4.3. Findings

In this section, we first discuss what our sysadmin participants report doing as their work (Section 4.3.1 and 'Sysadmin Tasks' in Appendix A.4, Table A.1) – leading to tasks in activities they have to perform for their jobs, associated responsibilities, and underlying goals. In Section 4.3.2, we detail lockdown-induced changes on sysadmins' tasks and responsibilities, and how these changes highlight the work of sysadmins' to support others. This covers 'Sysadmin Tasks', 'Social Interactions', and 'Lockdown Effects' from Table A.1. In Section 4.3.3, the lockdown-induced changes on sysadmins' coordination activities are presented, drawing from 'Lockdown Effects' and 'Social Interactions' in Table A.1, while also contextualizing the need for these changes under the premise of 'Security'.

4.3.1. Sysadmins' Tasks and Responsibilities

Our participants' reported tasks and responsibilities broadly in line with our initial description of what sysadmins do (Section 4.1.1), which is, as P9, put it, *"keeping all systems running and expanding them"*.

Participants variously reported performing maintenance tasks such as updating servers, software development, rolling out new services, deploying new tools, and ensuring that deployed IT systems conform to the requirements set for them. Twelve participants highlighted the 'problem-solving' aspect of their work, including addressing operational issues but also supporting others with their IT-related problems. The role of automation in these tasks was also mentioned, allowing teams to *"do better with the people we have"* (P5), and enable smaller teams to *"operate at scale"* (P20).

Many of our participants reported working in a fast-paced environment, with six participants noting that their tasks can change daily as *"it all comes down to whatever happens during the day"* (P24a). For example, Participant P5 described the role that system users have as a regular influence:

> *"[Users] have one short question and an hour later or something you are still trying to explain something to them and why they should be talking to the person in the next office and not you."* (P5)

Participant P16 noted that unplanned work is driven top-down *"usually when something's missing, somebody else has a deadline and yeah it needs something*

from my side of work that usually comes in at the last minute. [...] It's almost always, yeah, "we need this now!", where this can refer to *"infrastructure that's not working properly."* (P8). Seven participants reported working out of business hours to address unplanned work when something *"had to be fixed"* (P7).

Regarding the work itself, four participants touched upon a difference between how the work was expected to be done, as compared to how it was put into practice. Participant P14 recalled being asked to perform regular server updates by the IT department, but that the servers in question were *"not updated for years and also had other security issues"* (P14), or Participant P5 who shared that *"if you read our SLA agreements, [...] there's definitely a difference between practice and what is written there"* (P5). These occurrences are akin to the 'oscillations' between secure and non-secure states, reported by Kocksch et al. [156], in which system administrators would also need to 'tinker' with systems to not only fix them, but also understand how they work in order to know what can be done to fix a security-related problem or request.

Regarding work prioritization, participants reported different ways of going about this. Mostly, participants would decide for themselves what to prioritize based on their experience. Otherwise, prioritization was based on manager requests, deadlines or tasks that are perceived as urgent, such as responding to incidents.

While technical aspects of participants' work seem to be dominant, more social responsibilities are also mentioned, such as supporting people who needed immediate help for non-IT, yet 'technical', issues. Essentially, sysadmins seem to be seen as 'fixers', solving a variety of issues, or as Participant P7 explains:

> *"I have to make sure that the scientists can work.. whatever it costs. So, if I would be on site and the toilet would break, that also would be one of my tasks."* (P7)

Supporting others, such as users and colleagues, is consistently mentioned by the participants. Communication with users then also emerges as a general central theme in sysadmins' work. Providing regular support to users is so pivotal to system administration that at times this can mean that users develop a reliance on the sysadmins, sometimes even to the extent of needing their support *"for pressing a button on a printer" (P12)*. From another view users then rely on sysadmins to tell them *"how they can continue to work"* (P7). This can include when users have to be informed about any upcoming maintenance work that might affect them. This supportive nature of system administration work can nonetheless mean that the job of system administration is *"quite [an] invisible one"* (P12). Limoncelli et al. [170] have highlighted the distinction between perception (how people see you) and visibility (how much people see you), as a particular aspect of system administration work; in essence, if system operations are functioning as expected, people do not realize how much effort goes into that work and therefore sysadmins remain mostly invisible. This is put into context by P12, who describes *"[being] kind of excluded from social things [...] but we're always getting the contact when someone needs something."* (P12).

In addition to their interactions with users, sysadmins also interact with their colleagues, and supporting colleagues is a major part of daily tasks:

> *"if you are not very careful with your time, you can go a whole week without having anything to account for because you are spending your time trying to help other team members."* (P19)

While, with users, there is a mix between coordination and support, interaction with colleagues is usually coordination-driven. In line with Barret et al. [18] who find their sample to spend 23% of their time in meetings, we observe that our participants report spending a significant amount of time in meetings or coordinating for meetings. Examples of interactions with colleagues include *"meetings with developers about deploying their application"* (P1), coordinating with other departments about platform updates (P7), talking to new customers to *"see if we can build a system for them that they need or migrate to us"* (P9), team meetings about ongoing projects (P11) or *"planning ahead for the next three years"* (P18). Furthermore, four participants mention meetings and formal coordination that is necessary in conjunction with suppliers of hardware and software components in order to, for example, obtain *"quotes from suppliers because someone wants to order a new server"* (P3) or work together *"side by side"* (P11) for deploying new high-performance computing (HPC) clusters.

We find opposing perspectives on the effect of social interactions on the work itself, where eight participants said that socializing does affect the work. This effect can, for example, be positive when in *"an open landscape, it's much easier to sort of like hear if somebody is [...] struggling with something and then you're sort of like... aye! Yea!ht I might have a solution for that problem."* (P5). The effect can also be negative, in the form of work interruptions (coffee breaks (P8), or people asking *"dumb questions"* (P7)), which can make it difficult to concentrate. This is comparable to the group dynamics of 'tech caregivers', where many topics may be discussed between peers, and security is one of those, serving as an opportunity to offer advice [161]. Six participants felt that social interactions do not affect work, for example P9 said that *"we do miss the social interaction with all the guys. We miss that. But work-related, customer-related, task-related, those things just continue as they were"* (P9).

Despite the major time effort spent on formal coordination activities, unplanned and spontaneous coordination activities, including *"speaking with colleagues from different companies"* (P1), *"exchanging opinions at the coffee machine"* (P2), or spontaneous drop-ins to *"take a look over the shoulder"* (P8) of a colleague to gauge if they can be interrupted, are also perceived as essential for sysadmins' work. Informal interactions can also be a source of distraction, such as in the form of interruptions mentioned above, which was pointed out by eight participants. Informal interactions with colleagues from other companies are an interesting element, pointing at the communal nature of the system administration workforce, as also reported by Dietrich et al. [70].

Sysadmins have some security-related tasks, such as review of security configuration by *"connecting to systems, reviewing their security posture [...] and improving hardening settings for those systems"* (P22). There may also be a need to *"develop tools or automate things or implement tools and processes in order to detect security issues or also find security issues in that way"* (P21). Nine of our participants felt

that their team was '*"better than the average user"* (P14) or that they had *"always been a secure organization"*, and that those *"that weren't may have struggled there, but we haven't"* (P20). Some participants felt that the management's perspective on system security did not align with their own.

> *"The management says 'well, it works! Nobody has hacked in yet!'. 'Yet!' the admin says. And by that time the manager has stopped listening to him."* (P7)

Participants brought up the *"don't touch things"* (P16) attitude around security practices where if *"in 1980s this was a secure option, so just use it"* (P4). Participant P4 attributed this to complex interdependencies between systems which make it hard to change them and as a result short-term solutions are ultimately chosen over ideal solutions and *"with that you place your utopia on the road-map further away"* (P4).

In the following sections, we center the results around the two main narratives that we observed from our participants regarding system administration work: **helping people** (users and colleagues) and **coordination processes** (formal and informal).

4.3.2. Supporting Others: Lockdown-Induced Changes in Tasks and Responsibilities

Six participants reported that user requests changed during the lockdown. For example, they had to use a different machine/tool at home and *"needed to be talked through how it actually works"* (P12), or address the shock (P7) of the sudden change. There was, however, a reduction in the amount of requests initially.

Reflecting on a period of adjustment, nine participants felt that they performed more tasks during this time because there was *"a huge influx of people who needed connectivity from home"* (P5) and sysadmins were supporting users to set this up. Participant P12 expressed that users were *"overwhelmed what that means for their work and I needed to solve their overwhelmness"*, and that sometimes it was hard to *"get the time to help people because there was so much"* (P12). Certain ongoing sysadmin tasks, such as improvement of the company's internal IT communications platform (P21), became less of a priority during the period of adjustment, while others were accelerated, such as implementing projects that support online work (as reported by eight participants). Four participants noted that new projects emerged, such as supporting pandemic-response.

Two participants reported that existing projects were accelerated to support remote working (a consequence noted in other studies of workplaces during the pandemic [154]). These tasks included setting up infrastructure to facilitate remote work, and supporting colleagues to access this infrastructure and in setting up their home offices, for instance *"sending out the equipment"* (P15). This included provision of access and communication tools, such as the likes of MS Teams (P2) and Zoom (P17), but also supporting users to familiarise themselves with these communication tools (P7), and handling capacity issues with the VPN servers (P3, P5, P10), video conferencing software (P6), or even their private Internet connection

(P10). Similarly, one sysadmin reported supporting a help-desk team that was overloaded with requests from clients who were starting to work from home, and who needed their remote access to the office set up (P24a). Depending on the organization, work of this nature induced delays, in some occasions surpassing 9 months (P21).

Interestingly, organization type dictated priorities too, as exemplified by Participant P5 in a hospital setting:

> *"incidents, things that break always get top priority, that doesn't change. It's just that you don't have an extra priority and stuff that breaks that's related also to COVID-19 gets even more in front of the line than the other things."* (P5)

Adjustments to working practices induced more planned and asynchronous interactions, due to a reduction in informal interactions and physical proximity as a means to coordinate activities. A side-effect of asynchronous communication was that users were more patient with expecting responses from their colleagues when requesting meetings (P6, P16); users were more patient in expecting replies to their queries and started to use existing user-documentation to find a solution for their problem themselves, or as P7 notes on users dealing with small issues:

> *"[If sysadmins cannot] turn around and say: "Hey! do this, do that, do this.", they [users] usually find out that there's a wiki where they can find all this information. And this increased also within the lockdown. Later people started to read the wiki before they are asking me. That's a very nice thing. I mean I am working on this wiki for a reason so that people can read that."* (P7)

Four participants said that they received more security-related concerns from users regarding tools such as Zoom (P4), and two-factor authentication (2FA) (P21), but also from management (P20) (as discussed further in Subsection 4.3.3).

Sysadmins regularly support others by informally sharing advice, for example on how to configure a server (P3), or sharing historical knowledge with colleagues being the *"longest working member of the computer networking team"* when they don't understand something (P5). This mirrors the distinction between providing advice to non-experts for a specific query and providing unsolicited advice, as noted by Poole et al. [219]. Due to the lack of informal interactions during the lockdown, there was a shift to formal documentation of knowledge in forms such as detailed meeting notes (P16) and instruction manuals (P7, P12, P18).

There were implications specific to people who were hired during the lockdown (such as P16, P22 who changed work during the lockdown, and three others who reported new colleagues joining their team) and who had to integrate in their teams remotely; this included P12, who did not get *"the opportunity to build other types of lateral relationships that I typically would just by having lunch in the canteen"*. Other work has noted how sharing of expertise remotely requires trust and mutual respect among the expert and the person asking for advice [213].

4.3.3. Towards Formal Coordination: Lockdown-Induced Coordination Changes

The transition period in the shift to working from home was perceived in different ways among our participants. For example, P7 noted it as taking 1-2 days for everyone to get settled working in their homes, whereas elsewhere it was reported as requiring 6-8 weeks for users to adjust (P15), or in a more specific case 4-5 months to fully set up remote working after the sudden introduction of lockdown (P21).

In terms of the experience of the transition, P13 remarked that there were *"a lot of all-nighters pulled to try and get things fixed and patched and secured"* in the first 3-4 days, as the sudden shift to remote work also undid the prior assumption that no users were working outside of the office. However, at least six participants noted that the shift towards remote work was not a significant change for them. This may be reconciled with the additional finding that a majority of our participants were already used to working remotely and communicating online (Section 4.3.1), such as P1 and P19. This correlates with findings by Olson and Olson, who found that successful remote collaboration is determined by a workplace culture based on long-standing cooperation [213], i.e., the pre-existing continued practice of remote collaboration.

Five participants noted that their organization, specifically the IT department, was prepared in terms of software needs, because remote work was already happening in a limited capacity, where P20 attributed a successful response to the shift to existing *"high level DevOps maturity"*. Also of note are cases where aspects of sysadmins' work could be conducted remotely, such as maintaining computer clusters (P11) or configuring servers and network elements (P14).

Notably, six of our participants explicitly excluded social interaction and small talk from work, framing the reduction in these activities as improving their work, as P9 puts it: *"less social chat, so less time not spent on business"*. Similarly, a reduction in time spent on commuting is seen positively by these participants.

However, participants who were not already working remotely reported an increase in tasks during the period immediately following the lockdown events, and four participants reported an initial period of getting used to this shift towards remote working. This sudden shift to remote working impacted the capacity to coordinate and communicate with colleagues:

> *"the human to human communication has degraded while the engineer to engineer communication has increased."* (P16)

Coordination costs were in some cases amplified where, for instance, P2 reported that even to *"say a small thing to a colleague"* they would *"have to reach him maybe by phone, maybe by other means"*. Six participants reported that some form of a daily call (online meeting) was introduced when work-from-home started. An increase in online meetings during the lockdown was also reported in the work of Delfino and Kolk [66]. Despite all this, sixteen participants reported that they perceived the lockdown itself to not affect their tasks or how they work.

Formal Coordination as Compensation

We noted a shift for several participants not already in a distributed team, from implicit to explicit coordination, and from informal to formal interactions. This often took the form of adding formal coordination steps to an already existing process. P8 described this change in the way of working:

> *"I need 5 minutes to look at the system [...] there were some kind of extra security hurdles and steps that I needed to do to just get inside of the systems [...] since I wasn't able to travel to our customer."* (P8)

This formalization also meant that participants became aware of the formal processes underlying established tasks. Participant P8 remarked that they had to learn to obtain security clearances whereas earlier they would have obtained access by simply looking at another person's system when needed. Requesting and revoking access then adds additional tasks which can potentially affect system security (discussed in Subsection 4.3.3), and as reported elsewhere [156], is a process which often has formal expectations but freedom in how it is conducted by sysadmins.

The shift to remote working required more coordination, most notably in the form of more team meetings. This in itself entailed more coordination tasks such as planning meetings, more interactions and in turn, more time spent on these tasks as *"there's a lot more thought"* (P14), and tasks themselves taking longer to organize and complete. This also applied to routine tasks, such as code reviews which started to take longer to complete (P6). Four participants indicated that coordination itself is difficult when working from home and hence more coordination is needed to compensate for that as well, as for P21:

> *"when you are connecting virtually, you do not spend so much time with others, because now you need to make sure that person is available or not, setting up meeting with them, making sure that you have a very mutual free time. And that does take a lot of operational time of yours."* (P21)

Such activity added additional overhead (added coordination costs [176]), but had potential benefits for some participants, such as creating an audit trail (P13).

In line with increased formalization, existing policy or processes were more strictly enforced during the lockdown. Experiences noted by P11 exemplify this, when describing access to a data center during lockdown: on paper *"the rule was always there"* that this required advance planning so that it was not done alone, but *"usually when you went [...] there would always be someone there"*; when they required urgent access during lockdown and there was nobody at the site, P11 assessed the level of risk and went alone. Kocksch et al. [156] note there can be *oscillations* between security states as processes change, where increased formalization noted by our participants represents a shift to a more secure but rigid state of security with increased accountability. The need for P11 to make a judgement also highlights the role of the kinds of 'moralities' involved in caring for IT security [156].

Less Micro-Management due to Less Informal Interactions

Although increased coordination impacted autonomy, as above, five participants perceived working-from-home as leading to more autonomy in managing personal workload. Asynchronous communication provided the opportunity to manage one's time better and to not have to do something *"right now with 3 other people waiting"* (P7). Similarly, Participant P8 told us that due to strict ISO certifications, there are some resources that they *"couldn't use in the office"* but can do so at home, such as their *"whole private library of IT books"* or *"any private hardware"*. Prior work [66, 213] has reported similar findings regarding increased autonomy and flexibility in distributed work. Considering the act of how items in the home become available to meet work needs, this is akin to 'everyday design' where participants substitute personal items of technology to support their work activities [174], as a lens on their 'repair' of destabilized work processes [137], but here as another 'oscillation' in security [156] but from the perspective of workplace policies that would normally prohibit use of these items for maintaining IT systems.

Three of the participants expressed that the lockdown brought about a positive change in management's perspective on working from home, and less micro-management. For example, P5 told us that working from the office was the norm before lockdown and served as a way of monitoring work; after lockdown, it was accepted that employees can work from home, *"[e]specially when these bosses and supervisors do it themselves also and see that it does have some benefits actually"* (P5).

Furthermore, we see a connection between the lockdown forcing a formalization of coordination activity and a decline in perceived micro-management; spontaneous and chance interactions are replaced by asynchronous communications and planned meetings. For example, P8 noted that interactions around the office had evolved into *"condensed 15 minutes of talking"* (P8) which were work-focused and without small-talk. However, informal and spontaneous interactions disappeared:

> *"In the office I can just walk over and take a look at uh... over the shoulder of my colleague... gauge if I can interrupt him right now... if he's doing anything really important."* (P8)

Note that while this quote ties in more strictly with coordination cost and overhead, the ability to quickly interrupt to poll fine-grained information is also a common theme in micro-management [11, 297]. However, also note that informal interactions help in building trust which is essential for collaborative work [213]. Because informal interactions were difficult when working online (reported by thirteen participants), it is hard to establish trust. In such a case, people compensate through complex formal mechanisms which take more time and effort, and also take away resources from the work that needs to be done [213]. We hence conjecture a connection between increased coordination costs and a reduced ability to micro-manage for organizations that micro-managed *before* the pandemic. Nevertheless, even though not reported by our participants, the inverse *may* also occur based on the literature, which is an *increase* in micro-management due to the absence of established trust from informal interactions.

As also reported in prior work [213], it can be difficult to establish common ground – and develop implicit coordination [78] – with colleagues when working and coordinating remotely. For example, as explained by P4:

> *"When we're at the office, some people come in the room, ask a question and leave. Those questions trigger you to know [...] what those people are thinking about and what they're doing. [...] And now it's only my imaginary bubble of how people work and I think it can be a problem that people drift away with the idea of how other people work."* (P4)

Another example from P12 is regarding visibility of sysadmins' work:

> *"I kind of felt even more caught-out.. out of the work.. after the initial rush. I didn't know what happened. I didn't know who is doing what. Sometimes I was in a meeting and then I heard, 'yeah okay, we're getting this project or that project' [...] and I didn't know anything about it. And it was a bit depressing. And it was the same with my direct IT colleagues. [...] A job that's lonely anyway or more on the lonely side.. was even more lonely."* (P12)

At least six other participants mentioned missing the socializing aspects of work to various degrees, for example P15 shared that they *"really like to spend time both with colleagues and students and that's something that I miss now and I think the quality of the education is impacted by that"* (P15). Nevertheless, in our sample, there are multiple opinions on whether the ability to have in-person interactions is beneficial or not. Six of our participants said that in-person interactions are more effective while two felt that asynchronous communication was better. Still, this difference is in terms of the *effectiveness* of communication. Participants consistently report that from their perspective the amount of communication has increased during the lockdown. Again, this aligns with observations in prior work [66] and reports therein of an increase in overall meetings in order to compensate for the lower (perceived) effectiveness of online meetings.

More Formal Coordination Needed for Routine Tasks

As noted in Section 4.1, sysadmins have several routine activities such as patching, backups, code reviews or security reviews. We asked the participants if these routine tasks had been affected by the lockdown, and ten participants noted that their routine tasks were unaffected. In at least six cases, participants reported that some of their routine tasks were already automated, such that the system would *"install updates themselves and the backups are also automatic"* (P6).

Due to barriers in communication, five participants reported that routine tasks required more planning, such as for updates, or more coordination for code reviews/security reviews which are to be done with other sysadmins and colleagues. For example, the reviewing process *"usually involves more than one person. So you want to have the input of other people. [...] then you either have to wait for 1 day or 2 days until you have this person in a video conference or have to call them"* (P7). Due to the absence of informal interactions more coordination was required and

therefore, routine tasks took longer to complete than before. Such induced delays are also reported in prior work [213], where they are seen as an inherent part of remote work.

As coordination around planned changes and regular tasks has become more difficult, participants reported delaying tasks. Because of the physical lockdown restrictions, system updates and changes were executed with greater caution or *"completely blocked for [...] 3-4 weeks"* (P8). Often this would be because a customer preferred that if everything is stable *"then don't change it, don't touch it, don't do anything to it"* (P8), or changes over a certain severity-level were not allowed as, in the case of a hospital, the organization was on high alert in the lockdown (P5). This relates again to how the lockdown reduced the 'oscillations' between states of secure and non-secure systems that would naturally happen under changing circumstances in an organization [156].

Formal coordination and perceived security

With the introduction of more remote work, IT security has naturally become an important topic. Fourteen participants noted how working from home created several additional attack vectors such as people using private hardware, more online tools for communication, etc. One participant (P8) remarked that online meetings during the lockdown were recorded and stored, creating formal logs on the one hand, but that this also created a risk factor in case of a data breach on the other. Similarly, increased online communication also meant increased sharing of sensitive information online such as *"illegal password sharing"* (P8) via chat. Yet, about half of our participants felt that their system security remained unaffected in the lockdown. We note though that this may equally reflect a social desirability bias around security among sysadmins [70], or *"they're not allowed to talk about this or they are ashamed to talk about it"* (P7).

Contrary to this, five participants reported that they felt that system security had improved during the lockdown because of a renewed interest in security. This is because working remotely meant that security measures can be delivered easier as people are more concerned because everything is *"connected to the outside world"* (P4), new monitoring systems were implemented which normally were considered *"too expensive"* (P5) and everything is formally *"done by the book"* (P8). Similar to the noted shift toward formalization, working from home necessitates working with a process due to the lack of informal coordination and capacity to approach someone for assistance opportunistically, and instead *"now there's like a proper paper-trail"* (P13).

Similarly P8 expressed that while doing everything 'by the book' had the potential to increase overall security and accountability, it can have the opposite effect. Formalizing processes can add layers of complexity which also adds more vulnerability to the system as for example, superiors may forget to revoke system access (P8) or requesting permission for so many things that one has *"permission for everything in the building"* (P13).

Additionally, Participant P22, who joined their team during the pandemic noted that the lack of personal connections, i.e., *'being known'* led to additional barriers and coordination overhead when colleagues tried to flag potential security risks:

> *"it's always difficult for someone to reach out and say, look, I've got a risk here. Can you help me assess it? So if people know me they say "I think this is a problem. What do you think?" And then I can tell them, "yeah, I think that's a risk. Let's kind of do a risk analysis together". And it's a different type of engagement, I think."* (P22)

This ties with a broader theme of routine tasks like updates, patching, reviews etc. starting to take longer, while sometimes the security implications due to the delays went unnoticed. For example, P8 could not perform weekly updates on their Kubernetes cluster for some time after the lockdown since other teams had large backlogs of tasks.

Participants reported that the security awareness of users, managers, employees and, in one case, themselves had increased during the lockdown. Seven participants mentioned an increase in the security-related communication within the organization during the lockdown. This was in order to caution people about the increase in phishing scams (P5, P12, P16, P22), inform them about the security measures to take when working from home (P13, P19), and provide general security advice (P21). As for questions coming back to sysadmins, users and customers also became *"a lot less afraid of being seen as somebody who doesn't know something. They're a lot more open to like... feeling like an idiot"* (P13).

In fact, two participants felt that the security awareness of managers has improved as they raise more security concerns than before and put emphasis on systems' security. Nevertheless, higher awareness, and thereby polling for security-related questions does not necessarily lead to sysadmins introducing additional measures. As P20 explained:

> *"We get a lot of perhaps obvious questions to us, like, hey, is this secure? How is this secured? How is that secured? And it's like, well, how it's always been [...] But we do a lot more of soothing for these people [...] we'll do another pen-test if you want"* (P20)

This correlates with findings from interviews with senior information security managers [193], who reported needing to regularly placate company executives who hear about security attacks on similar organisations elsewhere, then want their staff to be seen to take action of some sort to minimize their own risk.

4.4. Related Work

The related work here is presented in two parts. First we present the studies related to system administration and distributed work in system administration. Then we present the studies related to system administration during crisis situations, including the impact of COVID-19.

4.4.1. System Administration as Distributed Work

Early work regarding sysadmins was either descriptive, e.g., Barret et al. [18], or focused on tools and usability, e.g., Haber and Bailey [108]. Later work then started to investigate the interaction and coordination of sysadmins, for example Maglio

et al. looking at distributed cognition [175], and Velasquez and Weisband who framed sysadmins as 'broker technicians' due to the high communication needs of the profession [282]. Kocksch et al. then expand beyond coordination alone, including discussion of the notion of care in system administration [156]. This general theme of moving from descriptive and tool-focused studies can also be found in the context of computer security [146], where (insufficient) coordination is an important factor in updating systems [271] and security issues [70].

Hence, our work continues along the path of earlier work on system administration, focusing on the coordination and care aspects. Furthermore, due to the work-from-home dimension of our study, we also tie in with related research on distributed work. Specifically, we find that remote coordination can be approached more efficiently by sysadmins depending on work context, as already noted by Holland and Stornetta in 1992 [127]. We also connect to Bjorn et al., who find that effective remote work is a matter of organizational practices and available supporting technology [26]. As our findings suggest, this further highlights the importance of sysadmins, as they are the very people who have to facilitate that supporting technology. Thereby, we further corroborate the **dual nature** of system administration work, between organizing one's own work and caring for the work of others.

4.4.2. System Administration During a Crisis

Crises in IT and system administration are usually considered singular events or incidents that have to be handled, as for example work by Riebe et al. shows, who surveyed CERTs' (Computer Emergency Response Teams) coordination during incident response [234], or De Souza et al., who similarly investigated sysadmins during incident response [253]. Similarly, Haber and Kandogan note that especially for security tasks and issues, sysadmins' work is 'event-driven' [107].

However, in contrast to this earlier work, we investigate sysadmins' coordination during a *prolonged* crisis that expands beyond a singular event. Also, distinct from earlier work, we find that in this long-term crisis, sysadmins did not only have to mitigate an issue *for others*, but at the same time had to organize their own work, as they were also impacted by the crisis itself.

4.4.3. Impact of COVID-19

The global impact of COVID-19 on employees' work has been the subject of several recent studies. For example, Delfino and Kolk examined the impact of the sudden shift to remote working on management control practices and employee responses [66]. They found an increase in the number of online meetings and in the technology used to monitor employees working remotely. Other studies such as the work of da Camara et al. investigated the impact of COVID-19 on an agile software startup in order to understand how they deal with resulting uncertainties [39]. They concluded with several lessons such as the need for socialization events and guidelines, importance of knowledge sharing, maintaining contact with customers etc. Kniffin et al. [154] presented a meta-review of expected employee reactions to COVID-19. They clustered their review around three major impact areas, namely *"i) emergent changes in work practices (WFH; virtual teamwork; virtual leadership*

and management), ii) emergent changes for workers (social distancing and loneliness; health and well-being; unemployment and inequality), and iii) the importance of moderating factors (demographic characteristics; individual differences; organizational norms)". Limoncelli shared five tips for remote working among sysadmins as learnt from the engineering department of Stack Overflow: no mixed-meetings, accurate chat status, a low overhead way for quick chats, work (silently) together virtually and remote social events [168]. Finally, from a security perspective, Lallie et al. investigate how the threat landscape on the Internet changed due to COVID-19 and associated effects [162]. While this latter study is tangential, it still documents how the environment outside of system administration work evolved, specifically here the related digital threats, which are—ultimately—an issue sysadmins have to deal with.

While these studies provide a general idea of the effects of remote working on employees similar to sysadmins, a survey of the literature in the field did not yield any concurrent studies on COVID-19's impact on sysadmins. Hence, our study is the first to address this gap, illuminating how COVID-19 uniquely impacted sysadmins' abilities to *enable* others to continue working through this crisis, while adjusting their own work and coordination practices at the same time.

4.5. Discussion

In this section we discuss and contextualize our overall findings, and relate our results back to the descriptive co-ladder model (Section 4.1). We conclude this section with recommendations and lessons learned, and document the limitations of our work.

4.5.1. Changes to Sysadmins' Tasks and Coordination in Lockdown

Here we return to our main research question regarding how the immediate COVID-19 lockdown changed the tasks of sysadmins. Before the COVID-19 lockdown, sharing advice and assisting colleagues was largely in the form of informal interactions; during the period immediately following lockdown, however, these interactions increased and became more streamlined.

Our results indicate that our sysadmin participants' technical work was generally perceived to have remained unaffected by the introduction of COVID-19 measures. Changes were experienced most directly in terms of the efforts required in the background to ensure that the effect upon that technical work was kept to a minimum. We refer again to the 'co-ladder model' [44] to understand the changes (as referred to in Section 4.1.2).

Firstly, the overall goals (G) of sysadmins did not change across all participants. Ensuring continuous operations and uninterrupted service to IT users was consistently the main goal (G) of our participants, both before and after the COVID-19 lockdown. New systems and services always had to be deployed, and those already deployed always required maintenance and changes. However, the lockdown lead to an influx of deployments and changes to respond to the suddenly widespread

need to work from home. Some of the immediate effects were drastic such as shock (P7), feeling overwhelmed (P12), feeling lonely (P12), negative health effects (P12), change freeze (P5, P8), budget cuts and layoffs of colleagues (P17, P23a) following the lockdown. Most of these effects from the lockdown correspond to findings on the general population, e.g., Kniffin et al. [154]; also see our report on these findings in Section 4.3.2.

We found that the two main aspects of sysadmins' work that were affected by the COVID-19 related measures were: i) An increase in tasks related to supporting others (users and colleagues, as part of IT-related care [156]), and; ii) An increase in formal coordination, with associated consequences for the costs of tasks and adaptability to ongoing needs as they emerge, as seen elsewhere [66, 213]. We will discuss coordination processes through the lens of the co-ladder model with respect to these two aspects. We provide an overview of the mechanisms we observed in our study in Figure 4.3.

Shift of resources to support remote-working. Projects supporting online/remote work were accelerated during the lockdown while some ongoing Plans (P) such as platform improvement were deprioritized. In this case, original plans were subject to Analysis (AN) and were modified to meet immediate needs resulting from the lockdown and surrounding crisis – this is the bidirectional arrow in Figure 4.3. This is seen in the model as EV →AN →P →AC →EX (updated plans after an analysis). We identified this process at least 40 times (13 codes) as mentioned by 19 participants. These coordination processes represent a 'shift of resources and transformation of interactions' based on changing priorities as a result of an Event (EV), which is the sudden shift to working from home for both the sysadmins and the system users. These resources were directed towards projects that support remote-working, and at the same time the interactions with coworkers and system users were changing to adapt to remote-working (usually requiring additional Plans (P)). One positive outcome for the work of sysadmins is the effect of COVID-19 measures on security awareness in participants' organizations and among their managers, see Section 4.3.3. While this is related to comparable effects, e.g., among information security managers [193], it distinguishes this aspect in our population from observations in related work.

Lockdown impact on users and added formal coordination creating distinct tasks for sysadmins. We represent the lockdown in response to COVID-19 as an Event (EV) at the bottom-left of the co-ladder model, which was noticed by participants as both *"a huge influx of people who needed connectivity from home"* (P5) and a range of new tasks and communication as would be expected in a continuous crisis response situation. These constitute new Activities (AC). A large portion of these tasks were in the immediate period after the lockdown, to support the shift to working from home, e.g., by addressing immediate needs by deploying VPN access capacity for users.

We also find a sustained increase in formal coordination due to lack of informal coordination, resulting in Plans (P) to be changed as apply to sysadmins' routine tasks, as well as less micro-management due to lack of physical proximity. When

physical proximity was taken away, participants were forced to perform distributed anomaly response to understand the implications of the lockdown Event (EV). For example, we find that during the lockdown, sysadmins have more online meetings to manage and anticipate Expectations (EX), as a direct result of not having informal interactions. This would have previously relied on physical proximity, such as opportunistically asking nearby colleagues for help. These interactions represent newly added tasks and also a 'shift toward formalisation of interactions'. In the model, added tasks are represented as EV →AC →EX and we identified this coordination process at least 31 times (10 codes) mentioned by 17 participants.

Where Delfino and Kolk note an increase in the number of online meetings and in the technology used to monitor employees who are working remotely at Professional Services Firms (PSF) [66], we found that some participants were shielded from some of the immediate impact of the crisis by processes which already had them working remotely (e.g., being part of an international organisation). Furthermore, similar to several earlier observations contexts, e.g., incident response by Maguire [176] and automation design by Klein et al. [152], we find that added tasks and communicative activities reflect the added costs of coordination during an anomalous situation. Again, similar to the work of Maguire [176], we also note that limitations in coordination practices only became visible due to the additional difficulties introduced by the lockdown. In the examples discussed in Section 4.3.3, added steps to do the extra meetings require extra coordination choreography (like checking availability, figuring out how to get in touch, contacting people, waiting for their response etc.), and remaking existing plans is also effortful, representing costs of coordination.

Asynchronous working changes expectations. Since formal coordination involved planned meetings and asynchronous messaging, we found that in some cases people are more patient with expecting responses from others in a remote scenario, and in two cases believe that asynchronous communication is more effective. We identified this mechanism 8 times (4 codes) in our data mentioned by 5 participants. In the model this is the case of the remote-working element of the lockdown Event (EV) directly modifying Expectation (EX), EV →EX, as 'weakened expectations'. Comparative work on 'tech caregiving' considers initiatives to enhance a sense of belonging, or to shift support to leverage technology [161]; our findings illustrate nuances in the interactions between such initiatives. Informal synchronisation was lost for those participants who were not already working remotely, but it was considered that predictable interactions could be effectively moved online – the background machinations of sysadmins' work were what suffered in this move. Interactions for those users and customers being supported were maintained, with a burden on sysadmins to adapt in order to still support each other. Where Kropczynski et al. [161] discuss building community, we have seen evidence of the role of technology in maintaining support dynamics in communities of professionals. A positive effect we encountered among our participants that has not yet been described in the literature is the positive impact of reduced informal coordination activities on micro-management.

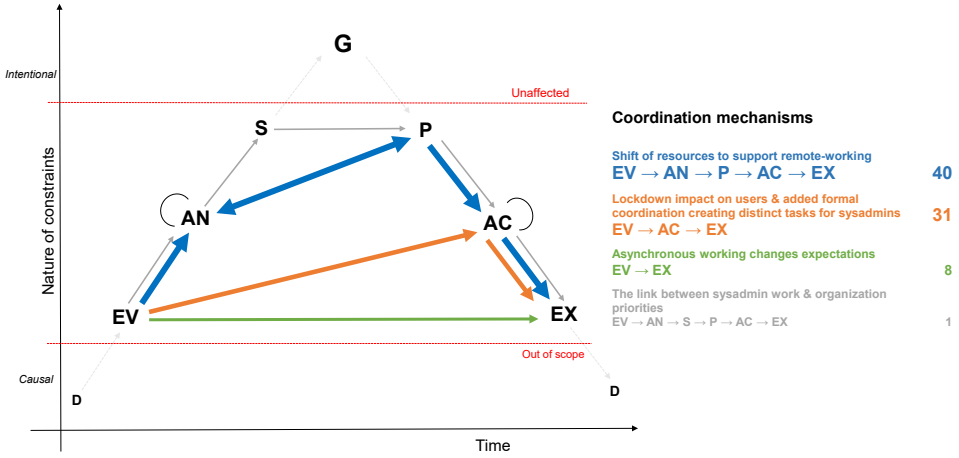


Figure 4.3: Coordination and communication mechanisms we identified in sysadmins' response to COVID-19 lockdowns in the distributed anomaly response and replanning model (co-ladder model). For reference: G = Goal; S = Stance; P = Plan; AN = Analysis; AC = Activity; EV = Event; EX = Expectation; D = Data.

The link between sysadmins' work and organisation priorities. In the case of one of our participants who works in the healthcare sector, we identified a change in Stance (S) following the lockdown event (EV). The corresponding coordination mechanism is EV →AN →S →P →AC →EX where the change in Stance (S) refers to the drastic change in priorities to address COVID-19-related hospital requirements while deprioritizing everything else. While this mechanism is only found once in our data and specific to the healthcare setting, we have included it here as it is relevant when examining coordination during a global pandemic.

Although we did not observe a change of Goals (G), in all these cases we see that sysadmins had to perform additional Activities (AC) while also in turn managing changing expectations (EX). Therefore, in case of an unexpected event like a sudden shift to remote work and related occurrences, such as a sudden increase in support requests or security concerns, it is important to support sysadmins with this added workload. There is a need for analysis and continuous modification of existing plans and priorities to understand how IT systems need to be adapted, in order to support others and to perform coordination activities as a steadfast Goal (G).

We also note that the co-ladder model was well suited for analyzing our data, and allowed us to observe and formalize sysadmins' activities in response to the COVID-19 pandemic, also highlighting differences between sysadmins depending on the organizational setting, e.g., that some participants had already shifted to remote working prior to the lockdown so did not have to change their Plans (P). While this is related to comparable effects, e.g., among information security managers [193], it distinguishes this aspect in our population from observations in related work.

4.5.2. Recommendations

Based on our findings we have several recommendations for practitioners and managers to improve sysadmins' work environments. Specifically, these are:

1. **Identify formal assurances from informal interactions.** The introduction of COVID-19 countermeasures is likely to have revealed technically established procedures and rules that were not stringently followed before the lockdown and were instead reliant on trust. These cases should be critically assessed by sysadmins and related departments, as to whether they provide a practical and perceived benefit by being enforced, and whether formal elements (with their associated costs) can be identified and kept to an effective minimum. Furthermore, any shift to a one-sided solution (remote-only or on-site-only) is not necessarily uniformly beneficial for all sysadmins.

2. **Tools for establishing common ground.** System administration tools—from communication tools to tools used to actually configure systems—should help in establishing common ground without themselves incurring additional coordination efforts, ideally as quickly as possible [108, 127]. Such tools must support sysadmins in sharing their analysis, updates to their plans, and task progress updates with their collaborators, thereby supporting coordination and reducing the need for formal coordination during remote work.

3. **Allow sysadmins to exercise their ownership of system administration.** To enable the supportive and collaborative nature of system administration work (see also Kocksch et al. [156]), decision makers and organizational leaders should ensure that system administrators have sufficient authority over their work and responsibilities to shape and implement working processes that aid them in accomplishing their tasks. By following such a bottom-up approach of informed policy design, processes that cater to the collaborative nature of sysadmins' work can emerge.

4.5.3. Limitations

Our study has limitations common for empirical work. Given that we conduct qualitative work, findings from our sample do not necessarily generalize to the broader population of sysadmins. Especially as most (21/24) of our participants are working in Europe and North-America our perspective on sysadmins outside of these regions is limited; within these areas, our sample covers 12 countries, including eight European countries, and two participants from India, one from Ghana, one from the U.S., and one written response from Canada. Our findings are rich beyond geographical context, providing connections to existing research that is broadly applicable, such as administration of systems in a crisis [234], and the role of care in managing IT and IT-security in organisations [156, 161].

In contrast to the original co-ladder model [44], we apply the model of anomaly response and replanning (co-ladder model) to self-reported data instead of event logs. Hence, our data set, especially in terms of communicated 'expectations (EX)', and whether 'activities (AC)' were appropriate to reach them, may incur the biases typical to participant self-reporting and social desirability bias.

4.6. Conclusions

This chapter presents the results of a qualitative study on impacts upon sysadmins' work related to various national lockdowns in response to COVID-19. We find that, while the *perceived* nature of their work did not change, the impact of the pandemic highlighted the relevance of sysadmins adjusting and sustaining their own practices to *continue* to enable and support others to perform their work. Through adaptation of an existing 'co-ladder' model for understanding coordination and communication, we illustrate that to support this shift, the way in which sysadmins explicitly coordinate was impacted by the pandemic - both task organization mechanisms and communication mechanisms. Formal communication has been translated to online working with increased formalization (less small talk, and more agenda-based meetings). The informal aspects which were integral to sysadmins' work (spontaneous conversations, helping each other etc.) have been replaced by formal communication or were otherwise replaced with ill-fitting approaches. The effort required to coordinate is also of importance, given that sysadmins are tasked with adapting in order to – in a sense – limit as much as possible the need for system users to adapt and in turn be able to continue working in a predictable manner.

Through the lens of the co-ladder model, we also find that many of the new tasks sysadmins encountered due to the pandemic-induced lockdown can be represented in the co-ladder model. Hence, even though our participants overwhelmingly perceived their tasks as unaffected by the lockdown, we claim that they were indeed operating in a "crisis mode" given frequent anomaly response patterns.

Future Work

Our findings currently present a snapshot taken several months after the first lockdown in connection with COVID-19 took place. To more accurately assess how events change the way sysadmins work where crises affect both sysadmins and their users, we anticipate conducting a long-term study on these effects. This would include exploring the representation of multiple instances of co-ladder models, across both sysadmins' own work environment and that of people using the IT infrastructure they maintain for them. In the case of lockdown(s), the capacity to conduct situated studies associated with these lockdowns is limited, where this could include combination of interviews with task/project logs, etc. Also, based on our findings regarding its applicability, further studies can use the co-ladder model to investigate sysadmins' distributed work and coordination.

In terms of the participant pool, our study consisted of mostly men and we did not properly account for gender, similar to the studies we reviewed in the literature review in Chapter 2. Future work must therefore strive hard to account for gender-diverse participant samples and also to understand the effects of one's identity while existing in certain spaces. In the following chapter, we present a focus group study which employs the lens of gender while investigating sysadmins' work experiences. This project is motivated by feminist goals and guided by feminist research methods.

5

Gendered System Administration

This chapter is based on an article published as: Mannat Kaur, Harshini Sri Ramulu, Yasemin Acar, and Tobias Fiebig. 2023. "Oh yes! over-preparing for meetings is my jam :)": The Gendered Experiences of System Administrators. In Proceedings of the ACM on Human-Computer Interaction 7, CSCW1, Article 141 (April 2023), 38 pages [148].

Along with the changes due to the pandemic, in Chapter 3 we identified *care* aspects as part of system administration work. Care work is often feminized and system administration is currently a men-dominated field. Previous research around system administration work rarely accounts for gender of the participants and what role it might play their work. While we did not consider gender as a factor in our last study, we faced difficulties in finding a diverse group of participants to talk to. Based on our findings about care work, the lack of diverse participants and the prevailing masculine culture within the system administration domain, we decided to take a feminist approach for this study.

STEM fields continue to be dominated by men, and people of other genders commonly face barriers to entering and remaining in the field. In the STEM industry and academia alike, cis men are the majority (in terms of the workforce [40, 179, 181], who is being studied [217], and who is *attributed* to producing the knowledge [206, 217]). In men-dominated workplaces, people of other genders face several challenges, such as structural and cultural barriers to entry and higher stress and anxiety, microaggressions, sexual harassment, etc., [21, 96, 139, 222]. Despite all of this, many people persevere and continue to work in STEM fields. In the field of system and network administration, gender diversity remains a goal with a long way to go, and most existing scientific literature does not take gender into account. Understanding the role of gender is, however, important. Not only because gender is socially constructed through interaction, but also because perspectives connected to one's gender shape *how* we build, design, and integrate technology [17, 258]. Hence, by taking a stance on system administration through the lens of gender allows us to better understand the underlying social structures and dynamics at play in the creation of the infrastructures our world depends upon.

In our study, we address this knowledge gap by engaging with 16 system administrators (sysadmins) from marginalized genders (non cis men) via focus groups. We take a constructive approach (inspired by safety science) that focuses on 'what works well' [62, 128] regarding what sysadmins find easy to do in their work, what are the difficulties that they face, and how they overcome these difficulties. Our constructive approach complements existing research that discusses challenges [18] and focuses less on the day-to-day successes [146]. Subsequently, we analyze the data using a thematic analysis (TA) approach. Our findings highlight diverse perspectives in the sysadmin community, such as doing extra gender identity and practitioner identity work and provide a perspective on the embeddedness of care work in system administration work. Understanding and accounting for these are essential for moving towards a more gender-inclusive and just work environment within the field, which in turn is instrumental for building infrastructure that is equitable and non-discriminatory. Since we take a feminist approach, our objective is not to correct the bad politics/practices of institutions or corporations in a top-down way but to find new solutions from the bottom up. To do this, we invited system administrators to share their experiences and better understand what an inclusive workplace—supporting the creation of equitable infrastructures—looks like for them.

This study makes the following contributions:

1. Using a feminist lens, we highlight the invisibilized and undervalued aspects of sysadmins' work, how participants' gender compounds these effects even further and how they persist. Furthermore, we identify and highlight the so-far understudied care work and emotional labour aspects, which are an instrumental part of sysadmins' work and propose more care for these care aspects by recognizing and appreciating them.

2. We explore and describe the negative interactions within non-inclusive environments and how these aspects permeate into the processes, infrastructures and systems created by such teams.

3. We identify the role of non-management facilitated communities and bottom-up self organization to create inclusive environments and highlight that management should not strive to hinder such developments.

4. We emphasize the use of feminist research approaches in investigating system administration work so as to provide more equitable sociotechnical solutions for enabling this work. We ultimately conjecture that the matter of an equitable workplace, which allows people to feel safe to be themselves and fosters a just and blame-free culture, is a prerequisite for secure system operations.

In this chapter, first we present briefly the background of our work in Section 5.1, including defining gender and why it matters in this context as well as the corresponding related work. Second, we present our research methodology in Section 5.2, including our feminist approach to research. Here we also discuss our method of conducting the focus groups, considering ethics, recruiting and analyzing data. This is followed by detailed findings in Section 5.3. Finally, we reflect on our findings and present recommendations in Section 5.4 and present the conclusions in Section 5.5.

5.1. Background

Earlier in the Background (Section 1) we introduced system administration work, its history (Section 1.1.2) and its caring nature (Section 1.1.3). Since care work tends to be feminized and invisibilized (as discussed in Section 1.1.3), this has consequences for gender equity in the workplace, and hence we believe this is a feminist issue. In their work, Kocksch et al. [156] reflect on their participant's suggestion about having more women on the board because *"they are good with the caring aspects of work"* [156, p. 1]. The authors critically discuss this statement:

> *"With this suggestion, the sales representative embraces calls to increase the number of women in business leadership positions across the IT sector. He endorses a feminist cause but, at the same time, invokes an utterly sexist archetype — the "caring" woman who works to redeem male carelessness. While we reject such sexism, we do believe that his suggestion conveys important points:* ***IT security demands care, and it demands a feminist perspective****." [156, p. 2].*

Like IT security, system administration is currently a men-dominated field and—following this reasoning—could benefit from a deeper understanding of care work and a feminist perspective. Feminist research is motivated by social justice and looks beyond privileged viewpoints. It encourages us to challenge the positivist notion of objective knowledge and understands that all knowledge is contextual [120]. Furthermore, it roots itself in the observation that *participants* have expert knowledge about *their own* experiences. Feminist research is also about self-reflection of our role as researchers and identifying and understanding the biases we bring to our research. In addition, we must acknowledge the power we hold as researchers and strive to remove this power imbalance. Finally, feminist research advocates for intersectionality [48] (how gender intersects with all other forms of oppression such as race, ethnicity, sexual orientation, ability, class or age), slow scholarship [195], open access [186], and feminist citation [8]. We discuss this further in Section 5.2.1.

Previous work has taken different approaches to conducting research through a gendered lens. Tanczer [265] interviewed a gender-equal sample of self-defined hacktivists regarding issues of gender, outlined the various mechanisms that create and sustain male-only stereotype within the hacktivitst community including the ways in which women hacktivists counteract these. Slupska et al. [249] engaged with users (65.6% women and 9.8% non-binary people [249]) to better understand how they define cybersecurity threats, how they defend themselves from these threats, and the role of cybersecurity in their lives. These studies take gender into account by engaging with a gender-equal sample (of men and women) or with a user group that is largely (but not exclusively) composed of women and also accounts for non-binary people. We also took a gendered approach in our work where we centered the standpoints of sysadmins who are marginalized in this particular professional domain by excluding cis men. Additionally, there have been numerous studies highlighting the experiences of people with queer identities and other marginalized genders in STEM workplaces. LGBTQ+ professionals in STEM are more likely to experience systemic inequities like harassment, marginalization, career limitations, and devaluation of professional caliber [14, 93]. In a study with students of minoritized genders and/or sexualities, participants explained that STEM fields have lower retention of non cis men due to a ubiquitous dude/bro culture of hyper-masculinity where assuming heterosexuality, treating marginalized students as less intelligent and not smart, anti-LGBTQ+ discourses are pertinent [60]. Mattheis et al. explain that such heteronormative and hyper-masculine cultures make it harder for people of marginalized genders and sexualities in the workplace, by silencing them and thereby resulting in major challenges in creating an inclusive environment for them to thrive in [54].

Throughout this study, we refer to the two-part work of Faulkner [83, 84] titled "Doing gender in engineering workplace cultures". In Part I, the author observed that doing the job often involved 'doing gender', i.e., performing socially guided activities that allude to the expression of masculinities and femininities [295]. Their fieldwork revealed both inclusive practices and dynamics (such as respectful styles of interaction, wide-ranging topics of conversation and humour, care taken to avoid, or challenge, potentially offensive jokes and talk and lastly, mixed-sex social networks)

and gender-exclusive dynamics and practices (such as the fraternal markers of familiarity and bonding, the generic 'he', conversation dominated by mens' interests, offensive humour and sanctions against challenging this, heteronormative and sexualised culture, pressures to conform to particular masculinities and organisationally powerful networks of men) [83]. In Part II, Faulkner presents "gender in/authenticity" to describe how engineering and similar technical pursuits are perceived as gender inauthentic choices for women and the "in/visibility paradox" which explains that women engineers are simultaneously highly visible as women yet invisible as engineers in engineering workplaces [84]. Faulkner's conclusions are directly visible in our study and their discussions in Part II [84] have helped shape our analysis and discussion (Section 5.4) as well.

Gender

Only an individual can state their own gender. *"Gender is not a set of traits, nor a variable, nor a role, but the product of social doings of some sort"* [295, p. 129]. Gender is *"constituted through interaction"* [295, p. 129].

System administration is a men-dominated profession, and social interaction is an integral part of system administration work [147, 282]. Since gender is socially constructed through interaction, it is essential to understand the gendered experiences of sysadmins who belong to excluded genders (people who are not cis men in this context). This is because *"an understanding of how gender is produced in situations will afford clarification of the interactional scaffolding social structure and the social control processes that sustain it"* [295, p. 147]. This way, we can better comprehend the social processes underlying system administration work and how they are sustained. Because gender is embedded in technological infrastructures [254], it impacts how infrastructures are built and how accessible they are [88], recognizing the role of gender is vital in building gender-inclusive technology and equitable workplaces.

5.2. Methodology

In this section, we describe the methods used for our qualitative study. We first discuss how our feminist research approach influenced our research methods. Next, we present how we conducted our focus groups, including how we constructed our question and prompt scripts under our research objective. We then describe how we handled research ethics, including ethics council review, and follow this by a description of our recruitment methods and data analysis process.

5.2.1. Feminist Approach

We centered our research from the standpoints of sysadmins who are not cis men, hence centering experiences of those who are excluded in this profession. Investigating the men-dominated field of system administration through a feminist lens will shed light on previously overlooked personal experiences and social processes, as also stated by Kocksch et al. [156] who in the context of IT security expressed that:

> *"When we use the feminist concept for studying a male-dominated field not previously analyzed in its terms, we draw attention to the invisibilized, undervalued, and also unruly aspects of doing IT security. In so doing, we hope to expand and deepen the debate about what it means to secure computer systems." [156, p. 2].*

Feminist research ethics teach us to make our work accessible and accountable [16], making the issue of open access a feminist one [186]. Hence, we only submit our work to venues that allow us to publish it in an open access way to invite and enable public engagement with our research.

Feminist Citation

We followed a feminist citation policy by being intentional with our citation choices in terms of ideas that we are building. This does not mean that we cited only a specific group of authors (such as only women). Instead, we reflected on the inter-subjectivity and specific relationality of citation [172] in terms of who we invite to be part of the discourse regarding our field of study. By doing so, we ensure that the discourse we create is not biased by what is acknowledged as established by social convention and construction in a patriarchal society that leads to the present. Instead, we take a reflected position in an attempt to provide a more objective perspective on the subject matter of our research, trying to acknowledge and reflect on historical bias in the literature and focusing on making all relevant voices and perspectives heard.

Reflexivity and Positionality

In line with both TA and a feminist research approach, we reflected on our role as researchers while collecting data, analyzing data and presenting the findings. Our research team consisted of four researchers: two engineers who are women of colour (also facilitators of the focus groups), one mathematician/computer scientist woman who is racialized in some Western countries, and one engineer who has experience working as a system administrator and is a cis white man. Everyone in our team has experience working in men-dominated workspaces and in researching expert user populations. The two authors who conducted the focus groups and interacted with the participants were able to deeply understand and connect with the participants' experiences, facilitated by their own professional backgrounds. In our work, we consider this participant-researcher inter-subjectivity as a resource [100]. Although these two authors did not have applied sysadmin experience themselves, they utilized a sysadmin's presence in the research team as a valuable sounding board to validate the directions they decided to take in the study and to request further contextualization of the results.

5.2.2. Online Focus Groups

We conducted our qualitative research in the form of focus groups [197]. Focus groups, given a sufficiently safe environment, enable participants to share experiences and—in a colloquial atmosphere—enrich and encourage each other's participation [252, 300]. To ensure that our focus groups would provide a safe space,

we established a code of conduct participants had to agree to before participating, see Appendix B.5. During the focus groups, no violations of the code of conduct occurred.

We decided to conduct text-based focus groups. Firstly, text-based participation and interview methods are a useful feature to enable wider participation by system administrators [70]. Secondly, it is long known since the extended work-from-home periods during COVID-19 [207], that remote participation options—especially those that de-identify the participants by removing aspects (like visual appearance or voice)—increase the accessibility of spaces to marginalized groups and participants' tendency to be more open [252]. This method is, therefore, well suited for our feminist research approach. Finally, written communication allows the use of emoji, which not only explicated tone and context [113], something usually lost in transcription, but also facilitates engagement without words. We did not evaluate emoji usage as part of the analysis.

In total, we conducted six online focus groups with 16 participants, which took place between 29 November 2021 and 8 March 2022. We set up a self-hosted chat service using the open source software Mattermost[1] for these focus groups. Each focus group meeting lasted around 90 minutes with 2-4 participants (except one session where only 1 participant joined). In total, we conducted six online focus groups with 16 participants who hailed from seven countries (see Table 5.1 for details). Two researchers (R1 and R2) moderated the focus groups. We used open questions to give the participants sufficient room to share what they felt was important in the context of our research questions. Prior to the focus groups, we solicited participants' consent through informed consent forms (see Appendix B.1) and other background information such as job title, job sector, job experience, job country and gender. We supplemented the informed consent with a 'code of conduct' (see Appendix B.5) during the focus groups to maintain a respectful and safe space for the participants.

We started each group by (re-)sharing the code of conduct in the chat. This was followed by welcoming everyone and introducing the two moderators. We then asked for participants' introduction by soliciting (a) a brief description of their day-to-day work, (b) their work experience in years and (c) gender distribution of the team within which they work. This served to start the conversation and to introduce the participants to each other, creating a friendly and safe online space while maintaining anonymity towards other participants, where participants felt welcomed and free to share their experiences and engage with other sysadmins.

Inspired by human factors research in safety science, we take a constructive approach to our question design. We focused more on processes that are working well and less on the problems. Our overall research question is: **In what ways do (non cis men) sysadmins manage to work in the cis men dominated field of system administration?** We devised three questions to try and answer our overarching RQ and used several prompts to solicit further information; see our detailed questions protocol in Appendix B.3.

1. What do you find easy to do in your work? And why?

[1] https://mattermost.com/

2. What do you find difficult to do in your work? And why?
3. How do you overcome the difficulties you face at work?

We planned to spend about 30 minutes exploring one question before moving on to the next, however, we did not enforce this strictly. Instead, we followed the natural flow of the discussion, deep-diving where necessary while providing space for the participants to engage with each other.

5.2.3. Ethics

TU Delft's Human Research Ethics Council (HREC) approved this project under report number 1826. In this process, the ethics council audited our data management plan, including data processing and data storage procedures, data privacy impact assessment and compliance with applicable privacy legislation. We did not collect participants' names during the focus groups; hence, our data (extracts of the group chats) does not contain this information. While we did collect participants' job titles during the focus groups as it helped inter-participant interactions, we do not share this information as it could potentially allow the identification of specific participants or workplaces due to unique job titles used in organizations. Furthermore, given that our participants belong to marginalized genders and the sensitive nature of our data, we deleted all personally identifying participant data after the completion of our study. Additionally, we also completely de-identified our dataset at the end of the research project and save only the aggregated metadata. Our ethical practices align with those proposed for security research with at-risk populations [23]. Finally, the review board also audited the informed consent form that we used for our study with which we collected participants' consent for participation in the online focus groups, see Appendix B.1. Via this form, we inform the participants what their participation entails, how we will collect, process, and store their data. We also informed them their rights about data deletion and withdrawal from the study.

5.2.4. Participants and Recruitment

We recruited via our personal and professional networks by directly reaching out to potential participants and to those who might know potential participants. Furthermore, we reached out directly to people who described themselves as 'system administrator', 'sysadmin', 'sysops', 'ITops', 'Ops' in their Twitter profiles. We also invited participants via a public Twitter post. Considering the scope of our study and our feminist research approach, we wanted to engage with people from marginalized genders (in this case, not-cis men). Hence, for all recruitment efforts, we shared our project description (see Appendix B.2) and asked them to get back to us if they were interested. We did not offer compensation to our participants as sysadmins are generally well paid but very busy in their profession and hence are more concerned about time commitments, as also explained by Dietrich et al. [70].

We were able to engage with 16 participants via six online focus groups; see Table 5.1. Work experience of our participants ranges from one year to 30+ years. The majority of our participants are located in Europe (11/16), while three work in North America, and one in India. Additionally, one participant works in North America and Europe. Participants work in various sectors, including IT, education,

law, biotechnology and non-profit organizations. Please note that this clustering towards European participants stems from our community driven recruitment approach and the comparatively strong community of system operators in Europe, see also Dietrich et al. [70], who observed a similar effect. We are not listing our participants' job titles as sysadmins' job titles can be unique and might make the specific participant or their employer identifiable.

Date/Group	Participant	Job Sector	Country	Experience	Team Distribution	Gender
29th Nov 2021 Group 1	P1	IT	Germany	6 years	One CIS colleague, one non-binary colleague who is not yet out.	Non-Binary
	P2	IT	India	23 years	Only woman on the team.	Woman
	P3	Education	Germany	1.5 years	Five men, two women. Notes that this 'many' women in a team is rare.	Woman
9th Dec 2021 Group 2	P4	Software Dev.	Germany	1-4 years	Currently working alone, had a male and a female colleague earlier.	Genderfluid
	P5	Education	Germany	14 years	Three women team of sysadmins.	Woman
	P6	Technology	U.S.	15 years	Only non-male person in that role. Before in a team of 20 with two women.	Non-Binary
16th Dec 2021 Group 3	P7	IT Security	Germany	17+ years	Only women in a technical position with two male colleagues.	Female
24th Jan 2022 Group 4	P8	IT Consulting	Germany	20-25 years	So far mostly worked with teams with less women than men.	Female
	P9	Education	Austria	10+ years	Until three years ago only women in a team of four.	Female
23rd Feb 2022 Group 5	P10	'La Zone'	France	30+ years	Works alone.	Both and neither
	P11	Technology	U.S./France	5 years	One woman colleague in a team of ca. 35 colleagues.	Non-Binary
	P12	Law	U.S.	1 year	Roughly 70% male colleagues.	Male
8th March 2022 Group 6	P13	IT University	Austria	10 years	Two men and one woman in a team of three.	Female
	P14	Bio-Tech	Germany	6 years	Only woman in a team of 30+.	Female
	P15	Non-Profit	Belgium	5 years	Has one male colleague; All prior colleagues were also male.	Female
	P16	Technology	Canada	25 years	Five male colleagues.	Female

Table 5.1: Focus groups and participants' details. All are self-reported, which leads to use of both "woman" and "female" as gender markers.

5.2.5. Data Analysis

We used the reflexive thematic analysis (TA) [32, 33] method to interpret the data. We approached coding and theme development in an inductive and data-driven way. This was done by the two researchers from the team who conducted all the focus groups and also analysed the transcripts. For Phase 1 - *data familiarisation* - two researchers facilitated the online focus groups and later read through the chat transcripts, asking follow-up questions to the participants as needed. For Phase 2 - *coding* - one of the researchers, being the primary coder inductively built the codebook by coding all the transcripts. The second researcher began by coding the first transcript separately and compared their interpretations with the first coder. This process revealed only slight differences in the codes; the researchers combined their codebooks. Moreover, in our approach, we did not strive for code agreement between the coders but instead used two subjective interpretations to obtain a richer understanding of the data. Therefore, we did not focus on inter-rater reliability (IRR), due to the complexity and nuances in our data [185]. The next five transcripts were first coded by the primary coder and then by the second coder, who a) reviewed

for any missed codes and b) checked the primary codes for consistency with the data. The two coders regularly (virtually) met to discuss questions and disagreements and refined the codebook to end up with 56 codes (see final codebook in Appendix B.6). For Phase 3 - *generating initial themes* - the researchers then regularly met to look for themes in the coded data and created visual code clustering and initial themes. They then discussed these themes and clusters with all the four authors. For Phase 4 - *developing and reviewing themes* - through team discussion, we finalized three main themes, namely: nature of system administration work from the perspective of marginalized genders, care work in system administration work as experienced by marginalized genders and role of gender in system administration work. For Phase 5 - *refining, defining and naming themes* - we identified connections between themes and began the process of reporting our findings. We were able to refine the themes further as we reported them and also name them accurately. For the final Phase 6 - *writing the report* - we reported the research process that led us to the findings, including situating our work within the societal and scientific contexts and reflecting on our roles as researchers.

Marginalized genders (non cis men) Throughout this work, we use "marginalized genders" except in cases where participants specifically mention "women" or a specific marginalized gender. Because we centered the perspectives of all sysadmins who are not cis men, our data does not clearly distinguish between the experiences of people from different marginalized genders. Our focus groups were not grouped by gender and therefore this is reflected in the data analysis. We further discuss this along our other limitations in Section 5.4.3. We refer to marginalized genders by saying "non cis men" and hence, bring attention to "cis men". We do this to call out the privilege that comes with being cis man in a heteronormative patriarchal workplace and hence, the responsibility to deal with the problem of gender inequity in the workplace.

Emoji Use In our group chats in Mattermost, we encouraged the participants to interact with each other as it helpful in building the discussion. One way this was done was by using emojis to react to participants' messages which enables participation without words. Emojis helped to bridge the gap between the unsaid aspects of communication and the spoken (written) text, and aided in setting/understanding the tone of the messages and the overall conversation. Emojis were also used by the researchers who facilitated the focus groups so as to fully (emotionally) engage with the participants and create a safe and inclusive space where everyone felt that they are on an equal footing [194].

5.3. Findings

First, we present system administration work as described by the participants, including aspects of care, visibility and gender. Next, we dive deeper into the aspects of care work as a part of system administration work and the effect of gender, which are the two main themes we identified. Lastly, we present the different suggestions

from our participants towards making system administration work more inclusive, drawing from those aspects of our participants' work that already help them.

5.3.1. Nature of Sysadmins' Work

Sysadmins' work is complex and includes both technical and social aspects. Sysadmins strive to ensure continuous system operations by maintaining the technical infrastructure they manage. This usually includes providing support to the end users of these systems as and when required. In addition to user support, sysadmins coordinate work with their team and interact with several stakeholders. The participants report coordination with their teams and colleagues (P5, P6, P7) as part of their work and also that *"anything that doesn't depend on others is usually easy"* (P16). Working with colleagues can entail mentoring and sharing experience with less experienced team members. The following exchange between participants P1 and P3 underlines the social aspects of sysadmins' work and how the social aspects might be trickier than the technical aspects of this work.

Participant P3 said in the excerpt [2] below that they found it easy to help their less experienced colleague in supporting the end users and noted that the technical aspects were easier by implying that help was not needed regarding those aspects.

***R1*:** What do you find easy to do in your work? And why?
P3: helping to teach the new guy (student) how to reply to confused or upset users.
P1: hehe, so more technical or more social helping? 😉
P3: social helping
P1: sigh... classic
P3: the technical aspect such as "why can I not use the webApp when I'm offline" is easy 🙂
P1: hehe, true. You have to directly talk to customers? While doing software dev? customers/users
P3: Some of them.
P1: that looks like a bunch of context switches. and I presume the "social helping" of men is not valued or acknowledged by the team, just taken for granted? 😉

Furthermore, a majority of our participants (10/16) reported the technical aspects of their job being easy. Participant P5, for example, said that the *"easiest things to do is the linux stuff: updates, configuration, new servers, because I've been a user and admin for 20 years now, so I know the system's pretty well."* (P5). Other participants noted that routine tasks are easy to do (P7, P8, P9), for example, Participant P7 shared that there are *"many routine tasks I do almost every day, these are very easy because I know them and my systems so well. For example, hunting for lost/stuck mail, adding and removing users on systems, the bread and butter work"* (P7). Participant P1 said that *"finding something to do"* (P1) was an easy part of their job. Several other participants reported fulfilling several roles in their job, sometimes being overwhelmed (P15) and overworked (P5). Participant P3, for example, continued (from the previous excerpt) to share the following:

[2] We use chat excerpts from the focus groups to support the findings. In these excerpts, RX and PX refer to researchers and participants respectively, where X is the number assigned. Researchers act as the facilitators, where *R1* is the main facilitator supported by *R2*.

P3: I was the first student hired, I still fill more roles than I like.
- ➥ ***R1*:** @P3 can you elaborate a bit more this? What kind of roles?
- ➥ **P3:** I peside [sic] over meetings which is kind of odd, since two team members are professors who just do not have the time to take care of another project such as a webapp in production.
  I also initially talked many stakeholders to find out requirements for the webapp.
  Me taking care of Servers was more or less an exidental [sic], since I'm the "linux resident nerd" regardless of being female.
- ➥ ***R1*:** @P3 so these are all the tasks that you do that aren't "supposed" to be your tasks?
- ➥ **P3:** yes since people who would usually do them have more official papers and a higher pay grade.

***R1*:** 🤔

Regarding social aspects, Participant P9 shared an image with us, see Figure B.1 in the Appendix B.4, to illustrate the experience of interacting with several stakeholders and *"to get them all to the same picture"* (P9). Past work has referred to sysadmins as 'broker technicians', highlighting their role as technical brokers who create a bridge between end users and the technical community [282]. A significant part of sysadmins' work is about supporting people and their work, as was noted by several participants. For example, providing *"live remote support via screen share"* (P6) and *"2nd-level support (to the teaching staff) and 1st-level to colleagues"* (P5). Previous work [147] has also highlighted helping and supporting others as a fundamental part of sysadmins' work, ranging from simple to complex tasks. As Participant P1 described it: *"My day work is user support for the internal IT, which involves everything from printer reset to Kubernetes deployments"* (P1). Going back to the first excerpt, when asked why they found the "social helping" part of their work easy, Participant P3 responded:

P3: I think I have better soft skills than the average 19 year old boy.
- ➥ **P1:** because of age, gender, or both? 🙂
- ➥ **P3:** I'm not sure. I suspect both.

P2: 🤣

***R1, R2*:** 👍

The above interaction points towards a relation between gender and social /communication skills. Two other participants (P13, P16) shared that they found it easy to communicate with users. Seven participants (P2, P8, P10, P11, P12, P13, P14) expressed difficulties in communicating/socializing with (cis) men. For example, *"men's social activities are not gender neutral"* (P2) and that *"they still feel put out when they need to be inclusive"* (P2), or the men in the team can sometimes be *"demeaning"* (P12), *"condescending or even belittling"* (P14). These difficulties can have widespread and lasting effects as system administration is a men-dominated field (also see 'team distribution' in Table 5.1). Four participants, in addition to sharing their teams' distribution (Table 5.1), remarked on the gross gender imbalance in the system administration work domain. They noted that *"women are often in software engineering jobs and not so much in network or server groups"* (P13), that they are *"yet to work with another woman in IT!"* (P14), that they saw in-

creasingly *"more women in webdesign jobs or UX/UI but the sysadmin field is still seemingly running behind"* (P15) and that in their career they *"have only ever met one other woman that did the same thing as me.* 🙂*"* (P16).

Our participants similarly shared their experiences of working in tech (and within a tech culture) where they saw other women leave the tech field (P2) and they struggled within the *"tech/startup culture, where the norm was that everyone was motivated all the time because our mission was so important. That made it really hard to admit that you had a sh*t job, also to yourself"* (P4). Previous work [288] has discussed this connection between technology culture and the culture of masculinity. Furthermore, three participants said that the hierarchical aspects of their job make it hard for them to say "no" to those who are higher up in the hierarchy (P2, P3), and this can also prevent them *"from doing the essential work necessary to keep things running"* (P5). Past work [191] has elaborated on this relation between organizational hierarchy and patriarchy. System administration work, which is by nature often considered to be invisible work, can compound feelings of being unseen, unwelcome and isolated for those belonging to a marginalized gender identities in these work spaces.

5.3.2. Care Work in Sysadmins' Work

We have discussed care in system administration work in Chapter 1, Section 1.1.3, in terms of caring for things (maintenance related) and for people (helping users and colleagues). Here we dive deeper into these care aspects to better understand the role they play in sysadmins' work from the perspective of marginalized genders, what (gendered) care practices look like and how care work was brought up in our conversations.

***R1*:** What do you find easy in your work considering that you work in a cis-men dominated field?

➥ **P15:** Empathy and relating to your non-IT colleagues. Oftentime people will say they feel stupid for asking questions or not getting it and I feel like I'm really good at putting them at ease (maybe because I'm a woman and perceived more as caring).

P14, P16, *R2*: ❤️

➥ **P14:** @P15 good answer!! I also feel this. I think empathy comes so naturally and easy to me I didn't even consider it here!

P13: yes empathy is an important thing in user support I think

User communication and support are key to system administration work, and previous work has noted the same [147]. The aforementioned excerpt highlights the importance of empathy in user support related tasks. Participant P15 notes how their gender might be playing a role in how caring they are perceived to be and, consequently, how this aids in performing care work in the form of support tasks. In addition to being important, Participant P14 alludes to how easy it is to overlook empathy as a professional quality. When asked if being empathetic affects system administration work, Participant P14 said, *"I have heard for years I have great communication skills and I don't think that'd be the case without good empathy skills"* (P14). These attitudes are in stark contrast to 'BOfH' attitudes discussed earlier in Section 1.1.3 where user requests for support are seen as a nuisance and burden to sysadmins' work. The following excerpt describes in further detail how

being empathetic, being understanding of users' issues and taking the time to explain things to them in a way that would make sense to them fits into sysadmins' work.

P16: - Talking to people at their level when explaining something to them. This is a super useful skill! Not sure what I can attribute this to, but I like to attribute it to my "soft skill" of being empathetic with people when they're frustrated with their tech

➥ ***R2*:** @P16 Why do you think Empathy is useful, how did you pick it up & do you see others working with you being empathetic as well?

➥ **P14:** i also like explaining at the level of others. its one of my favorite things. Because I like learning and sharing knowledge. But its not always easy to me. Sometimes things just click for me and I end up twisting my brain trying to find ways it might click for someone else 😅

P15, P16, *R2*: 👍

➥ **P15:** Oh I feel this 😀 Trying to explain it at a low level makes me understand it way better too. In IT sometimes you take things for granted and "this just works this way" but when you need to explain it to a non IT person, they need to know why it works that way. Or they will sometimes ask question you didn't even think off and it makes you learn something new too

P14, P15: 👍

➥ **P16:** I've had a lot of people say they didn't like working with "the other IT" person because they were treated badly, or like they were stupid for not understanding something. I don't think it's something I picked up but it's definitely something I've honed as an important skill. It sets me apart as a consultant... and especially with women operators (like office controllers, managers, those that pick the consultants 😉) I do see it in others I work with, but it's not as prevalent. I can think of 2 people on my team other than myself that I would consider good at talking to people at their level.

P15: 👍, **P14, *R2*:** ❤️

➥ **P14:** @P16 yes!! i see that commonly in IT (especially as female), people treating others stupid or badly for not understanding or knowing something. I despise this.

Not only does being empathetic help with support and communication to resolve users' issues, but *"people appreciate if they have one who stays calm and do not [sic] loose [sic] patience at their desk"* (P13). This naturally leads to the question of how one's ability to empathize relates to one's identity and how—in turn—this means that some sysadmins are more empathetic than others. We find participants to indeed attribute this to traditional gender constructs, e.g., see the third excerpt, where Participant P3 attributes their soft skills of "social helping" to both their gender and experience. Another example, continuing from the excerpt above:

P14: @P16 yes!! i see that commonly in IT (especially as female), people treating others stupid or badly for not understanding or knowing something. I despise this.

➥ ***R1*:** @P14 do you think that being a female in IT helps you notice such things?

➥ **P14:** @R1 yes and no. I notice things like that regardless. But in many cases in work I have been on the receiving end of that - the one who is made to feel stupid for asking a question. So I notice it much more when it is done to others as well. I've stepped in many times also.

***R1, R2*:** ❤️, **P15, P16, *R2*:** 👏

Participant P14 attributes their qualities of being understanding and standing up for others to their own experience of being treated less-than. In another interaction about social skills, participants shared how they felt their gender played a role. For

instance, Participant P2 also shared how learning social skills was a way of coping while working in a men-dominated field as otherwise they risked being overlooked:

> ***R1*:** @all Since everyone mentioned that the social aspects of work are relatively easy to do... do you think your gender has something to do with this?
>
> ➥ **P2:** I'm not a very... sociable woman in general. Being a woman in tech forced me to become more social or risk getting overlooked.
>
> **P3, *R2*:** 🤗
>
> ➥ **P1:** I think I got most of my social skills by interacting and learning from non-cis non-male people. My own gender came after that and probably is based on much of that, so idk what relates to what in that regard 🙂
>
> **P3, *R2*:** 💕

We further elaborate on gender-related aspects in Section 5.3.3. In the excerpt below, Participant P5 shares their experience working in an emotion-oriented workplace:

> **P5:** I general, I experience this workplace as much more emotion-oriented than previous ones (which were all male-dominated). So, for example, often "i feel bad I didn't do a task" is enough to "resolve" the issue, without the task actually being done by anyone afterwards.
> The problem of feeling personally attacked when asked to do something work-related differently is a huge obstacle to establishing a functional working relationship with some coworkers.
> And I think some of us are so used to having to defend ourselves against men in previous working environments, we take this defensive attitude into our new jobs. I see this with new colleagues, and it usually gets better within a year or two, though
>
> **P6, *R2*:** ❤️
>
> ➥ ***R1*:** @P5 do you think that having to defend yourself (and the defensive attitude) has an impact on your work?
>
> ➥ **P5:** I think, I personally don't feel this way. It's more that I'm sometimes afraid to really stand my ground because I don't know if people know I'm trans*, and if they will attribute it to "male socialization." But others behaving like this towards me makes it hard for me to bring up problems and ask for solutions. Especially if that would involve changes on the coworker's part.
>
> **P6, *R2*:** 😖

When Participant P5 was asked in a follow-up email, if they thought there were any system security implications of an emotion-oriented workplace such as theirs, they mentioned:

> **P5:** It may have, but both ways, for the better and the worse. The positive effect is that I believe (I hope) that my co-workers are more likely to trust us in the system's administration department than if we were men, and so they're more likely to admit to errors that may have an impact on our systems' security. The negative effect is that some co-workers will find it legitimate to not follow protocols that are security-related (e.g. installing the latest updates on their mobile computers, even when informed it is critical to do so) because of personal, non-work-related reasons.

In the above two excerpts, there are several different aspects of an 'emotion-oriented workplace' mentioned. Firstly, the culture of open communication and speaking up has positive effects in terms of asking for help and admitting when mistakes happen. This helps to create a culture of learning from mistakes instead of blaming for mistakes [59]. On the flip side, Participant P5 shared that coworkers might find it okay to not follow protocols in such a workplace. However, we know that people do that anyway (by mistake or deliberately [60, 80]), so it is better if people are open about it. Secondly, even in an emotion-oriented workplace, it can sometimes be difficult to stand your ground (to do the right thing operations-wise) because a) gender considerations come into play and b) it can become difficult for the other person to speak up as it can lead to one feeling attacked/blamed and in turn, a dysfunctional work relationship. Gender considerations, in this case, include having to consider if one's behaviour will be interpreted through a gendered lens which makes one afraid of being stereotyped, misunderstood and in turn, underappreciated in work one does.

Community in the Workplace Another way care was brought up was in the form of community support in the workplace. This was in the form of workplaces that have a *"higher-than-usual level of understanding for personal "problems" and health-related issues"* (P5), where *"personal comes first always"* (P4) and *"conflict resolution always gets the space it needs"* (P4). Participant P4 said that such workplace dynamics were enabled by *"company culture"* (P4) and further explaining *"that most of us are anarchists, including our "boss"* 😀 *he's just doing most of the administrative stuff, but also social coordination, and some hierarchy comes from that of course, also formal/legal hierarchy. But yeah, it's a special ~~place~~network* 😀*"* (P4). When talking about a good workplace atmosphere, Participant P5 stated that *"Working atmosphere is super essential! On several levels: being able to trust my co-workers (also in terms of identity. Like, my team knows I'm trans*, they're all queer, that helps a lot) [...]"* (P5). When asked about the organizational factors that enable work, Participant P7 emphasised the importance of trust and elaborated that *"we are a small group in a small company, so we know each other rather well and have mutual trust. I think that's a key factor, that I'm trusted to do my work well. And because we are so small there is just no place for hierarchies. We have only one layer below the CEO and owner, and even that is more or less on paper, coordinating rather than disciplining."* (P7). In another focus group, Participant P8 shared a similar experience regarding the (limited) role of hierarchies in the workplace (see excerpt below). Workplace dynamics may also be influenced by the kind of work the organization is doing, as in the case of Participant P15, who shared that *"I currently work at an organisation with more women than men so I do think that helps me. My job works with a lot of minorities and progressive humanitarian projects so they're definitely more openminded than a lot of other organisations. This does have an impact I believe"* (P15).

P8: I have an environment where there are hierarchies, but it doesn't feel very hierarchical.
***R2*:** why doesn't it feel hierarchical?
P8: because the tone of the superiors is right, it is not commanding, communication is mostly appreciative

In another example, we see how the workplace community can persevere in the face of harmful and regressive messaging from management. It shows how organizational culture can be influenced in a bottom-up way. However, we also find that these dynamics and workplace communities are far from the norm.

P1: The CEO lately wanted to "keep politics out of work-communication" with regard to our social channel, which is also work to discuss against, when the "politics" is your existence (gender sensitive language discussions are the context)
***R2*:** 😕
➥ ***R1*:** @P1 you mentioned that the CEO wanted to keep politics out of work. I'm wondering what aspects of your company make it better than others (as u said)?
➥ **P1:** its >60% admins and they value ethics, open source, freedom of speech (not the right-wing kind) and such.
therefore, it's clear that just because he wants to, that doesn't mean we do it.
P2: 👆, ***R1*, *R2*:** 👋
➥ **P1:** Most people are there because we do Things better that elsewhere and because the people are cool.
Knowing this, and knowing we are here for ourselves, salaries are way better elsewhere, gives us all (perceived) power
➥ **P1:** Most people are experts and cannot be easily replaced.
➥ **P1:** leads to community
***R2*:** 💯
➥ **P2:** Now I really want to know where you work. Don't say it. Just - wow
➥ **P1:** my pitch is not that inspiring in reality. Or I might have not seen the darkness of other companies..

There were also mentions of a lack of understanding in the workplace which caused difficulties in establishing processes (P5), expectations (P7) and boundaries (P15). For example, Participant P5 first shared with us that their work environment was a supportive one and that they often missed this in their *" "larger team" outside sysad"* (P5), and they *"would have quit several times"* if it wasn't for their supportive sysadmin team. In the following excerpt, they elaborate what they were missing and how it affected their system administration work.

P5: Working atmosphere is super essential! On several levels: being able to trust my co-workers (also in terms of identity. Like, my team knows I'm trans*, they're all queer, that helps a lot), being supportive with each others tasks and challenges without being derisive, trying to find solutions for schedule-related issues (we all work part-time) and holiday-planning that work as good as possible for everyone. Being mindful of what the others are doing and their workload.
I miss a lot of that often in my "larger team" outside sysad, and I would have quit several times, if it wasn't for my team.

P6, *R2*: ❤️

➥ ***R2*:** I am really glad that your team is supportive!! Can you tell me a little bit more about what you miss with the larger team and how it affects your work?

➥ **P5:** Thank you. One thing that's super annoying is that we try to establish processes (like, having a shared mail-address for support, so we can react quickly at all times, independent of who works on that day, or requesting certain information in writing, because of the GDPR[a] documentation), and they keep forgetting to use the channels, writing to us individually, requesting new permissions for users verbally in the hallway, they forget that we need to know things beforehand so we can prepare (e.g. a new class with participant accounts to set up cannot be requested on the day the class starts). A lot of it is not intentional but due to everyone's being overworked, but it makes work a lot less easy, and there is a certain level of disregard involved, too.
Also, our boss piling up extra tasks that "can just quickly be done" without realising how much work it is, which keeps us from doing the essential work necessary to keep things running.

P4, P6, *R2*: 😕

[a]General Data Protection Regulation (GDPR) is a privacy regulation in the European Union (EU) law

The explanation of Participant P5 also alludes to the general unawareness of what their work entails and how it remains invisible, only remembered when something isn't working or is needed. Participant P7 further elaborated on a similar experience.

***R1*:** In this "invisibility" an hinderance for you? Work or otherwise?
P7: Sometimes, yes. Others sometimes expect to get difficult problems fixed in a short time because they can't estimate the amount of work involved with them.
P7: They call and ask why xyz *still* isn't working and that brings me out of my concentration and I have to refocus after that, pick up where I was. That's a nuisance.
***R1*:** So, with the invisibility comes this aspect of underestimation of your work? Is that correct?
P7: Yes, I guess you could say that.

The invisibility and unawareness can further lead to underestimation and underappreciation of the work sysadmins do. Such work environments compound the feeling of invisibility and under-appreciation for sysadmins belonging to marginalized genders. Participant P15, for instance, shared one way this might be happening.

***R1*:** The next part of the focus group is about the difficulties you face at work. You have already mentioned some such as the negative effects of standing out at work.
Are there any other obstacles that your face that you haven't already mentioned?
➥ **P15:** Project management. I have sooo many things to work at simultaneously and it sometimes gets a bit overwhelming. Also boundaries. I really try to set the boundary that my IT support colleague is the one that will be helping with computer issues (everything 1st line) but some people don't get it or don't want to get it. It's mostly the older women at my job who want me to fix stuff
P16: ❤️
➥ ***R1*:** @P15 why do you think people don't respect these boundaries?
➥ **P15:** They probably don't think it's a big deal and don't understand why this order of 1^{st} line - 2^{nd} line exists. Also maybe they feel more comfortable with a woman because we're "softer"? I'm not sure
➥ **P14:** @P15 Agreed, this is also not a strong suit of mine.
➥ **P13:** That's right. They are feeling comfortable with women.

The previous three chat excerpts show different ways in which sysadmins' work has been affected due to the lack of a supportive and understanding workplace. If not in their own workplace or team, sysadmins find community in other places such as Reddit and StackOverflow (P14, P16), culture (P16), a women-in-tech Slack group (P16), *"a "group" with my female colleague to exchange experience"* (P13) and *"an all-women's side-channel chat that we run independently from the main work channels"* (P6).

5.3.3. Gendered Experiences in Sysadmins' Work

Challenges System administrators often face challenges due to their gender in men-dominated spaces, as briefly introduced in Section 5.3.1. Participants mentioned some challenges directly related to gender at their workplace, like having to do extra work to prove themselves (6/16). For instance, in the excerpt below, Participant P14 mentioned that they have to go above and beyond to get accepted by the team; otherwise, they mentioned *male* colleagues explaining topics they are an expert at. Participant P12 said that they felt a sense *"being demeaning [sic] by the male especially when dealing with deep aspects of their line of duty (law)"* (P12), Participant P14 mentioned being *mansplained* to by some colleagues who *"do not talk to our other male colleagues like that"* (P14) and Participant P13 said they were often ignored and condescended by their male colleagues.

P14: i think my biggest difficulties at work are the fact that I feel like I need to go above and beyond what my male colleagues do just to get a spot on the team.
People just assume you don't know stuff. I get explained simple stuff all the time where I want to say: how do you think I got this job without knowing that?? most recently I got explained what the /24 means at the end of a IP. This colleague even knows I worked in networking department in the past. How do you get so far and not know that, where you think you need to explain that to someone. I don't feel that need to explain that to any one I work with.
P15, P16, *R2*: 😡
➥ ***R1*:** This is infuriating! Do you think this extra effort/ annoyance has an impact on your sysadmin work?
➥ **P13:** I think the same, as a woman you have to give more than 100 percent where men's work is just fine with 70 percent or 80 percent.
***R1, R2*:** ☹️

Furthermore, our participants mentioned having to perform higher than men to succeed. *"I think the ratio of high performing women in IT is likely a LOT higher than men, so I agree. In general women do have to perform better to succeed"* (P16). Participants P13, P14, P15 and P16 also mentioned that when dealing with external parties and clients, they need to be more prepared for these meetings because they not only have to talk about the topic at hand but also have the onus of proving their expertise in the subject matter. This is a challenge that women in IT need to tackle on top of their daily activities. As a participant explains, *"I think my biggest difficulties at work are the fact that I feel like I need to go above and beyond what my male colleagues do just to get a spot on the team"* (P14). Participants mentioned that their male counterparts, on the other hand, seem to do well even if they are under prepared in these situations. For example, Participant P14 noticed that their *"male colleagues come to meetings with externals completely unprepared and all is good"* (P14) whereas *"... as a woman you have to give more than 100% where men's work is just fine with 70% or 80%"* (P13). Earlier work [84] has reported similar findings where women in engineering have to do extra practitioner identity work as their professional (engineer) identity is seen as 'gender inauthentic'. Participant P14 summarized this:

> *"Nothing is really easy. I feel like I have to give 110% to even compete or something. even on the parts that I personally find easy"* (P14)

Generally, since subject matter expertise seems to be under scrutiny, our participants reported allocating a large amount of time to prepare for meetings. As Participant P15 mentioned, *"I never ever want to not have an answer because I'm afraid it will reinforce any underestimation"* (P15). This is not referred to as *'preparing'* for the meeting but rather *'over-preparing'*. Participants reported a significant pressure to be at the top of their game so as not to lose credibility as this is seen as *"fuel to those who aren't very nice to us females in IT"* (P15). These pressures relate to the issue of workplaces invisibilizing marginalized genders in IT; see also Section 5.3.3. One may often be alone (and sometimes the first!) to exist in certain work spaces. This, in turn, can induce a feeling/burden of representing the community one belongs to, tied with a fear that every minor imperfection will be picked up and framed as re-enforcing harmful stereotypes by the environment [84]. Moreover, the higher performance requirement is not only related to performance at a job level, women also need to show *"more "experience" than men"* (P13) while applying for the same job. In an example shared by Participant P10, we can see how gender-stereotypes and prejudice played a role in hiring:

P10: As independent, I just moved the hardships to getting paid work. An example: I was approached with a problem. Asked two rounds of questions while working on an approach. Took me two weeks to make a very decent approach. Communication died. Sent three emails. No reply. Spoke with the manager a year later at an Agile Open (which I organized as part of my marketing strategy). He said, the plan was perfect, and they hired a "Kostwinner" to implement it.

***R1*:** 😳

➥ **P10:** "Kostwinner" = "Head of household who needs to make money"

➥ ***R1*:** @P10 did you find out why they blatantly ignored your emails and went with a "kostwinner"?

➥ **P10:** Yes, at the [X conference], he said, "That man needed the money". I replied, "so do I, shall I send you a bill for those two weeks?". He got red faced and buggered off from the event.

P11, P12, *R1*, *R2*: 😡

The above excerpt is a striking example of sexist hiring practice. Not only do workplaces see engineers from marginalized genders as gender inauthentic in their profession, but they are not perceived as breadwinners and hence, not perceived as suitable as men to be salaried employees. In addition, their labour is considered open for the taking. Other ways in which we identified participants having to establish their professional expertise in our study were being *"left alone to move a 300lbs server"* (P2), being *"straightforward and technical in my first communication whenever possible just so they know I "play ball" and know what I'm talking about"* (P15), using *"full official title/signature in email"* (P16), and trying *"hard to prove those people who have bias' towards women in IT wrong"* (P14). Participant P5 elaborated on having to do extra work;

> *"...always having to prove that I know what I'm talking about, that they can 'talk tech' to me, and that I really literally mean what I'm saying when using tech terms (and not just having picked them up from my boyfriend, or whatever they seem to think), that's super exhausting. I double- and triple-check most of my mails before sending them, which I wouldn't do otherwise, I think."* (P5)

Previous work [84] has noted that this extra layer of work done to establish one's professional expertise doesn't really end as it has to be performed "every time they encounter a new colleague, associate or client for the first time" [84].

Coping strategies The study participants reported coping with working in such men-dominated professions by accepting *"that not everyone will want to work with me"* (P2), by *"picking my battles"* (P2), ignoring prevalent structural issues that have *"always been that way. Like the only woman in the meeting has to bring the coffee because she has to be the secretary"* (P9) and *"gritting my teeth and plowing on, venting with colleagues - especially with the one female colleague I have now <3"* (P9), by supporting other women (P9), by **not** asking for accommodations (P14) so as not to *"reinforce any cultural biases against women "soft/weak/unable to handle stress" "* (P16), by letting *"roll off the comments from my back"* (P13) and not taking them personally even though *"you are the only gal in the room and the only one being treated like that"* (P14), and by anticipating *"being underestimated"* in meetings (P15).

In addition to accepting reality as it is, coping strategies are also about actively disrupting the status quo, such as by questioning everything (P8), by behaving *"properly towards people and make sexism look like silly foolishness"* (P8), by amplifying *"my opinions and thoughts during meetings"* (P12) and speaking up *"when I see gender bias and I always never hesitate to praise my work infront of my colleagues"* (P12), and by enforcing boundaries (P15, P16). Coping can also look like removing oneself from an unwelcoming environment by abandoning *"a project that I like if there's a man on it that's is insecure about women"* (P2) and limiting after-work socializing because *"men's wives have been known to get jealous or men's social activities are not gender neutral"* (P2), changing departments (P8) and changing jobs (P11). Participant P2 expressed that such avoidance strategies have *"cost me promotions"* (P2). Another participant noted that sysadmins change jobs *"more often than in other fields"* (P1) for several reasons such as better salary or for "fresh wind" and *"sadly, this leads to few people "doing the work" and actually improving social conditions, when there are many companies to choose"* (P1). Many of the aforementioned ways of coping with discrimination and unfairness constitute emotional labour [126].

Some of the coping strategies mentioned above constitute gender identity work which stems from being highly visibilized as a marginalized gender who might stand out in men-dominated workplaces [84]. For example, not asking for accommodations (P14) to not reinforce any unfavourable gender stereotypes. Participant P2 shared the ways in which they do gender identity work:

> *"ways I overcome my gender at work: 1) I dress differently. I stay away from over femininity at work. 2) I am more conciliatory than in my personal life. 3) I change my voice (lower the register) on purpose as I have found it's easier to get my point across. 4) Avoid any natural tendencies that might be overtly feminine."* (P2)

Participant P2 added that, in remote work, there was less socializing, and hence, fewer gender considerations came into play. This was perceived as better in terms of doing gender at work but also called for added efforts around *"relationship building"* (P2). Visibility as women takes shape in the form of stereotypically feminine identities - most commonly as (hetero)sexually available or as mother [84]. As Participant P13 shared, *"if you mention you have kids (I have 3) they are amazed, "uuu - can you do your work without the kids are interrupting you? 😢"* (P13).

Coping strategies affect sysadmins' work Doing this extra work in terms of practitioner identity and coping strategies leads to other effects. For example, sysadmin tasks can take longer to complete because participants reported being slowed down (P2, P14) by the extra tasks being performed and also due to nitpicking where other *"people get their stuff passed in a day with typos and errors that I would get blocked for"* (P11). Therefore, these additional chores performed in the form of coping can ultimately affect participants' system administration work. Participant P3 said that in order to cope with all the extra tasks, *"I need to be very organized and have clear priorities. I do try to limit working overtime. Avoiding it is not easy*

though. I try to delegate whenever possible, though of cause [sic] that causes other issues too" (P3). Other adverse effects of these coping methods that we observed were missing out "on a fun learning experience" (P2), decreased motivation (P1, P14), "super exhaustion" (P5) and appearing unprepared when fully prepared (P11). As Participant P11 explained:

> *"especially in engineering where it seems like men will go into maintenance with little preparation thinking it's fine and everything will go well, and when you do prepare more you seem unsure of your ability."* (P11)

Finally, the participants also reported harmful health effects stemming from gender-related workplace issues. In addition to demotivation and feelings of burnout (P16, P14), Participant P9 reported that it had an *"effect on my self-esteem and on how outgoing I am"* (P9). Participant P4 shared their experience of working in a men-dominated tech/startup workplace:

P4: yes, at my previous job it was a lot harder. I got a lot of harsh feedback which I thought I had just to accept, even though I couldn't process it emotionally. One time when I got feedback I was drunk for two days.
I'm not sure whether it was because the company was male-dominated or had this tech/startup-culture, which has of course many patriarchal implications.
P6, *R2*: 😕, **P5, P6, *R1, R2*:** ☹️
➥ ***R2*:** @P4 could you share how this affected/impacted your work?
➥ **P4:** I had a hard time to focus, tried to look busy anyway, couldn't open up... back then I was focussed on writing technical/promotional blogposts instead of sysadmin tasks, so it was creative work, which suffered a lot from this.
P5, *R1, R2*: ☹️
➥ **P4:** It was especially bad because of the tech/startup culture, where the norm was that everyone was motivated all the time because our mission was so important. That made it really hard to admit that you had a shit job, also to yourself.
P5, P6: 😡

Gendered In/Visibility

In engineering spaces, "women engineers are simultaneously highly visible as women yet invisible as engineers" [84]. Faulkner explains,

> *"Although the inauthenticity and invisibility of women engineers as engineers means they have to do extra layers of practitioner identity work, their visibility as women often means – paradoxically – that they also have to do an extra layer of gender identity work."* [84].

As we learn from our participants, this effect carries over to people not fitting with the gender binary system. Similar to women, they might not be seen as "real engineers" [83, 84] because such spaces tend to be cis men-dominated and anyone that does not belong to that identity will be seen as an outsider. And just like women have to do extra gender identity work in the form of being feminine "enough", trans, non binary, genderfluid and agender people might feel pressured to conform to heteronormative expectations. They might also struggle with feelings of belonging and/or might be made to feel like they don't belong in certain work spaces [28].

Sysadmins' work is invisible and is usually brought to light when someone needs something or something stops working [147]. As Participant P7 shared with us:

> *"Sometimes I think my work is not really seen by others outside of my field. If I do my work as a systems administrator really good it is more or less invisible, because everything "just works" and if not others just see me typing at my computer, and then it works again."* (P7)

Sysadmins' work is invisible and underestimated, as mentioned previously by Participant P7, but also described in earlier studies [147], and traditional textbooks [169]. Due to the invisibility of women engineers and engineers who do not fit in the gender binary, and the invisibility of system administration work in their organizations, our participants can experience double invisibility. As a result, these people end up doing extra work both in terms of professional and personal identity. In the following excerpt, Participant P11 shared their experience of being left out of work communication (invisibility) and having to redo their work (extra practitioner identity work). We also see how these dynamics have not only an effect on the participants' work but also on their mental health in terms of losing motivation and interest, as exemplified in the following chat excerpt:

P11: so, we have a pretty big timezone difference with most of my colleagues, which used to work fine and not be a big deal
- ➥ **P11:** but over the past year and a half, I found myself left out of projects, and finding out about them through company emails announcing the project, for instance
- ➥ **P11:** or, as I said, getting all my work nitpicked for days, or re-done again after I'd done it
- ➥ ***R2*:** @P11 So sorry that this is happening. However, just to confirm for the purpose of interpretation, Can you confirm if the nitpicking happens due to gender / working remote?
- ➥ **P11:** well, as always, it's hard to say definitely if it's for a specific reason, but I know it didn't happen as of a year ago when I was clearly read as male, and I know it doesn't happen for other coworkers, even ones that are remote with a similar time difference
- ➥ **P11:** so, I would say it's probably related

***R2*:** 👍

P10: Losing way too much time on the power play communication reduces my effectiveness at getting things started/done.
- ➥ **P11:** yeah, it makes me feel demotivated, disinterested, and it materially stops me from working on projects with colleagues, etc

5.3.4. Inclusive System Administration Work-Environment

In this section, we present the different recommendations and ideas offered by our participants for an inclusive workplace in terms of formal and informal processes. In addition, we also report on the current practices at workplaces of certain participants that work well for them. We finish by reporting our participants' reasons for staying in this men-dominated field of work. These thoughts and suggestions shared by our participants provide a practical starting point toward positive change.

Supportive Workplace In all the focus groups, we asked the participants about the organizational, social and environmental factors that help them overcome challenges they face at their respective workplaces. Almost all our participants mentioned that an inclusive workplace is a requirement for a good working atmosphere. Of multiple aspects that were mentioned, some of the most common asks were mutual understanding, trust, and respect from their team members and co-workers. For instance, one of the participants stated the following when asked about important aspects for them to thrive in the workplace:

> ***R1*:** [...] I was wondering, what aspects of the workplace would be most important for you to thrive well in it?
> **P7:** As I said, freedom to work as I want to (within sensible bounds, of course). Not having to discuss every step I'm going to do with someone higher up. Mutual understanding, respect and trust with my coworkers. I wouldn't want to work somewhere I know I'm not respected as I am, or are not trusted to do my work.
> ***R2*:** 👍

Participant P7 shared that *"..of course in the beginning the old name and pronoun sometimes slipped out by accident when coworkers were talking with or of me, but that got fewer and fewer over time"* (P7). Another common aspect that the participants mentioned was diversity within teams. Promoting diversity by hiring people from diverse backgrounds, gender, race, sexuality and people with disabilities. Participant P3 suggests, *"Hire and promote more diversity, such as immigrants, people with disability and females. Respect those who are different, instead of underestimating their skills"* (P3). In addition to diversity in hiring, timely promotions to qualified people and supportive management were also highlighted, as Participant P7 stated: *"When I read 'Good working atmosphere', I think about team-focused behaviour, cooperation, responsive communication, timely promotions to those who are qualified, supportive management, and sensitivity especially when it comes to race/gender/sexuality/disability, and I find that incredibly important"* .

Participant P1 stated that they expected Human Resource (HR) departments to practice what they profess as a part of the company culture: *"Make HR actually do the workshops for a company to BE the things they write on their homepages. Same for C-Level. Just don't think you're better than other companies, try to get the data on that - and than work with it."* In addition, Participants P2 and P7 mentioned that every HR department and DEI (Diversity, Equity and Inclusion) initiative needs to be supported by the upper management to champion better policies and practices at every workplace. As Participant P2 stated about their workplace: *"The HR needs the backing from management, without it, it tends to go now where. HR needs to be very progressive and walk the talk. I knew we had the right person to sponsor change when she was overheard saying: I dress how I like and I don't have to meet anyone else's idea of gender norms"* (P2). Participant P7, regarding company culture and DEI practices, also stated that, *"The upper level(s) of a company have to support it, but I think it also needs support from the bottom"* (P7). Having a supportive and unbiased team manager *"..that takes notice of communication problems and works on solving them would also be appreciable"*

(P11) and *"encouraging openness and transparency in managements treatment to the general workforce regardless of gender"* (P12). When asked about whether any organizational factors help participants overcome gender related obstacles they face at work, Participant P2 mentioned, *"DEI, Resource groups like GayStraightAlliance. Good clear policies. A strong HR department"*. We discuss below in detail the formal processes for gender equity that we encountered.

Process for gender equity Organizations that some of our participants worked at had some DEI practices in place. Participants P2, P12 and P7 mentioned that their workplaces have HR policies, information and education in place to support gender equity. Participant P12 even stated that policies around biases are followed strictly and in some circumstances *"have previously caused termination of some employees"* (P12). Even when these practices are in place, they still have a long way to go in terms of adoption. While some organizations have these practices in place, Participants P8 and P11 reported that their organizations did not have any such measures in place. In some organizations, DEI resources were not equitably distributed; while some employees had access to them, system administrators were among the few who did not. Participant P9, who works at a university, mentioned that education and coaching are not available for all employees:

***R1*:** @P9 @P8 Are there any measures in place to address your needs at work considering you work in a cis-men-dominated field?
P8: no not with my workplace
P9: I think my boss would get a red head when I tell him with a dead pan face there should be bins on the women's toilets ... 🤔
***R1*:** 😶
P9: well, there are supposed to be measures in place. In theory, in practice, I would not go there because I would be afraid everyone would know about it soon after
P9: in theory, in practice, I would not go there because I would be afraid everyone would know about it soon after
P8, *R1*, *R2*: 😔
P9: It would be nice if there would be some coaching in place, it does exist but 'only' for scientists.
P9: Like doing research in a male dominated scientific field. but there is nothing for administrative personnel

It can be helpful and vital to have a tangible picture of what a just and inclusive workplace looks like. Participant P1 mentioned using data driven analytics, Objectives and Key Results (OKR), and project management tools to support and keep track of inclusion initiatives. Such initiatives should not just be written in words but rigorously followed upon. Regularly surveying employees about *"how accessible and inclusive the workplace is"* (P1) would help to better understand how employees perceive the workplace. Participant P1 suggested that open/vague survey questions such as *"How is the work life balance?"* (P1) could be reformulated to solicit more detailed information from employees such as by asking *"what changed for you, if anything, since the last time. What would help you"*? (P1). Furthermore, certain *"traditions need to be broken and not carried along"* e.g., only hiring female

secretaries (P9). Such metrics can help to avoid the trap of performativity where companies have a DEI program in place while simultaneously the employees feel that they *"shouldn't have to thank someone for not taking the department to a strip club"* (P2).

Why stay in a men-dominated field? As highlighted in the previous sections, system administration remains a very cis men dominated field. And participants highlighted a multitude of challenges they face were related to their gender. Most participants indicated that technical aspects of their job were easy for them to do, as mentioned in Section 5.3.1, while the environment is sometimes hostile and impedes their actual job. Passion and liking for their job was one of the common drivers that came up as a common response by 6/16 participants, for instance, *"It's IT. That's my life, there is nothing else* 😀*"* (P1) and further elaborated by Participant P7:

> *"I love the work I do. I feel I'm enabling others to do their work and to communicate, and that is something I really like, enabling communication. I also love hunting bugs, figuring out tricky situations. It is very rewarding for me to get to the point where I understand why something isn't working the way it is expected to. It's often a kind of detective work, discovering clues and following them."* (P7)

System administration is a field that is ubiquitous, there is a need for system administrators in almost every organization. For instance, a quote by Participant P1 emphasizes this, *"I am right now looking for more people for my team. The recruiter told me 'There are NO unemployed sysadmins in Germany. Good luck', that's what I mean"* (P1). Availability of jobs was one of the reasons participants mentioned as to why they wanted to stay. Participants P1 and P9 also mentioned that switching companies for a higher salary is easy without having the need to acquire new skills. Job security (P9) was another reason in response to this, *"..also a reason to stay for me is that it is a very secure job and a lot of leeway in other things like free time planing, vacation time"* (P9). Money was yet another reason that came up, one of the participants mentioned that they left the field but came back to the field to an organization that did feminist and anti-racist work, as indicated the excerpt below:

> **P5:** Tbh, I quit after 7 years, studied something entirely different at uni, and never wanted to go back into the field. But money was an issue, and my organisation does really important feminist (and some anti-racist) work, supporting women entering the job market and stuff. So working for this particular org. was the initial motivation to get back into systems administration. Now it's partly working for the organisation, partly the lack of alternatives (I'm over 40, trans*, and have (mental) health issues, after all), partly that I actually do like to do Linux and networking stuff.

Workplace better than others Some participants mentioned that they stay in their current position because they feel that their workplace is better than their previous ones. Participant P1 expressed that *"The company is better than others,*

so it's at least kinda rewarding, because there are many political and queer people and we just support each other in our Agenda to queer the place up 😀*"* (P1). Supportive bosses and flat hierarchies were other factors that was mentioned by Participant P4, as reported in Section 5.3.2. Participants P4 and P7 stated that lack of hierarchies is important for them to stay at their current workplace, due to the ease of communication, task distribution, and trust among team-members, *"..we have very flat hierarchies, so it has rarely been a problem. If something (amount of tasks) is too much for us we either do it later or not at all"* (P4). While some participants mentioned positive aspects of their workplace being better than others (P6 and P5) they have worked at or are familiar with, we found a troubling aspect to this because there were some who *felt stuck* at such places. This is reflected in the exchange between P6 and P5 below:

P5: Ah, okay!
One thing is that the prospect of leaving my job and returning into an "all-gender" (aka: male-dominated, or all-cis-male) team is so horrible, it sometimes feels like I'm "stuck" at my current workplace.
(Right now, I'm quite content with the job, but it used to be different, and my very well change over time.)
Dealing with other people outside the institution (support staff from companies we buy services from, etc.) is often challenging, because they treat us as Lusers. Which sometimes means bug reports are simply dismissed, mails not read properly, stuff like that.
P4, P6, *R2*: 😕

➥ **P6:** @P5 Feeling stuck because I've finally found an inclusive job is a huge feeling! I want to leave because I want to expand my horizons, but I remember how awful my past workplaces were and I don't want to give up what I have here with coworkers who gender me correctly and include me in decisions/announcements and respect me personally as well as my contributions. I ended up asking my manager to find me dev work to do instead of applying for a dev job elsewhere because of this even though I do want to move on from doing support so bad it hurts.
***R2*:** 🤗, **P5:** ❤️

And while some of our participants mentioned the importance of being able to choose/leave their workplace (P4, P6, P10), (seen also in previous work [15]), others acknowledged how difficult it is to find a workplace where you feel like you belong.

5.4. Discussion

Here we discuss our overall findings, recommendations for enabling sysadmins' work and the limitations of our work.

5.4.1. Ways of Managing System Administration Work in a Men-dominated Field

First, we discuss the findings in the context of our main research question which is: In what ways do (non cis men) sysadmins manage to work in the cis men dominated field of system administration?

Being excellent

Being *good* at their profession was not sufficient for our participants. Instead, the environment created a constant expectation of completely error-free excellence. At the same time, our participants felt that their men-counterparts were not subject to the same pressure to *constantly* excel. The participants excelled at their technical tasks and know-how and by honing their social and communication skills. Similar to earlier findings [15, 84], our participants tried to establish their professional mastery with the expectation of being recognized and respected by their colleagues. Having to deal with other peoples' gender prejudice and discrimination, they spend extra time and effort in the communications aspects, to do their tasks and in the form of emotional labour [126]. This impacts the sysadmins' work in several ways such as extra (and sometimes repetitive) tasks which reduces work effectiveness and produces negative effects on mental health.

Doing gender

Doing gender entails the performance of various masculinities and femininities within existing social constructs and dynamics [83, 295]. Among our participants, dealing with gender inauthenticity and gender in/visibility in their role (see [84]) were two prevalent aspects. They coped with this by going above and beyond in the work that they do in both technical and social aspects (as discussed above) but also by constantly taking gender considerations into account. We elaborate below:

Gender inauthenticity: Are you really the sysadmin? Gender inauthenticity is about the perception of someone as not fitting the norm (in their professional role) due to their gender [84]. Despite being an expert user, one participant experienced being treated as a 'luser' by external support staff, based on our participant's gender identity. Traditionally, 'luser' refers to users who may not be computer-literate and is also used in the context of BOFH work culture where such users are seen as a nuisance. And while this term is problematic to be used for any group of people, it is worth reflecting on why sysadmins (expert users) are facing this treatment as it ultimately is about gender. Faulkner talks about gender in/authenticity in the context of women in engineering spaces [84] where a woman who is an engineering profession is seen 'gender inauthentic'. They highlight how consequential it is to, both, be an exception and to conform to the norm (the norm in this case is to be an engineer who is a man). People who may not conform to this norm, such as the participants in our study, may then be seen an 'gender inauthentic'. And once someone does not see you as a 'real engineer', they begin to question your professional ability and even gender identity [84]. In response to this dynamic, many people do extra practitioner identity work by being extremely well-prepared, being excellent at what they do and repeatedly establishing technical prowess in social settings, and gender identity work which is discussed below.

Doubly invisible: Too good to be visible Our data allows us to identify a phenomenon of double invisibility, not previously described in the literature. This

relates to gender-related in/visbility issues, i.e., women in engineering spaces tending to be invisible as engineers but be highly visible as women at the same time as described by Faulkner [84] being combined with the 'System Administration Visibility Paradox' described by Limoncelli et al. [169]. What they describe is that due to their job, system administrators are invisible as long as the infrastructure functions, and are *"noticed only if something breaks"* [169]. This means that they remain especially *invisible* as long as they do an *excellent* job. Hence, people of marginalized genders working in system administration are affected by both of these effects, *especially* as they feel additional pressure to excel, which in turn makes them *more* invisible professionally, while the visibility they do receive tends to revolve around their gender *and* things not working well/breaking. Participants overcome this invisibility by doing both practitioner identity work (as discussed above) and gender identity work. Gender identity work takes several forms such as adjusting their femininity (dressing style, voice register, being agreeable) so as to be "better able to strengthen or protect their fragile membership" [84] within a men-dominated profession and steering clear of enforcing any negative gender-stereotypes (like not asking for accommodations so as not to seem weak).

Finding community

Standing up for others and advocating for betterment is of course not part of system administration work but 4/16 of our participants spoke about it. Participants recounted incidents of empathetic bravery where they stepped in when someone was being treated badly. This signifies caring at the level of the community by fostering an inclusive workplace. As reported in Section 5.3.4, we found that a strong HR department, DEI resource groups, good and clear policies (such as clear processes to address discrimination and tangible objectives for inclusivity) were thought to be necessary in overcoming gender-related obstacles at work. However, previous work has shown that HR departments (since 1980s) are seen as the "compliance cop" or the "double agent" or "smiling assassin" [52] due to their core function being that of protecting the company and being answerable to top-management. This is also demonstrated in a recent example from Uber where employees' complaints of workplace sexual harassment were not only not acted upon by HR but HR actively protected the accused (who had a long history of misconduct) [90, 143].

Community care can be in the form of an understanding ("emotion-oriented") workplace and solidarity with coworkers. Participants found and sustained supportive and inclusive environments in their workplaces in a bottom-up way and forming a community that persisted through microaggressions, unfairness and harmful messaging from top-management. Sharing experiences and finding a support system through other people of marginalized genders often can lead to a feeling of community and being supported at the workplace, for instance the excitement of having another *"female colleague"* for *"venting"* as shared by a participant. Such a work environment, while highly treasured, is an exception to the norm. In fact when they do find a caring workplace, some participants reported experiencing a feeling of being stuck. This is because being able to change workplaces is an important aspect in one's career development, i.e., to gain a salary increase or promotion [281], and for participants who finally found a caring and inclusive workplace, this creates a

difficult situation described by participants as 'feeling stuck'. Due to the dire state of the industry in terms of *good* working environments, they saw themselves in a dilemma between advancing their career and risk giving up the caring environment they found themselves in or staying where they are at the cost of career progression. Here, we want to make explicit that this is *not* an issue of caring workplaces, but instead highlights the transitive impact of the hostile environments in *other* companies on career prospects for people of marginalized genders.

5.4.2. Recommendations for Enabling Sysadmins' Work

Here we discuss recommendations a) as found in related work in the field, b) based on participants' input (Section 5.3.4) and c) according to authors' insights.

Suggestions based on Related Work (Mainstream vs Feminist)

Mainstream Prior mainstream qualitative research focused on system administration work [18, 70, 282] and similar research provides various recommendations to enable sysadmins' work, for example, by designing better sysadmin tools, technical support systems [18, 108] and automation [70] to support the complex and coordinative work of sysadmins. In addition to technical solutions, organizational changes such as blameless postmortems and clarifying responsibilities have been recommended in order to mitigate security misconfigurations made by sysadmins [70]. The book "The practice of system and network administration" by Limoncelli et al. [169] ends with a extensive list of suggestions for "what to do when" (including "fixing the perception of being unprofessional") followed by the "many roles of sysadmins" (including "positive roles" such as "the hero" and "the disaster worrier" and "negative roles" such as "the SA[3] who cried wolf" and "the martyr"). It appears that traditional system administration literature mainly puts the onus on the sysadmins to better their work and/or largely relies on technical support to do so. These suggestions miss the feminist perspective and do not account for the gendered reality of system administration work. Hence they do not address the socio-cultural processes underlying system administration work and do little to comment on the issues that need addressing in order to enable this work.

Feminist Related feminist research (introduced in Section 2.3.5), provided care-related suggestions for gender-equity in the workplace. For example, Tanczer [265] expressed the critical need for change in the quantitative gender imbalance in the workplace as well as the way in which society talks about gender [265] and Faulkner [84] asserted the desperate need for changing the engineering workplace culture and the understating of gender within it:

> *"there is a crying need for sustained, organisation-wide equality and diversity promoting efforts to affect profound 'culture change' in/of engineering workplaces. [...] any such efforts need to challenge stereotyped dualisms – to create space for more plural versions of masculinities and femininities, and more heterogeneous understandings of engineering"* [84, p. 185].

[3] System Administrator

Yoder and Mattheis highlight the value of social/institutional policies in promoting supportive and inclusive work environments but also remind us to acknowledge and allow for different individual expressions in workplaces [307]. Mattheis et al. advocate for increasing awareness regarding diversity of gender and sexuality and specifically, trans-inclusive policies and practices, reasoning that trans individuals are made particularly vulnerable by mainstream practices and expectations [183]. Cech and Waidzunas emphasize the need for STEM domains to address anti-LGBTQ attitudes by including LGBTQ status in diversity efforts, providing networking and support opportunities for LGBTQ employees, and ensuring equal access to (in)formal benefits [41].

Research that employed a lens of care (Section 1.1.3), for example the work of Kocksch et al. [156], argues for the need of care in IT security. They noted that while secure technology may tolerate carelessness, keeping technology secure requires a lot of carefulness [156]. The work of Tseng et al. examined digital security-as-care in the context on Intimate Partner Violence (IPV) by using a model for providing security advice that "incorporates the feminist notions of care into an overall sociotechnical infrastructure for caring" [275]. They advocated for care infrastructures for IT security, specially in the context of high-risk survivors.

Suggestions based on Participant Inputs

Our participants shared their suggestions regarding different ways in which their workplace could be better and more inclusive (reported in Section 5.3.4). These included care-ful practices like a supportive and empathetic workplace environment, and formal processes that protect against discrimination.

Fostering a supportive workplace A supportive workplace, according to the participants, is one that is inclusive. It is a workplace where teams are comprised of people from diverse backgrounds and where the working atmosphere is based on mutual understanding, trust, respect, openness and transparency. To create and foster such a work environment, participants suggest hiring from a more diverse pool of people (inclusive of immigrants, disabled persons, marginalized genders etc.) and enabling a working culture that puts people-first (such as via timely promotions, sensitivity towards topics of race/gender/sexuality/disability, being vigilant of one's own implicit bias and prejudice regarding others). Workplaces with relatively flat hierarchies and supportive management that reject outdated traditions (such as solely hiring women secretaries) help in facilitating an inclusive working atmosphere. Additionally, an HR department that truly implements their progressive policies and is supported by the management is seen as important. We elaborate the suggestions regarding processes and policies below.

Having formal processes defined and followed Having DEI practices and HR policies that uphold equity and protect from discrimination is vital. Often these policies exist on paper but are not well-implemented and followed, if at all. Participants suggest that having tangible goals and metrics to measure progress are necessary to ensure that these policies are rightly followed. Suggestions by Participant P1, for example, are to *"have a clear picture and write it down, what the just*

and inclusive workplace looks like" and *"get the data of where you are right now and plan/interact with the employees how you can get to your ideal"*, and use *"data driven analytics with regard to inclusion and social skills"*. To collect this data, Participant P1 suggested to move away from questionnaires/surveys with a 5-point rating/Likert-like scale and a generic comments box at the end. Instead, the suggestion is to move towards soliciting open text inputs for improvement suggestions in specific areas and asking *"detailed questions like "how accessible do you think our workplace is", "what changed for you, if anything, since last time" and "what would help you" "* instead of the usual *"how is the work life balance"*.

Suggestions based on Authors' Insights

Finally, based on our observations of the role of care in system administration across genders, we recommend more care for care work and underscore the importance of a feminist perspective as it relates to computer security.

Caring for care work The invisibility and unawareness of system administration work can bring with it an underestimation and underappreciation of this work. This, we find based on participant reports, creates a situation where those performing care work are uncared for. Sysadmins are mostly contacted when someone needs something [147, 169]. This can cause work interruptions, high workload and unrealistic work expectations for sysadmins. We find that if such conditions persist, sysadmins might experience stress, frustrations, demotivation and other negative effects. Toxic workplaces have been said to enable the BOfH (Bastard Operator from Hell [274]) working culture [54] which is the antithesis of a care culture, specially when it comes to interacting with people. A self-reinforcing circle emerges where the undervaluation of care work on an institutional level increases the frustration of performing invisible care work and leads to BOfH (Bastard Operator from Hell [274]) inspired coping mechanisms, which in turn affect the organizations' interaction with and treatment of sysadmins. However, we hypothesize that a workplace culture of community and care has the potential to disrupt this cycle and maybe even reverse it.

Based on our results and prior literature, we claim that to care for sysadmins' work is to recognize the vital contribution of sysadmins in forming the bedrock of modern society, and therefore to visibilize[4] and value this work. In addition, care work tends to be badly accounted for *and* operations-critical, so it becomes that much more important to better understand and appreciate it. However, it is also important to not put the responsibility of this on the sysadmins themselves. Instead, we have to (re)build organizations around a just culture, a culture of care, that enables operators to realize good outcomes, that is, building reliable and equitable infrastructure that supports the needs of people and society.

From Feminism to Computer Security Our feminist research approach is driven by social justice and it guides us towards creating more just and equitable work environments for sysadmins. In our study we centered the experiences of

[4] to make visible something that was previously intangible or invisible to the naked eye [173]

those who have been excluded in this domain so as understand from them what an inclusive workplace is/could be like for them. An inclusive work environment for sysadmins, we find, is about recognizing the many invisibilized gendered aspects and care aspects of system administration work, to *care* for them by understanding and valuing them and to support sysadmins' work as it is done in practice. The matter of an equitable workplace is not only a question of gender. Instead, it is a pre-condition to fulfill the basic requirements for an environment to let just culture take effect (for e.g. in the form of blameless postmortems [70]) and make lasting social changes. Ultimately we believe this is essential to perform secure and reliable systems operations, meaning that a safe and equitable workplace in which people can be themselves contributes to computer security and safety in organizations.

5.4.3. Limitations

Experiences of people from marginalized genders are not all the same. We engaged with sysadmins who are not cis men to highlight excluded perspectives but we did not focus on the differences and nuances between the experiences of people from marginalized genders. The effects described in our findings therefore will vary for individuals. Moreover, much of the related work we present focuses on women only (and not much on marginalized genders), which affects the framing of our work and comparability to earlier work.

Our study also has limitations that are common for qualitative empirical work. Our participant population hails mainly from the Global West. Findings from our sample cannot directly be transferred to a broader population of sysadmins outside of the Global West since the dynamics of men-dominated workplaces may be different. However, men-dominated engineering workplaces are the norm worldwide and hence, our findings can be interpreted contextually.

We remained open to intersectional aspects (intersection of gender with other aspects of identity such as race, ethnicity, sexual orientation, ability, class or age) in our work but did not solicit this information from the participants and neither were we able to identify them during the analysis. This could also be because our participant pool of 16 sysadmins was not large enough to capture the diverse perspectives.

5.5. Conclusions

We engaged with 16 sysadmins who are not cis men via six online focus groups and solicited their system administration work experiences particularly through the lens of gender. Using a feminist research approach, we were able to identify and describe the hidden/less understood parts of sysadmins' work such as the care aspects and the gendered social processes. From the perspective of those who are marginalized (sysadmins who are not cis men), we reported on how they managed their work in a men-dominated profession (see Section 5.4.1). They do so by a) being excellent in the system administration work that they do, b) *doing gender* by performing extra work to establish their professional identity and constantly taking gender considerations into account, and c) finding and creating community in their workplace.

In addition to the care work that we discussed in Section 5.1, we found that care aspects are present in other ways, such as empathy for people (both users and/or coworkers) and communication skills or 'soft skills' in the form of care practice, looking out for each other in the form of community care and the lack of care for care workers. We identified community care and support as an important way of managing work in a men-dominated work environment. As for the role of gender, we found that gender is deeply intertwined in sysadmins' work and observable in the form of doing gender identity work and practitioner identity work.

We know that "there are no technical solutions for social and societal problems" [86] and we cannot hope to enable sysadmins' work only through technical means, especially when a major part of this work is social. Traditional research that qualitatively examined system administration work generally proposed technical solutions and sometimes social changes. However, in order to truly capture the social dimension and do so equitably, we must employ a feminist lens. We highlighted this by comparing suggestions for enabling system administration work by mainstream sources to feminist sources (see Section 5.4.2). Overall we find that sysadmins' work, especially the care aspects should be more cared for by being better recognized, understood and rightly appreciated. Finally, yet importantly, we discover that the feminist lens of care can ultimately contribute to increased computer security and safety in organizations by shedding light on the invisibilized care work and emotional labour, which are a significant part of the participants' system administration work, and hence fostering a just culture in the workplace.

Future Work

Future work should investigate the similarities, differences and nuances between the experiences of people from marginalized genders not to enforce 'one size fits all' solutions. Similarly, it should also delve into the intersectional aspects by understanding how other factors of identity, such as race, class, or ability play a role. Finally, in line with employing feminist approaches, future work should investigate sysadmins' work through a technofeminist lens [55] by further exploring intersections between gender, capitalism, and technology and technological infrastructures.

In the following chapter, we discuss our findings spanning the whole PhD project and then develop recommendations for enabling sysadmins' work and moving towards safe and just system administration work environments. We discuss the overall limitations and also elaborate on the future work directions.

6

Discussion

"Underneath every simple, obvious story about 'human error', there is a deeper, more complex story about the organization."

Sidney Dekker, The Field Guide to Understanding 'Human Error' (2002)

"If a world can be what we learn not to notice, noticing becomes a form of political labor."

Sara Ahmed, Living a Feminist Life (2017)

This chapter converges our observations from individual research projects to an overarching perspective on system administration, and how we expanded the state of knowledge. First we talk about the human factors of system administration work followed by care work and how it is embedded within. Next we reflect on what a just and caring workplace culture would look like for all sysadmins. We then take a step further and devise practical recommendations as starting points to shift toward a more just workplace culture. Finally, the limitations of our research are contextualized and suggestions for future work are made.

6.1. Human Factors of System Administration - the "problem"

Originating in the mid-20^{th} century, the study of human factors used to be about preventing accidents by focusing on root causes (e.g. human error) and eliminating them [6]. Over the years, (also refer to the safety science timeline in Figure 3.2) the focus of human factors research has shifted away from individual human behaviour and towards organizational and societal level factors. Recent research, for example the work of Hollnagel et. al. [128], highlights the complexity of operations in sociotechnical systems and advocates for humans-as-a-solution approach in order to make everyday operations more resilient. Another example is the work of Leveson [166] who developed a system-theoretic model of accidents (STAMP) which is a systems-level approach for accident analysis and system safety in the context of ever-increasing complexity of systems.

In contrast, human factors research is relatively new in the context of computer science. Hence, in this work we set out to understand this so-called "problem" of human factors and how it is handled in the information systems and computer security domain. We refer to human factors as a "problem" (in double quotations) to draw attention to the fact that humans are seen as a problem (weakest-link) in computer security that needs to be controlled or eliminated. This problematization of the human factor is in contrast to the safety science perspective. Comparing computer security with fields working on human factors for longer (like safety science), we find that these fields have moved on from the idea of proposing and implementing technical solutions to the human-error issue and trying to mitigate or eliminate it. Instead, the focus has shifted to comprehension [58, 60], and on understanding which circumstances lead to good outcomes–and which facilitate negative outcomes–all the while acknowledging the important role of people in such systems [128]. Such an approach paves the way for designing systems and processes in a way that enables safe and secure operations [128]. Note, systems here refer to the full composition of social and societal interaction, governance and organizational structure, human behavior *and* technology, aka sociotechnical systems.

While the prevention approach has its place, it is important to first understand the work done on the daily by professionals so as to ensure that the solutions offered are needed, wanted and effective for those who will be implementing and navigating them. When we conducted a structured investigation of human factors research in computer security (Chapter 3), we found that computer security research still com-

monly takes the prevention and elimination approach, with the all too well known limited success, as security incidents remain prevalent and often get attributed to "human error" [302] or other human limitations [157, 158]. From this we concluded that there is a need for a different perspective, converging lessons learned from safety science with computer security, especially–as our literature review demonstrated–in the context of system administration.

When we set out to study system administration using a model of coordination and communication for distributed anomaly response (Chapter 4), we could indeed confirm common patterns and obstacles in coordination impacting safety and security. We found that some formal organizational work processes were in conflict with the actual work performed by sysadmins and that top-down (micro-)management strategies were an obstacle for sysadmins' work autonomy. However, this study also highlighted the importance of social factors and dynamics for the reliable operation of digital infrastructure. Specifically we found that, in running and maintaining of digital infrastructure and services for users, (a) sysadmins perform **care work**, (b) sysadmins' work remains largely **invisible**, specially when everything is working as expected for the system users and, based on these two points, (c) the invisibilization of system administration work brings with it its **underappreciation** which can contribute to a toxic workplace culture (see Figure 6.1). In so far, system administration includes factors that are not at the core of safety science, but have been studied before in a feminist context (we discuss this further in Section 6.2).

Again, human factors research in the computer security domain remains behind these other fields. Prior work tends to be cis-men dominated, focusing mainly on the global north (Chapter 3) and the conclusions of studies with such biased samples are often presented as useful-for-all without sufficiently acknowledging the gender or geographical bias. Such "evidence-based" advice is ineffective at best and downright harmful at worst for those belonging to marginalized identities [296]. Doing sociotechnical research without an intersectional feminist lens therefore continues to enforce the status quo, overlooks the issues and dynamics of people who have been historically excluded from such spaces and that, as we already know [116, 188], further perpetuates their exclusion.

As the sample of our first study was mainly centered around the global north and cis-men participants as well, we decided to start filling this gap in our own work and the field as a whole. We decided to further investigate the gendered component of system administration work while deep diving into those aspects that set system administration apart from other fields. These aspects, as mentioned previously, are the invisibilization of system administration work, the performance of care work as part of system administration work and the subsequent underappreciation and underestimation of this work. Hence, we designed a study using a feminist research approach and engaged with those sysadmins who belong to marginalized genders in the sysadmin professions (i.e. sysadmins who are not cis men).

In our study, we find again that system administration work involves significant amount of care work and emotional labour. We find that these aspects are invisible, unknown and not really considered formally as part of work, which only increases the burden of work on sysadmins. Importantly, we discover that these

effects are compounded for sysadmins belonging to marginalized identities in the cis-men-dominated field of system administration. Interestingly, the field of system administration has not always been this way. In fact, women played a central role developing and running computer systems during the second world war (detailed in Section 1.1.2). However, this profession was taken over and (non cis men) pioneers were driven out when it became lucrative in the post-war era. In our study, we find that sysadmins who are not cis men experience **double invisibility**–both due to their profession and their gender–and feelings of **being stuck** in their job–due to not wanting to work in toxic men-dominated workplaces. These phenomena also reveal the illusion of meritocracy in workplaces and highlights the various other factors apart from merit (such as the freedom to change jobs) that play a role in career advancement, specially for those people belonging to marginalized genders. Ultimately we believe that workplaces that are inclusive and provide psychological safety for *all* sysadmins are a pre-requisite to ensuring safe and secure organizational system operations.

Therefore, in summary, the problem of human factors of system administration work is not about limiting or preventing the human influence. But instead it is about deeply investigating the various social processes that impact the work of individuals. For example, it is about comprehending how the societal cultural norms inform workplace culture, how this affects people differently depending on their identities and how this further uniquely impacts their sysadmins' work processes. The study of human factors therefore must be about understanding these interconnections and then supporting the work processes by focusing on equity. Our work in this matter sheds first light on these interactions. Nevertheless, thoroughly subjecting the field of system administration to a feminist lens to unravel existing injustices and transform the field to a more safe and secure environment will remain an ongoing challenge.

6.2. Care Work in System Administration - the feminist lens

Care work is commonly associated with taking care of others in, for example, the healthcare domain. However, care work can also be in the form of caring for digital infrastructure (see Section 1.1.3). Within system administration, care work shows up as the dedicated running and maintenance of digital infrastructure along with supporting colleagues and the end-users. Another way in which (the lack of) care can be seen is the popularity of a series called 'The Bastard Operator from Hell (BOfH)' [274] in sysadmin communities. The series centers around a rogue sysadmin who is angry and frustrated at the system users who lack in IT literacy and pester him for help. Such BOfH-inspired working attitudes can cause real harm not only to the end-users but also to sysadmins themselves (see Figure 6.1) and also to the organizational outcomes.

We first identified care work in the interview study (Chapter 4) which inspired us to dive deeper into these care aspects, specially when the need for it has also been previously recognized [156]. In their work Kocksch et al. [156] talk about

the feminization of care work and the need for a feminist perspective to better understand the *"invisibilized, undervalued, and also unruly aspects"* [156] of working in a men-dominated field. Therefore, we decided to use a feminist research approach and employ the lens of gender to not only better understand the different ways in which care work shows up (or lacks) in sysadmins' work but also to do so by engaging with those sysadmins who belong to marginalized genders. To center our study around non cis men sysadmins is at the core of our feminist approach. With this choice, we highlight the voices that have for decades been excluded first, by being pushed out of the domain as the socio-cultural perception of the profession changed (explained in Section 1.1.2) and second, in literature through the overlooking of gender (by conducting "genderless" research that simply continues to enforce the status quo).

In our study we found that sysadmins who are not cis men do perform extra care work that is not expected from cis men (Chapter 5). In the context of working in a men-dominated profession specifically, we found that sysadmins manage their work in three main ways (see Section 5.4.1), all of which constitute tasks that require carefulness. Firstly, they manage their work by **being–not just good– but excellent** in their daily work. This entails extra care in the form of (over)preparation for meetings, having to establish professional expertise in order to simply be accepted, and dealing with other people's gender prejudices and the sexism embedded in organizational processes along with the associated emotional labour. The second way sysadmins manage their work is by constantly taking gender considerations into account in order to deal with the phenomenon of (a) **gender inauthenticity** and (b) **double invisibility**. In this case, care work shows up in the performance of many masculinities and femininities (for example by dressing differently or altering one's voice register) in order to be accepted and taken seriously. Thirdly, sysadmins **find and maintain supportive communities** both in the workplace and in the form of online communities. Here care work shows up as the extra effort needed to find and foster supportive spaces, to find or create inclusive workplaces and then to persist in these places without feeling like you have any real option for change due to rarity of such inclusive environments.

Overall we discover that sysadmins who are not cis men perform care in various ways all of which are invisibilized. The care work pertaining to the technical tasks remains unseen, undervalued and underestimated. Similarly, the care work pertaining to the gendered aspects of sysadmins' work is also invisible but the effects are compounded for those who are systematically excluded for these spaces. In other words, it leads to an overall increased burden in the work while also dealing with invisibilization both due to profession and gender prejudices, and the subsequent underestimation of the work itself due to it's invisibiliation and the sysadmins' gender. Also accounting for the BOfH-inspired workplace attitudes, sysadmins of all genders working in patriarchial men-dominated workplaces have to put in a lot of extra effort and care work which remains unseen, even more so when done well. A vicious cycle of uncaring emerges (see Figure 6.1). This effect impacts sysadmins who are not cis men significantly more, as they have to be excellent simply to be accepted in these spaces, while their presence and success propels their invisibilization

and underestimation, all the while patriachaical expectations on care work increase the workload put on them.

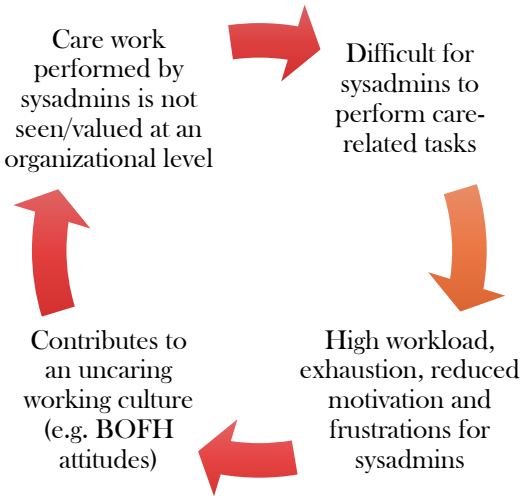


Figure 6.1: The self-reinforcing cycle of uncaring

We believe that this cycle of uncaring can be disrupted through care. We recommend to care for sysadmins' work by appreciating the vital contribution of sysadmins in the everyday functioning of modern society. The care for sysadmins' work is to **visibilize and value** this work. It is about carefully taking account of real work done by sysadmins, specially those who have been historically excluded, and to formally recognize it as part of work. We find that the kind of and amount of care work being performed depends on one's identity. This is because of the coordination processes and social interactions that are underlying the day-to-day system administration work. These processes are affected by the socio-cultural and -political patriarchal contexts within which they exist. We can only understand and describe these processes by accounting for these contexts and their influence, moving beyond a simple and shallow analysis that ignores these socio-cultural and -political contexts created, supported, and maintained by the patriarchy. By employing a feminist research approach, we acknowledge the different aspects of peoples' identities and how their daily life/work is impacted by it.

In summary, the first step was to understand care work as part of system administration work (Chapter 5) and the next step is to accept that not all sysadmins are doing the same kind or amount of care work and focus on better understanding these differences and nuances. With this knowledge, we are better equipped to create equitable workplaces by catering to everyone's different individual needs instead of simply treating everyone equally which may contribute to maintaining existing in-

equalities. Inclusive workplaces create psychologically safe spaces for *all* employees, which we believe is an essential precondition for sustaining and improving organizational computer security. Such a workplace can be supported by a restorative and just working culture.

6.3. Just and Caring Workplaces

The roots of a restorative approach can be traced back to many ancient traditions across the globe [29]. A **restorative** justice approach is one that is about reducing harm and learning from incidents, and does not focus on blame and punishment. The questions in a restorative approach therefore investigate who has been hurt, what their needs are and whose responsibility is it to meet these needs [59]. Hence, it is more about gathering peoples' honest accounts of what happened without fear of blame, and learning from these accounts [59, 61]. A restorative just culture involves the moral engagement of stakeholders, reintegration of care workers into the community, community-level care, emotional healing of those affected by the incident, and eventually, long-term organizational learning and improvement [145]. In contrast, more widely used is the **retributive** justice approach where the focus is on culpability in terms of which rule was broken, who broke it and how bad was the infraction (in order to determine the magnitude of punishment) [59].

In today's society however, restorative approaches can be found mainly in specific reconciliation programs where long-term healing and empowerment drives the ultimate (justice) goal. For example, in victim-offender (e.g. IPV) mediation programs [264], in the context of patient safety and harm in healthcare [145], in addressing online harm in adolescent lives [304] and in schools to address student behaviour through traditional Māori protocols [216]. The modern safety science approach strives too for a restorative just workplace culture (refer to safety science timeline, Figure 3.2). Some recent work, such as examining just culture approaches–substantive justice, procedural justice and restorative justice–in the context of impacting organizational safety culture [59], also brings these ideas into the domain of system safety.

In the context of system administration, a just and caring workplace is one that sustains and nourishes a restorative working culture and cares for *all* its employees by supporting their individual needs. Caring for sysadmins starts with acknowledging the scope and amount of system administration work being done, specially the invisibilized aspects of their work. It is then about supporting their work based on their different needs, deferring to their expertise in difficult situations and promoting inclusion by first accepting the systemic exclusion that is ongoing. We elaborate on these suggestions in the following section, Section 6.4. In addition, a restorative workplace culture focuses on learning from incidents/mistakes by soliciting employees' honest accounts without them being concerned about blame (for e.g. blameless postmortems [70]). This is possible in an environment which puts people-first, where a restorative culture has replaced a retributive one accompanied by organizational processes and safeguards that enable it, and hence employees do not work under a fear of retribution. Not only is a restorative culture beneficial for employees but also benefits the organization in both practical and economic ways [145]. Crucially,

the implementation of a restorative justice approach needs to be done in a feminist way as it is important to account for the different ways in which different people are affected (for e.g. due to their racial [216] or gender [257] identity).

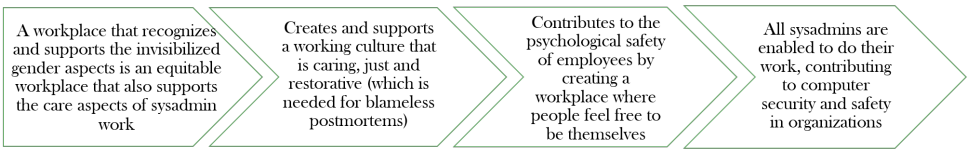


Figure 6.2: From feminism to computer security: equitable workplaces are a prerequisite to just workplaces, which are a precondition to psychologically safe work environments for all employees. This enables people to perform their work without fear of retribution and exclusion, enabling them to do their work and ultimately contributing to positive security outcomes.

A feminist and equitable workplace is one that supports a restorative working culture and hence plays an important part in improving organizational digital security, as visualised in Figure 6.2. While we believe that feminist and equitable workplaces are a pre-condition to improving security outcomes, it is important to reiterate that feminism is driven by social justice and not by organizational outcomes in a capitalist (non-feminist) society. Hence, we develop recommendations for enabling system administration work and environments to move toward being more just and not for improving organizational security. Our recommendations focus on support and equity, and not on prevention, elimination and control of the human factor. Finally, a truly feminist workplace must be created by re-imagining something new and cannot be simply made by reforming existing patriarchal institutions and processes. It is paradoxical to expect existing patriarchal organizations to become more feminist, even if it is in order to improve their own computer security. And if the shift towards more inclusion does occur, is it really feminist if it was driven by capitalist incentives (such as for improving team performance) instead of social justice [106]?

To summarize, a just and caring work environment for sysadmins is one that fosters a restorative culture and strives to be equitable. It recognizes the invisibilized social work and care work aspects as part of sysadmins' work which helps to create a culture of caring. It creates an environment where people feel psychologically safe and do not live under fear of retribution. Such a **people-first work environment is a pre-requisite for creating and supporting computer security** in organizations.

6.4. Recommendations

Recommendations based on the two empirical studies are presented in Sections 4.5.2 and 5.4.2. Building on these, here we present the overall practical recommendations for managers to enable *all* sysadmins to perform their work. We focus on long-lasting

changes in terms of organizational processes and culture. The recommendations focus on supporting sysadmins' work as it is being done in practice, thereby enabling the expertise of the professional. The recommendations do not focus on limiting the human factor and prevention of human errors/security misconfigurations. This is because human error is part of normal operations in a complex sociotechnical system, such as the one in which sysadmins operate. Organizational processes must therefore focus on ensuring safety and security despite human errors and realize instead the invaluable contribution of people of which the errors are only a minuscule part.

The adaption of these recommendations rests on the willingness to change and be uncomfortable. It necessitates the acceptance of ignorance and discrimination that is occurring, reflecting inward into our prejudices and outward at the culture in which we participate. When the problems are organizational, systemic and societal, the solutions must also be implemented at those levels [86]. Individual employees and organizations cannot be expected to simply change while existing within or around unchanging contexts. Individual and community driven efforts must be met with equal traction from high-level legislative bodies to bring about lasting positive change, such as creating workplace cultures that put people first. The current capitalist structures that we live in have however demonstrated that this is a high ask. Keeping in mind the inherent conflict between feminist workplaces in a capitalist society, we develop the following recommendations.

6.4.1. For Managers

1. **Appreciate the scope and importance of sysadmins' work:** In both the empirical studies (Chapters 4 and 5), we asked our participants what their day-to-day system administration work comprised of. In addition to the well-documented technical tasks, we wanted to better understand the lesser known social aspects (explicit and implicit coordination) of system administration work. Both studies highlight the operations-critical and invisible nature of system administration work. We see that the invisibility can lead to it's under-appreciation and -estimation, and how this contributes to negative effects for sysadmins and subsequently, their work.

   It is therefore essential to understand and appreciate the full extent of the work that sysadmins perform so as not to overburden them and have more realistic expectations. It is important to support sysadmins' work processes not only because this work is crucial to continuous operations but also because the social aspects of sysadmins' work, that manifest in the form of coordination, care work, gender considerations, emotional labour etc., need better acknowledgement and support from their work environments.

2. **Identify conflicts between sysadmins' work processes and hierarchical workplaces:** Our empirical studies highlight the social aspects of sysadmins' work. In the interview study (Chapter 4) we find that non-technical helping of others was a significant part of sysadmins' work and in the focus group study (Chapter 5) we identify and describe care work performed by sysadmins. The first study brought to light the invisible nature of sys-

tem administration work, and with the second study we dove deeper into the invisibilized and feminized (care) aspects of system administration work.

The care aspects of system administration work can often be in conflict with the established practices and expectations of an hierarchical (authoritative, heteronormative and patriarchal) workplace. Care work tends to be feminized and is often unseen, unaccounted for, unknown, underappreciated, underestimated and unsupported in such contexts. Care work is often not formally accepted as part of work. It is important therefore to identify these points of conflict and ensure that they don't hinder the work processes of sysadmins and/or take a mental toll on them. Managers must try to resolve them together with the sysadmins in order for sysadmins to continue to effectively do their tasks.

3. **Defer to the expertise of sysadmins, specially in hierarchical settings:** System administration work is sociotechnical in nature involving many (informal) social aspects. This part of sysamdins' work is relatively less understood and less documented in academic literature (Chapter 3), and hence was the focus of our empirical investigation. We find that organizational hierarchical processes, such as micromanagement and strict top-down management, can be detrimental to sysadmins' work processes (Chapter 4), which in turn impact the organizational safety and security as a whole.

   We must defer to their expertise when it comes to their profession. While having processes in place can be helpful in setting guidelines and limits, their enforcement should not become a hindrance in performing system administration work. This can put sysadmins in a predicament where following the protocol might hurt the systems but breaking the protocol might hurt their employment. The harmful consequences of working under such psychologically stressful/unsafe conditions can be felt by not only the sysadmins but the systems they manage and subsequently, the organizations. Deferring to their expertise and supporting their coordination is particularly important during disruptive crisis situations as they are rapidly-evolving, unusual and complex.

4. **Promote a restorative and caring working culture:** Our studies have shown that sysadmins' work is unseen and underestimated but also is brought to light only when something breaks or someone needs help. Sysadmins are often overburdened while trying to ensure continuous and secure system operations behind-the-scenes and often blamed for security misconfigurations that lead to security incidents. In the focus group study (Chapter 5), we identified a self-reinforcing circle that maintains this culture of uncaring and propose that it can be disrupted with care.

   A restorative workplace culture must focus on *learning from mistakes* as opposed to *blaming for mistakes*. Following any incidents, accountability must be found in the form of hearing peoples' accounts regarding what occurred, the events that lead up to it and the conditions that enabled it to happen. The focus should be on learning from the incident, sharing this learning within

the workplace and ensuring that the learning is embedded in organizational memory. Safety and security processes should prioritize human safety above all and then aim to ensure safety despite human mistakes instead of trying to control the behaviour of people.

A caring workplace is one that appreciates the work of sysadmins during everyday operations, and not only when something goes wrong or someone needs help. To acknowledge this work on regular days is to *care for* this work and to take *care of* those doing this work by visibilizing it. The next step then is to support the work processes of *all* sysadmins by identifying how the work environment/processes are inherently unequal and disproportionately affects those in marginalized identities. It is important not to burden the sysadmins themselves to identify such systemic inequalities. We discuss this further in the point below.

5. **Promote inclusion by accepting the exclusion:** We find that gender is not well-accounted for in literature, and in our first empirical study (Chapter 4) we were not able to recruit a gender diverse sample despite our efforts. System administration is currently a men-dominated field and hence sysadmins from other genders are facing obstacles and having to do extra to succeed in this field. In the focus group study (Chapter 5) we found that sysadmins who are not cis men face *double invisibility* - both due to their profession and their gender.

   It is important to ensure that the workplace culture and processes are inclusive, accessible and fair to all those who want to participate. The starting point is to accept the current inequalities and exclusion that is taking place, both with regards to the workers and through workplace cultural norms. It is about addressing these inequalities and creating new equitable processes along with a supportive and empathetic workplace culture. It is the responsibility of the workplaces and those who make the existing majority within the sysadmin community (cis men sysadmins) to foster diversity and inclusiveness by focusing on equity instead of equality. At the organizational level, it is the responsibility to the management to bring in paid experts.

6.4.2. For Sysadmins

The responsibility of visibilizing system administration work and creating inclusive workplace environments should not be on sysadmins. Sysadmins can instead support their work by finding, fostering and maintaining supportive communities. Being part of such a community can help with emotional support and feeling seen among peers (in the workplace or in online communities). While it is not sysadmins' responsibility to fight exclusion, having a supportive community may help in working in cis-men-dominated workplaces and dealing with the pressures that it brings.

In the above recommendations for managers (Section 6.4.1), we have identified some practical starting points for instilling positive and lasting social changes in system administration work environments and culture. For example, in point 3 we recommend that managers identify points of conflict for system administration work

processes in hierarchical workplaces. If sysadmins volunteer their help and inputs, then it is important to seriously consider those and do so in a feminist way. In this example, it would mean to engage with a diverse group to solicit all possible viewpoints and not just of those who constitute the workplace majority/are the loudest.

As another example, in recommendation 4 we advocate for a restorative workplace culture which focuses on accountability after incidents instead for pointing fingers. Accountability takes the form of sharing one's account of what happened, which leads to learning from incidents and creates opportunities for improvement for the organization. This exercise can reveal important social and organizational factors that may have played a role while also appreciating that individual peoples' actions or errors cannot be blamed for organizational incidents. In such a workplace, sysadmins may feel encouraged to share their accounts without fear of blame. In the same point we also recommend to care more for care work and workers. Managers, together with sysadmin who are interested, can identify these (often invisible) social and care aspects of work so as to better support them.

6.5. Limitations

This research took place at TU Delft, the Netherlands and since we recruited through our professional networks, our participants hail largely from European countries. Therefore this project is (unintentionally) centering a European/Western worldview. This is visible also in what we considered to be top conference venues (see Table 3.1) where the papers were mainly sourced from western countries.

The main focus of this PhD is system administration work which currently happens to be a men-dominated profession. In addition, STEM fields (like ours) also continue to be men-dominated. Together, this created a gender imbalance both in terms of the participants and the researchers. In the final focus group project however, we addressed this head-on by creating a gender-diverse research team that engaged with participants belonging to marginalized genders.

In terms of feminist research, this PhD project only scratched the surface. First the literature review highlighted the lack of geographical diversity of the participants in the samples (Section 3.3.5) and then the interview study about COVID-19 impact brought to light the care-work embedded in sysadmins' work (Section 4.5.1). Together these projects were the stepping stones to the final focus group study that embraced the feminist research approach from its inception and followed it through as much as possible.

The focus group study is not perfectly feminist. It still has a Western bias which we tried to mitigate by recruiting from non-European and non-Western countries as much as possible and creating a research team that consisted of researchers from different parts of the world (Section 5.2.1). It is important to highlight this bias and mitigate it because results from such studies cannot directly be generalized to the rest of the world due to differences in ethnicity, culture and value systems. Lastly, this study is not intersectional enough as it does not consider the many different aspects of people's identities that may be affecting their experience at work (such as ability or ethnicity).

6.6. Future Work Directions

1. Our extensive literature review of human factors literature, presented in Chapter 3, highlights the need for stronger theoretical foundations for human factors research in the computer security domain. For future work we recommend moving towards more theoretically founded human factors research that goes beyond technical and design solutions for existing non-technical problems. These studies should focus on expert users, such as system administrators, as their work and behaviour has widespread effects, often on a large-scale.

2. The literature review (Chapter 3) also revealed the different perspectives on 'human errors' in this domain. Studies and organizations often take the 'elimination' perspective where various solutions (both technical and social) are developed for eliminating the human error and influence. Security misconfigurations, however, continue to occur and sysadmins are often the ones to take the fall, specially when security incidents occur. Drawing on lessons from the safety science domain, we suggest that future research should move towards understanding and enabling the human factor instead of eliminating and controlling it.

3. The empirical study, presented in Chapter 4, sheds light on the complex and social nature of sysadmins' work, including care work aspects. This study, together with the literature review in Chapter 3, suggests that there are several overlooked aspects of sysadmins' work which can be comprehended by grounding the qualitative user studies in strong theoretical foundations. Future work should dive deeper into the social aspects of system administration work such as the culture in system administration work environments, how it impacts sysadmins' work processes and ways in which it is (or isn't) just and restorative. Furthermore, such sociotechnical research should use a feminist lens so as to ensure that the knowledge we are creating and the solutions we are proposing are equitable and fair for *all* sysadmins.

4. Our feminist research approach in Chapter 5 is limited as it only took participants' gender into account and not other aspects of their identities. This limits our understanding of the underlying social dynamics and processes. For a more complete understanding, future work therefore must further investigate sysadmins' work with an intersectional lens to determine how different aspects of one's identity (such as ethnicity, class, ability, caste etc.) influences their system administration work.

5. The focus group study, presented in Chapter 5, underscored the connection between technical/technological workplaces and their underlying social/societal processes. As future work, it would be beneficial to employ a technofeminist lens to investigate sysadmins' work so as to identify and describe the interconnections between peoples' various identities and the design and operation of technological infrastructure situated within existing social structures and capitalist frameworks.

7

Conclusions

"Queer and feminist worlds are built through the effort to support those who are not supported because of who they are, what they want, what they do."

Sara Ahmed, Living a Feminist Life (2017)

System administrators perform operations-critical work day after day. However, their work often remains behind-the-scenes and is often brought to light when something breaks, fails or is needed. Due to this, the mainstream research pertaining to system administration work is often solutions-oriented from both technical and design perspectives. A prevalent goal of such research is to limit, control or eliminate the human factors so as to enable positive system security outcomes. Research in other fields however, such as safety science, has shown that such an approach of eliminating the human factor and controlling the behaviour of people does not simply lead to better security or safety. Drawing from these interdisciplinary lessons, we set out to investigate the human factors of system administration work so as to better comprehend what constitutes sysadmins' work and find ways in which we can support sysadmins to do their work.

The research questions for this PhD project are presented in Section 1.4, and the first question is: *"What is the state of knowledge of human factors research in the computer security domain?"* We performed an extensive literature review (detailed in Chapter 3) to answer this research question and identify scientific knowledge gaps. The literature review revealed that computer security literature that focuses on expert users (such as sysadmins) is limited as only 9% of the total papers reviewed were focusing on this group. In addition to revealing a scientific knowledge gap, this is concerning because the behaviour of expert users usually has widespread impact.

We also find that, in the reviewed literature, user studies were largely dominated by a Western (U.S. and Eurocentric) worldview, majority of the user studies did not consider/report the participants' gender and if they did, the participant sample was men-dominated. Furthermore, we see that the majority of the research was not deeply rooted in a theoretical framework, which is essential for qualitative inquiry. The human factors research, specially in expert-user studies, continues to take an elimination perspective which is in contrast with the safety science perspective. Based on these knowledge gaps and insights, we decided to investigate the work of system administration by centering the experiences of sysadmins via interviews and focus groups. We choose different theoretical frameworks to guide our research.

The second research question asks: *"What does the day-to-day work (and coordination) of system administrators look like and how was it impacted by the COVID-19 lockdowns?"* To answer this, we conduct an interview study with 24 sysadmins (detailed in Chapter 4) to better understand their work from their perspective. We find that participants' day-to-day tasks were both technical, such as doing security reviews, and social, like helping users and colleagues. However, the social aspects were reportedly perceived as being more complex than the technical tasks, mainly due to social coordination and its associated time and efforts.

We also find that the day-to-day work of the participants was affected by the COVID-19 lockdown in two main ways: i) An increase in tasks related to supporting users and colleagues (also identified as care work), and; ii) An increase in formal coordination, with associated consequences for the costs of tasks and adaptability to on-going needs as they emerge. We use a model of coordination and communication (co-ladder [44]) and identified coordination processes that were used by sysadmins

to manage their work (overview in Figure 4.3). This helps us to better understand sysadmins' work during a crisis and be better prepared to enable their work when the next crisis arrives.

The third research question is: *"What is the role of personal/individual factors (e.g. gender) in the work of system administrators?"*. In this study (detailed in Chapter 5) we dive deeper into the traditionally-feminized care-work aspects of system administration work, identified in the previous study. We therefore employ a feminist research approach [120] and the lens of gender while engaging with 16 sysadmins via 6 focus groups. The participant pool of this study consisted of sysadmins who are not cis men as we wanted to understand what system administration work looks like for those who belong to marginalized genders in this men-dominated profession.

We find that gender identity plays a significant role in the daily work of the study participants and that they manage their work in several ways in order to continue to work in a cis men dominated field. They do so by being excellent and going above and beyond in system administration tasks, by constantly taking gender considerations in account during social interactions and by finding, fostering and maintaining a supportive community, in the workplace or outside (such as online). We highlight the invisible and undervalued aspects of sysadmins' work, and how the participants' gender compounds these effects even further. These appear in the form of gender inauthenticity (when their gender doesn't match the expected gender for that profession and hence their skills are doubted) and double invisibility (due to their gender identity and due to the profession).

The fourth research question asks: *"In what ways can we enable system administrators' work to be more safe and equitable?"* Our final recommendations (Section 6.4) for system administration work are mainly directed at the managers and those responsible for ensuring good workplaces for sysadmins. The recommendations pertain to appreciation of the extent of the work sysadmins do, identifying the conditions that help sysadmins' to do their work and finding ways to enable these conditions. We recommend to identify conflicts that might exist between sysadmins' work and hierarchical workplaces and, when in doubt, defer to the expertise of sysadmins. We suggest to practice care in the form of acknowledgement of the various unseen aspects of sysadmins' work and in the form of a restorative working culture when faced with mistakes and security events. Finally, we advocate for just work environments because we stand for social justice and also because we find that just and inclusive work environments are an important pre-condition for system security.

For sysadmins, our recommendation is finding and being part of a supportive community in or outside the workplace, specially if they feel that their workplace is not welcoming. This helps as an act of self-preservation but is not at all a substitute for organizational change and just workplaces. The responsibility of creating these spaces is not on the sysadmins we believe, but on the people who constitute the majority these workplaces, the management and the executives.

We consider the main research question which is: **"What are the important human factors that affect system administration work and in what ways can we enable this work?"** We find that social interactions and coordination are central to sysadmins' work and sociotechnical, sociocultural and socioeconomic factors influence the social processes embedded in their work. The sociotechnical factors refer, for example, to the ability of sysadmins' technical tools to support their vital coordination processes. The sociocultural factors are about how the culture of the workplace and organization influences the social processes of sysadmins' work, for instance, the cultural norms around gender, sexuality etc., affect those sysadmins who do not belong to straight cis man identity. The socioeconomic factors come into play because of intersectionality, as the pressures of one's economic status can be intensified if they also belong to other marginalized social groups (such as gender) and this can in turn impact one's opportunities for career advancement.

We find that individual factors, such as gender, very much influence system administration work. Gender identity is socially constructed, and social interactions and coordination are a significant part of system administration work. System administration work therefore, particularly for those who belong to marginalized gender identities (in our context, those who are not cis men), is rife with gender considerations embedded within work processes. In order to enable this work, the first step is to accept that system administration work environments are inherently inequitable and people from different genders are having different experiences and challenges. There is a need for acknowledging the privilege and responsibility of those who constitute the majority in the workplace to take action to shake the status quo to bring about an equitable, just and safe working culture for *all* sysadmins. Our recommendations are presented in detail in Section 6.4.

The main scientific contribution of this PhD project lies a) in the knowledge transfer from the field of safety science to the field of computer security and b) in the qualitative investigation of the work of system administrators via two empirical studies: first, through the lens of coordination (in the context of the COVID-19 lockdown) and second, through the feminist lens of gender. When comparing to prior related work, both these studies make a novel contributions to the scientific literature studying sysadmins' work. The first study does so by **formalizing coordination processes** of sysadmins during a prolonged crisis situation (COVID-19 lockdown) using a theoretical model and identifying the **invisible care work** that is embedded within the work processes. The second study does so by engaging with sysadmins who belong to marginalized genders, and employing a feminist research methodology throughout the study process, where the most remarkable findings were the widespread effects of gender in sysadmins' work. Particularly, we shed light on the phenomenon of **"double invisibility"** which refers to sysadmins belonging to marginalized genders experiencing invisibility at work due to both their job role and their gender.

System administration is a men-dominated field with gender diversity and equity as distant goals. It is the responsibility of the management and the existing sysadmin community to create and sustain a momentum towards achieving this goal. Not only is this important for social justice but also for enabling positive system security outcomes. We believe that inclusive and diverse workplaces that are supportive and understanding of their workers foster a safe and just culture that contributes to computer security in organizations. Creating and maintaining a safe and equitable workplace enables sysadmins to perform their work by reducing the burdens they face due to their gender while coordinating and interacting in such spaces. It is important to note that during times of crises, it becomes that much more important to support these coordination processes in order to ensure continuous (and often vital) system operations. We must strive towards a workplace culture that is safe, just and feminist which ultimately promotes continuous, safe and secure system operations.

Bibliography

[1] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. "Obstacles to the Adoption of Secure Communication Tools". In: *Proceedings of the 38th IEEE Symposium on Security & Privacy (S&P)*. 2017.

[2] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. L. Mazurek, and C. Stransky. "Comparing the Usability of Cryptographic APIs". In: *Proceedings of the 38th IEEE Symposium on Security & Privacy (S&P)*. 2017.

[3] Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek, and C. Stransky. "You Get Where You're Looking for: The Impact of Information Sources on Code Security". In: *Proceedings of the 37th IEEE Symposium on Security & Privacy (S&P)*. 2016.

[4] Y. Acar, C. Stransky, D. Wermke, M. L. Mazurek, and S. Fahl. "Security Developer Studies with Github Users: Exploring a Convenience Sample". In: *Proceedings of the 13th Symposium On Usable Privacy and Security (SOUPS)*. 2017.

[5] A. Adams and A. L. Cox. *Questionnaires, in-depth interviews and focus groups*. Cambridge University Press, 2008.

[6] D. Adams. *A Layman's Introduction to Human Factors in Aircraft Accident and Incident Investigation*. B2006/0094. ATSB, 2006.

[7] D. Adams, A. Bah, C. Barwulor, N. Musaby, K. Pitkin, and E. M. Redmiles. "Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[8] S. Ahmed. *Living a feminist life*. Duke University Press, 2016.

[9] L. C. Aiello. "The multifaceted impact of Ada Lovelace in the digital age". In: *Artificial Intelligence* 235 (2016).

[10] L. Alfrey and F. W. Twine. "Gender-fluid geek girls: Negotiating inequality regimes in the tech industry". In: *Gender & Society* 31.1 (2017).

[11] M. Alvesson and S. Sveningsson. "Good visions, bad micro-management and ugly ambiguity: Contradictions of (non-) leadership in a knowledge-intensive organization". In: *Organization studies* 24.6 (2003).

[12] J. Angulo and M. Ortlieb. ""WTH..!?!" Experiences, Reactions, and Expectations Related to Online Privacy Panic Situations". In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 2015.

[13] H. Assal and S. Chiasson. "Security in the Software Development Lifecycle". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[14] A. J. Aviv and D. Fichter. "Understanding Visual Perceptions of Usability and Security of Android's Graphical Password Pattern". In: *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC)*. 2014.

[15] M. Ayre, J. Mills, and J. Gill. "'Yes, I do belong': the women who stay in engineering". In: *Engineering studies* 5.3 (2013).

[16] M. Bailey. "# transform (ing) DH Writing and Research: An Autoethnography of Digital Humanities and Feminist Ethics." In: *DHQ: Digital Humanities Quarterly* 9.2 (2015).

[17] S. Bardzell. "Feminist HCI: taking stock and outlining an agenda for design". In: *Proceedings of the SIGCHI conference on human factors in computing systems (CHI)*. 2010.

[18] R. Barrett, E. Kandogan, P. P. Maglio, E. M. Haber, L. A. Takayama, and M. Prabaker. "Field studies of computer system administrators: analysis of system management tools and practices". In: *Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW)*. 2004.

[19] L. Bauer, L. F. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. "Real life challenges in access-control management". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2009.

[20] M. Beckerle and L. A. Martucci. "Formal Definitions for Usable Access Control Rule Sets from Goals to Metrics". In: *Proceedings of the 9th Symposium On Usable Privacy and Security (SOUPS)*. 2013.

[21] J. L. Berdahl, M. Cooper, P. Glick, R. W. Livingston, and J. C. Williams. "Work as a masculinity contest". In: *Journal of Social Issues* 74 (2018).

[22] B. Beyer, C. Jones, J. Petoff, and N. R. Murphy. *Site reliability engineering: How Google runs production systems*. O'Reilly Media, Inc., 2016.

[23] R. Bhalerao, V. Hamilton, A. McDonald, E. M. Redmiles, and A. Strohmayer. "Ethical Practices for Security Research with At-Risk Populations". In: *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 2022.

[24] A. Bianchi, J. Corbetta, L. Invernizzi, Y. Fratantonio, C. Kruegel, and G. Vigna. "What the App is That? Deception and Countermeasures in the Android User Interface". In: *Proceedings of the 36th IEEE Symposium on Security & Privacy (S&P)*. 2016.

[25] V. Binkhorst, T. Fiebig, K. Krombholz, W. Pieters, and K. Labunets. "Security at the end of the tunnel: The anatomy of VPN mental models among experts and non-experts in a corporate context". In: *Proceedings of the 31st USENIX Security Symposium (USENIX Security)*. 2022.

[26] P. Bjørn, M. Esbensen, R. E. Jensen, and S. Matthiesen. "Does distance still matter? Revisiting the CSCW fundamentals on distributed collaboration". In: *ACM Transactions on Computer-Human Interaction (TOCHI)* 21.5 (2014).

[27] A. Boin and F. Bynander. "Explaining success and failure in crisis coordination". In: *Geografiska Annaler: Series A, Physical Geography* 97.1 (2015).

[28] I. Boncori, L. M. Sicca, and D. Bizjak. "Transgender and gender non - conforming people in the workplace: Direct and invisible discrimination". In: *Inequality and organizational practice*. 2019.

[29] J. Braithwaite. *Restorative justice*. Routledge London, UK, 2002.

[30] D. Braue. *At least 10m records compromised in single Australian data breach despite drop in NDB reports*. May 16, 2019. URL: https://web.archive.org/save/https://www.csoonline.com/article/3501141/at-least-10m-records-compromised-in-single-australian-data-breach-despite-drop-in-ndb-reports.html (visited on 05/28/2019).

[31] V. Braun and V. Clarke. "Using thematic analysis in psychology". In: *Qualitative Research in Psychology* 3.2 (2006).

[32] V. Braun and V. Clarke. "Reflecting on reflexive thematic analysis". In: *Qualitative research in sport, exercise and health* 11.4 (2019).

[33] V. Braun and V. Clarke. "One size fits all? What counts as quality practice in (reflexive) thematic analysis?" In: *Qualitative research in psychology* 18.3 (2021).

[34] V. Braun and V. Clarke. *Doing Reflexive TA*. URL: https://web.archive.org/save/https://www.thematicanalysis.net/doing-reflexive-ta/ (visited on 08/12/2022).

[35] J. Bundy, M. D. Pfarrer, C. E. Short, and W. T. Coombs. "Crises and crisis management: Integration, interpretation, and research development". In: *Journal of Management* 43.6 (2017).

[36] M. Burgess. "On the theory of system administration". In: *Science of Computer Programming* 49.1-3 (2003).

[37] S. Burnett and N. Feamster. "Encore: Lightweight measurement of web censorship with cross-origin requests". In: *Proceedings of the 2015 ACM conference on special interest group on data communication (SIGCOMM)*. 2015.

[38] J. Burnham. *Accident prone: a history of technology, psychology, and misfits of the machine age*. University of Chicago Press, 2010.

[39] R. da Camara, M. Marinho, S. Sampaio, and S. Cadete. "How do Agile Software Startups deal with uncertainties by Covid-19 pandemic?" In: *arXiv preprint arXiv:2006.13715* (2020).

[40] E. D. Canedo, H. A. Tives, M. B. Marioti, F. Fagundes, and J. A. S. de Cerqueira. "Barriers faced by women in software development projects". In: *Information* 10.10 (2019).

[41] E. A. Cech and T. J. Waidzunas. "Systemic inequalities for LGBTQ professionals in STEM". In: *Science advances* 7.3 (2021).

[42] F. Chanchary and S. Chiasson. "User Perceptions of Sharing, Advertising, and Tracking". In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 2015.

[43] R. Chatterjee, J. Woodage, Y. Pnueli, A. Chowdhury, and T. Ristenpart. "The TypTop System: Personalized Typo-Tolerant Password Checking". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[44] R. Chow, K. Christoffersen, and D. D. Woods. "A model of communication in support of distributed anomaly response and replanning". In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting (HFES)*. 2000.

[45] T. Christensen and L. Ma. "Coordination structures and mechanisms for crisis management in China: Challenges of complexity". In: *Public Organization Review* 20.1 (2020).

[46] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin. ""It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2018.

[47] J. M. Corbin and A. Strauss. "Grounded theory research: Procedures, canons, and evaluative criteria". In: *Qualitative sociology* 13.1 (1990).

[48] K. Crenshaw. "Mapping the margins: Intersectionality, identity politics, and violence against women of color". In: *Stanford Law Review* 43 (1990).

[49] J. W. Creswell and J. D. Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE, 2017.

[50] csrc.nist.gov. *System administrator*. URL: https://web.archive.org/web/20220715165521/https://csrc.nist.gov/glossary/term/system_administrator (visited on 07/08/2022).

[51] J. Czyz, M. J. Luckie, M. Allman, and M. Bailey. "Don't Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy". In: *Proceedings of the 23rd Network and Distributed System Security Symposium (NDSS)*. 2016.

[52] T. A. Daniel. "Friend or Assassin: Whose Side Is HR On, Anyway?" In: *Organizational Toxin Handlers*. 2020.

[53] S. Das, J. Lo, L. Dabbish, and J. I. Hong. "Breaking! A Typology of Security and Privacy News and How It's Shared". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2018.

[54] J. Davis and R. Daniels. *Effective DevOps: building a culture of collaboration, affinity, and tooling at scale*. O'Reilly Media, Inc., 2016.

[55] L. B. De Hertogh, L. Lane, and J. Ouellette. ""Feminist Leanings:" Tracing Technofeminist and Intersectional Practices and Values in Three Decades of Computers and Composition". In: *Computers and Composition* 51 (2019).

[56] A. De Luca, S. Das, M. Ortlieb, I. Ion, and B. Laurie. "Expert and Non-expert Attitudes Towards (Secure) Instant Messaging". In: *Proceedings of the 12th Symposium On Usable Privacy and Security (SOUPS)*. 2016.

[57] S. Dekker. "In the system view of human factors, who is accountable for failure and success?" In: *Proceedings of the Human Factors and Ergonomics Society Europe Chapter Annual Meeting (HFES)*. 2010.

[58] S. Dekker. *Safety differently: Human factors for a new era*. CRC Press, 2014.

[59] S. Dekker. *Just culture: Balancing safety and accountability*. CRC Press, 2016.

[60] S. Dekker. *The field guide to understanding 'human error'*. CRC press, 2017.

[61] S. Dekker. *Just culture: restoring trust and accountability in your organization*. CRC Press, 2018.

[62] S. Dekker. *Foundations of safety science: A century of understanding accidents and disasters*. Routledge, 2019.

[63] S. Dekker, E. Hollnagel, D. Woods, and R. Cook. *Resilience Engineering: New directions for measuring and maintaining safety in complex systems*. Tech. rep. 2008.

[64] S. Dekker and C. Pitzer. "Examining the asymptote in safety progress: a literature review". In: *International Journal of Occupational Safety and Ergonomics* 22.1 (2016).

[65] L. F. DeKoven, A. Randall, A. Mirian, G. Akiwate, A. Blume, L. K. Saul, A. Schulman, G. M. Voelker, and S. Savage. "Measuring Security Practices and How They Impact Security". In: *Proceedings of the 2019 Internet Measurement Conference (IMC)*. 2019.

[66] G. F. Delfino and B. van der Kolk. "Remote working, management control changes and employee responses during the COVID-19 crisis". In: *Accounting, Auditing and Accountability Journal* (2021).

[67] T. Denning, A. Lerner, A. Shostack, and T. Kohno. "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education". In: *Proceedings of the 20th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2013.

[68] E. Derr, S. Bugiel, S. Fahl, Y. Acar, and M. Backes. "Keep Me Updated: An Empirical Study of Third-Party Library Updatability on Android". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[69] D. J. Devine. "A review and integration of classification systems relevant to teams in organizations." In: *Group Dynamics: Theory, Research, and Practice* 6.4 (2002).

[70] C. Dietrich, K. Krombholz, K. Borgolte, and T. Fiebig. "Investigating System Operators' Perspective on Security Misconfigurations". In: *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2018.

[71] D. Dittrich, E. Kenneally, et al. *The Menlo Report: Ethical principles guiding information and communication technology research*. Tech. rep. US Department of Homeland Security, 2012.

[72] L. Doan. “Queer history queer memory: The case of Alan Turing”. In: *GLQ: A Journal of Lesbian and Gay Studies* 23.1 (2017).

[73] S. Dodier-Lazaro, R. Abu-Salma, I. Becker, and M. Sasse. “From paternalistic to user-centred security: Putting users first with value-sensitive design”. In: *Proceedings of the ACM CHI Workshop on Values in Computing*. 2017.

[74] S. B. Edwards and J. Duchess Harris. *Hidden human computers: The Black women of NASA*. ABDO Publishing, 2017.

[75] S. Egelman, L. F. Cranor, and J. Hong. “You’ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings”. In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2008.

[76] S. Egelman and E. Peer. “Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)”. In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2015.

[77] J. Epstein. “A Survey of Vendor Software Assurance Practices”. In: *Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC)*. 2009.

[78] J. A. Espinosa, F. J. Lerch, and R. E. Kraut. “Explicit versus implicit coordination mechanisms and task dependencies: One size does not fit all”. In: *Team cognition: Understanding the factors that drive process and performance*. American Psychological Association, 2004.

[79] M. Fagan and M. M. H. Khan. “Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice”. In: *Proceedings of the 12th Symposium On Usable Privacy and Security (SOUPS)*. 2016.

[80] S. Fahl, Y. Acar, H. Perl, and M. Smith. “Why Eve and Mallory (Also) Love Webmasters: A Study on the Root Causes of SSL Misconfigurations”. In: *Proceedings of the 9th ACM ASIA Conference on Computer and Communications Security (ASIACCS)*. 2014.

[81] S. Fahl, M. Harbach, H. Perl, M. Koetter, and M. Smith. “Rethinking SSL Development in an Appified World”. In: *Proceedings of the 20th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2013.

[82] L. Falsina, Y. Fratantonio, S. Zanero, C. Kruegel, G. Vigna, and F. Maggi. “Grab ’N Run: Secure and Practical Dynamic Code Loading for Android Applications”. In: *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC)*. 2015.

[83] W. Faulkner. “Doing gender in engineering workplace cultures. I. Observations from the field”. In: *Engineering studies* 1.1 (2009).

[84] W. Faulkner. “Doing gender in engineering workplace cultures. II. Gender in/authenticity and the in/visibility paradox”. In: *Engineering Studies* 1.3 (2009).

[85] S. Fenz and A. Ekelhart. "Formalizing Information Security Knowledge". In: *Proceedings of the 4th ACM ASIA Conference on Computer and Communications Security (ASIACCS)*. 2009.

[86] T. Fiebig and D. Aschenbrenner. "13 Propositions on an Internet for a "Burning World"". In: *ACM SIGCOMM 2022 Joint Workshops on "Technologies, Applications, and Uses of a Responsible Internet" and "Building Greener Internet"*. 2022.

[87] M. Fishbein and I. Ajzen. "Belief, attitude, intention, and behavior: An introduction to theory and research". In: *Journal of Business Venturing* (1977).

[88] H. Ford and J. Wajcman. "'Anyone can edit', not everyone does: Wikipedia's infrastructure and the gender gap". In: *Social studies of science* 47.4 (2017).

[89] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle. ""We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products". In: *Proceedings of the 4th Symposium On Usable Privacy and Security (SOUPS)*. 2008.

[90] S. Fowler. *Reflecting On One Very, Very Strange Year At Uber*. Feb. 19, 2017. URL: https://web.archive.org/web/20220715165254/https://www.susanjfowler.com/blog/2017/2/19/reflecting-on-one-very-strange-year-at-uber (visited on 07/15/2022).

[91] J. Frederick and N. Lessin. "Blame the worker". In: *Multinational Monitor* 21.11 (2000).

[92] A. Frik, L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman. "Privacy and security threat models and mitigation strategies of older adults". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS)*. 2019.

[93] K. Gallagher, S. Patil, and N. Memon. "New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network". In: *Proceedings of the 13th Symposium On Usable Privacy and Security (SOUPS)*. 2017.

[94] A. Gamero-Garrido, S. Savage, K. Levchenko, and A. C. Snoeren. "Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[95] X. Gao, Y. Yang, C. Liu, C. Mitropoulos, J. Lindqvist, and A. Oulasvirta. "Forgetting of Passwords: Ecological Theory and Data". In: *Proceedings of the 27th USENIX Security Symposium (USENIX Security)*. 2018.

[96] C. P. García Johnson and K. Otto. "Better together: A model for women and LGBTQ equality in the workplace". In: *Frontiers in Psychology* 10 (2019).

[97] A. Gember-Jacobson, W. Wu, X. Li, A. Akella, and R. Mahajan. "Management Plane Analytics". In: *Proceedings of the 2015 Internet Measurement Conference (IMC)*. 2015.

[98] M. Golla, M. Wei, J. Hainline, L. Filipe, M. Dürmuth, E. M. Redmiles, and B. Ur. "What was that site doing with my Facebook password?: Designing Password-Reuse Notifications". In: *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2018.

[99] P. L. Gorski, L. L. Iacono, D. Wermke, C. Stransky, S. Moeller, Y. Acar, and S. Fahl. "Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic API Misuse". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[100] B. Gough and A. Madill. "Subjectivity in psychological science: From problem to prospect." In: *Psychological methods* 17.3 (2012).

[101] M. R. Grayson. "Cognitive work of hypothesis exploration during anomaly response". In: *Communications of the ACM* 63.4 (2020).

[102] S. Gregor. "The nature of theory in information systems". In: *Management Information Systems quarterly* (2006).

[103] M. Grimley. "Law, morality and secularisation: the Church of England and the Wolfenden Report, 1954–1967". In: *The Journal of Ecclesiastical History* 60.4 (2009).

[104] M. Guarnieri. "Landmarks in the history of safety". In: *Journal of Safety Research* 23.3 (1992).

[105] E. G. Guba, Y. S. Lincoln, et al. "Competing paradigms in qualitative research". In: *Handbook of qualitative research* 2.163-194 (1994).

[106] D. Guillory. "Combating Anti-Blackness in the AI Community". In: *arXiv preprint arXiv:2006.16879* (2020).

[107] E. Haber and E. Kandogan. "Security administrators: A breed apart". In: *Proceedings of the SOUPS Workshop on Usable IT Security Management (USM)*. 2007.

[108] E. M. Haber and J. Bailey. "Design guidelines for system administration tools developed through ethnographic field studies". In: *Proceedings of the ACM Symposium on Computer Human Interaction for the Management of Information Technology (CHIMIT)*. 2007.

[109] E. M. Haber, E. Kandogan, and P. Maglio. "Collaboration in System Administration: For sysadmins, solving problems usually involves collaborating with others. How can we make it more effective?" In: *Queue* 8.12 (2010).

[110] H. Habib, J. Colnago, V. Gopalakrishnan, S. Pearman, J. Thomas, A. Acquisti, N. Christin, and L. F. Cranor. "Away from Prying Eyes: Analyzing Usage and Understanding of Private Browsing". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[111] H. Habib, P. Emami-Naeini, S. Devlin, M. Oates, C. Swoopes, L. Bauer, N. Christin, and L. F. Cranor. "User Behaviors and Attitudes Under Password Expiration Policies". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[112] B. D. Haig, B. D. Haig, and D. Cecco. *Method matters in psychology*. Springer, 2018.

[113] K. F. Hallam. "Moving on from trials and errors: a discussion on the use of a forum as an online focus group in qualitative research". In: *International Journal of Social Research Methodology* (2021).

[114] P. Hamm, D. Harborth, and S. Pape. "A Systematic Analysis of User Evaluations in Security Research". In: *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES)*. 2019.

[115] B. P. Hámornik and C. Krasznay. "A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers". In: *Proceedings of the AHFE International Conference on Human Factors in Cybersecurity*. 2018.

[116] I. M. Handley, E. R. Brown, C. A. Moss-Racusin, and J. L. Smith. "Quality of evidence revealing subtle gender biases in science is in the eye of the beholder". In: *Proceedings of the National Academy of Sciences*. 43. 2015.

[117] J. M. Haney and W. G. Lutters. ""It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[118] J. M. Haney, M. Theofanos, Y. Acar, and S. S. Prettyman. ""We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[119] N. Hänsch, A. Schankin, M. Protsenko, F. Freiling, and Z. Benenson. "Programming Experience Might Not Help in Comprehending Obfuscated Source Code Efficiently". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[120] D. Haraway. "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective1". In: *Women, science, and technology*. 2013.

[121] N. H. Hashim and M. Jones. "Activity Theory: A framework for qualitative analysis". In: *Proceedings of the 4th International Qualitative Research Convention (QRC)*. 2007.

[122] J. Henrich, S. J. Heine, and A. Norenzayan. "Most people are not WEIRD". In: *Nature* 466.7302 (2010).

[123] C. Herley and P. C. Oorschot. "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit". In: *Proceedings of the 38th IEEE Symposium on Security & Privacy (S&P)*. 2017.

[124] A. R. Hevner. "A three cycle view of design science research". In: *Scandinavian journal of information systems* 19.2 (2007).

[125] M. Hiskey. *Before Blaming Hackers, Check Your Configurations*. URL: https://web.archive.org/web/20230504142634/https://www.infosecurity-magazine.com/opinions/blaming-hackers-configurations-1-1-1/ (visited on 05/28/2019).

[126] A. R. Hochschild. "The managed heart: Commercialization of human feeling". In: *The Production of Reality: Essays and Readings on Social Interaction* (2010).

[127] J. Hollan and S. Stornetta. "Beyond being there". In: *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI)*. 1992.

[128] E. Hollnagel, J. Leonhardt, T. Licu, and S. Shorrock. *From Safety-I to Safety-II: A white paper*. 2013.

[129] X. Huang, F. Monrose, and M. K. Reiter. "Amplifying limited expert input to sanitize large network traces". In: *Proceedings of the 41st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 2011.

[130] T. Hupperich, D. Maiorca, M. Kührer, T. Holz, and G. Giacinto. "On the Robustness of Mobile Device Fingerprinting: Can Mobile Users Escape Modern Web-Tracking Mechanisms?" In: *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC)*. 2015.

[131] indeed.com. *How To Avoid Researcher Bias (With Types and Examples)*. Feb. 4, 2023. URL: https://web.archive.org/save/https://www.indeed.com/career-advice/career-development/how-to-avoid-researcher-bias (visited on 05/11/2023).

[132] I. Ion, M. Langheinrich, P. Kumaraguru, and S. Čapkun. "Influence of User Perception, Security Needs, and Social Factors on Device Pairing Method Choices". In: *Proceedings of the 6th Symposium On Usable Privacy and Security (SOUPS)*. 2010.

[133] I. Ion, R. Reeder, and S. Consolvo. ""...No One Can Hack My Mind": Comparing Expert and Non-expert Security Practices". In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 2015.

[134] P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas, and K. Beznosov. "Heuristics for Evaluating IT Security Management Tools". In: *Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS)*. 2011.

[135] P. Jaferian, H. Rashtian, and K. Beznosov. "To Authorize or Not Authorize: Helping Users Review Access Policies in Organizations". In: *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS)*. 2014.

[136] M. Johnson, J. Karat, C.-M. Karat, and K. Grueneberg. "Optimizing a Policy Authoring Framework for Security and Privacy Policies". In: *Proceedings of the 6th Symposium On Usable Privacy and Security (SOUPS)*. 2010.

[137] J. Y. Jung, T. Steinberger, J. L. King, and M. S. Ackerman. "Negotiating Repairedness: How Artifacts Under Repair Become Contingently Stabilized". In: *Proceedings of the ACM on Human-Computer Interaction (CSCW2)*. 2021.

[138] D. Kahn. "Cryptology and the origins of spread spectrum: Engineers during World War II developed an unbreakable scrambler to guarantee secure communications between Allied leaders; actress Hedy Lamarr played a role in the technology". In: *IEEE spectrum* 21.9 (1984).

[139] R. Kaner and E. Frachtenberg. *Experience and Representation of Gender Minorities in Undergraduate Computer Science*. Tech. rep. 2020.

[140] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. ""My Data Just Goes Everywhere": User Mental Models of the Internet and Implications for Privacy and Security". In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 2015.

[141] C. Karlof, J. D. Tygar, and D. Wagner. "Conditioned-safe Ceremonies and a User Study of an Application to Web Authentication". In: *Proceedings of the 5th Symposium On Usable Privacy and Security (SOUPS)*. 2009.

[142] S. Karunakaran, K. Thomas, E. Bursztein, and O. Comanescu. "Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[143] J. Kasperkevic. *HR is not there to be your friend. It's there to protect the company*. Oct. 30, 2017. URL: https://web.archive.org/web/20220714132724/https://www.marketplace.org/2017/10/30/human-resources-protect-employee-employer/ (visited on 07/14/2022).

[144] M. Kaur. "Causes, identification and repair of loss of common ground in coordination in ATM (air traffic management)". Master Thesis. TU Delft, Feb. 2017.

[145] M. Kaur, R. J. De Boer, A. Oates, J. Rafferty, and S. Dekker. "Restorative just culture: a study of the practical and economic effects of implementing restorative justice in an NHS trust". In: *MATEC Web of Conferences*. EDP Sciences. 2019.

[146] M. Kaur, M. van Eeten, M. Janssen, K. Borgolte, and T. Fiebig. "Human Factors in Security Research: Lessons Learned from 2008-2018". In: *arXiv preprint arXiv:2103.13287* (2021).

[147] M. Kaur, S. Parkin, M. Janssen, and T. Fiebig. ""I needed to solve their overwhelmness": How system administration work was affected by COVID-19". In: *25th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW2)*. 2022.

[148] M. Kaur, H. Sri Ramulu, Y. Acar, and T. Fiebig. ""Oh yes! over-preparing for meetings is my jam :)": The Gendered Experiences of System Administrators". In: *26th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW1)* 7 (2023).

[149] M. H. Kiesler and A. George. *Secret communication system*. US Patent 2,292,387. Aug. 1942.

[150] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman. "Systematic literature reviews in software engineering - A systematic literature review". In: *Information and Software Technology* 51.1 (2009).

[151] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall. ""When I Am on Wi-Fi, I Am Fearless": Privacy Concerns & Practices in Eeryday Wi-Fi Use". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2009.

[152] G. Klein, P. J. Feltovich, J. M. Bradshaw, and D. D. Woods. "Common ground and coordination in joint activity". In: *Organizational simulation* 53 (2005).

[153] H. K. Klein and M. D. Myers. "A classification scheme for interpretive research in information systems". In: *Qualitative research in IS: issues and trends*. 2001.

[154] K. M. Kniffin, J. Narayanan, F. Anseel, J. Antonakis, S. P. Ashford, A. B. Bakker, P. Bamberger, H. Bapuji, D. P. Bhave, V. K. Choi, et al. "COVID-19 and the workplace: Implications, issues, and insights for future research and action." In: *American Psychologist* 76.1 (2021).

[155] knowyourmeme.com. *Tree Swing Cartoon Parodies*. Jan. 9, 2013. URL: https://web.archive.org/web/20220708165030/https://knowyourmeme.com/memes/tree-swing-cartoon-parodies (visited on 07/08/2022).

[156] L. Kocksch, M. Korn, A. Poller, and S. Wagenknecht. "Caring for IT security: Accountabilities, moralities, and oscillations in IT security practices". In: *Proceedings of the ACM on Human-Computer Interaction (CSCW)*. 2018.

[157] S. Kraemer and P. Carayon. "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists". In: *Applied ergonomics* 38.2 (2007).

[158] E. Kritzinger and S. H. von Solms. "Cyber security for home users: A new way of protection through awareness enforcement". In: *Computers & Security* 29.8 (2010).

[159] K. Krol, J. M. Spring, S. Parkin, and M. A. Sasse. "Towards robust experimental design for user studies in security and privacy". In: *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016)*. 2016.

[160] K. Krombholz, W. Mayer, M. Schmiedecker, and E. Weippl. ""I Have No Idea What I'm Doing"-On the Usability of Deploying HTTPS". In: *Proceedings of the 26th USENIX Security Symposium (USENIX Security)*. 2017.

[161] J. Kropczynski, R. Ghaiumy Anaraky, M. Akter, A. J. Godfrey, H. Lipford, and P. J. Wisniewski. "Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving". In: *Proceedings of the ACM on Human-Computer Interaction (CSCW2)*. 2021.

[162] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens. "Cyber security in the age of Covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic". In: *Computers & Security* 105 (2021).

[163] E. Lastdrager, I. C. Gallardo, P. Hartel, and M. Junger. "How Effective is Anti-phishing Training for Children?" In: *Proceedings of the 13th Symposium On Usable Privacy and Security (SOUPS)*. 2017.

[164] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner. "Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users". In: *Proceedings of the 39th IEEE Symposium on Security & Privacy (S&P)*. 2018.

[165] A. Levanon, P. England, and P. Allison. "Occupational feminization and pay: Assessing causal dynamics using 1950–2000 US census data". In: *Social forces* 88.2 (2009).

[166] N. Leveson, N. Dulac, K. Marais, and J. Carroll. "Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems". In: *Organization studies* 30.2-3 (2009).

[167] B.-C. Lim and K. J. Klein. "Team mental models and team performance: A field study of the effects of team mental model similarity and accuracy". In: *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior* 27.4 (2006).

[168] T. A. Limoncelli. "Five Nonobvious Remote Work Techniques: Emulating the efficiency of in-person conversations". In: *Queue* 18.3 (2020).

[169] T. A. Limoncelli, C. J. Hogan, and S. R. Chalup. *The Practice of System and Network Administration: Volume 1: DevOps and other Best Practices for Enterprise IT*. Vol. 1. Addison-Wesley Professional, 2016.

[170] T. Limoncelli, S. R. Chalup, and C. J. Hogan. *The Practice of Cloud System Administration: Designing and Operating Large Distributed Systems*. Vol. 2. Pearson Education, 2014.

[171] J. Liu, C. Wang, Y. Chen, and N. Saxena. "VibWrite: Towards Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[172] X. Liu. "The use/less citations in feminist research". In: *Australian Feminist Studies* 36.108 (2021).

[173] macmillandictionary.com. *visibilize*. Mar. 28, 2019. URL: https://web.archive.org/web/20221014131151/https://www.macmillandictionary.com/dictionary/british/visibilize (visited on 10/14/2022).

[174] L. Maestri and R. Wakkary. "Understanding repair as a creative process of everyday design". In: *Proceedings of the 8th ACM Conference on Creativity and Cognition*. 2011.

[175] P. P. Maglio, E. Kandogan, and E. Haber. "Distributed Cognition and Joint Activity in Computer System Administration". In: *Resources, Co-Evolution and Artifacts*. 2008.

[176] L. M. Maguire. "Managing the hidden costs of coordination". In: *Communications of the ACM* 63.4 (2020).

[177] T. W. Malone and K. Crowston. "What is coordination theory and how can it help design cooperative work systems?" In: *Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW)*. 1990.

[178] S. T. March and G. F. Smith. "Design and natural science research on information technology". In: *Decision support systems* 15.4 (1995).

[179] N. Marchant. *The gender gap in science and technology, in numbers*. July 14, 2021. URL: https://web.archive.org/web/20220713183304/https://europeansting.com/2021/07/14/the-gender-gap-in-science-and-technology-in-numbers/ (visited on 07/13/2022).

[180] D. Marti. "From the Editor: The Trouble with the Bastard Operator from Hell". In: *Linux Journal* 2000.80es (2000).

[181] A. Martinez and C. Christnacht. *Women Are Nearly Half of U.S. Workforce but Only 27% of STEM Workers*. Jan. 26, 2021. URL: https://web.archive.org/web/20220713182225/https://www.census.gov/library/stories/2021/01/women-making-gains-in-stem-occupations-but-still-underrepresented.html (visited on 07/13/2022).

[182] A. Mathur, J. Engel, S. Sobti, V. Chang, and M. Chetty. ""They Keep Coming Back Like Zombies": Improving Software Updating Interfaces". In: *Proceedings of the 12th Symposium On Usable Privacy and Security (SOUPS)*. 2016.

[183] A. Mattheis, D. C.-R. De Arellano, and J. B. Yoder. "A model of queer STEM identity in the workplace". In: *Journal of Homosexuality* (2019).

[184] A. M. Mcdonald, R. W. Reeder, P. G. Kelley, and L. F. Cranor. "A Comparative Study of Online Privacy Policies and Formats". In: *Proceedings of the 9th Privacy Enhancing Technologies Symposium (PETS)*. 2009.

[185] N. McDonald, S. Schoenebeck, and A. Forte. "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice". In: *Proceedings of the ACM on Human-Computer Interaction (CSCW)* 3 (2019).

[186] H. McGregor. *Open Access Is a Feminist Issue*. Nov. 6, 2019. URL: http://web.archive.org/web/20220614110500/https://hookandeye.ca/2019/11/06/guest-post-open-access-is-a-feminist-issue/ (visited on 06/14/2022).

[187] S. McLennan and M. Gainer. "When the Computer Wore a Skirt: Langleys Computers, 19351970". In: *NASA History Program Office News & Notes* 29.1 (2012).

[188] I. de Melo-Martín and K. Intemann. "Interpreting evidence: why values can matter as much as science". In: *Perspectives in biology and medicine* 55.1 (2012).

[189] merriam-webster.com. *marginalize, verb.* URL: https://web.archive.org/web/20230515131153/https://www.merriam-webster.com/dictionary/marginalize (visited on 05/15/2023).

[190] N. Merrill and J. Chuang. "From Scanning Brains to Reading Minds: Talking to Engineers About Brain-Computer Interface". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2018.

[191] G. Moane. "Hierarchical systems: Patriarchy and colonialism". In: *Gender and Colonialism*. 1999.

[192] M. Mohamed, N. Sachdeva, M. Georgescu, S. Gao, N. Saxena, C. Zhang, P. Kumaraguru, P. C. van Oorschot, and W.-B. Chen. "A Three-way Investigation of a game-CAPTCHA: Automated Attacks, Relay Attacks and Usability". In: *Proceedings of the 9th ACM ASIA Conference on Computer and Communications Security (ASIACCS)*. 2014.

[193] T. Moore, S. Dynes, and F. R. Chang. "Identifying how firms manage cybersecurity investment". In: *Workshop on the Economics of Information Security (WEIS)* (2016).

[194] D. Morris and D. Cudworth. *Having a secure and safe place to conduct the fieldwork: Further anecdotal tales in pursuit of the elusive doctorate*. Mar. 29, 2019. URL: https://web.archive.org/web/20220714134342/https://www.bera.ac.uk/blog/having-a-secure-and-safe-place-to-conduct-the-fieldwork (visited on 07/14/2022).

[195] A. Mountz, A. Bonds, B. Mansfield, J. Loyd, J. Hyndman, M. Walton-Roberts, R. Basu, R. Whitson, R. Hawkins, T. Hamilton, et al. "For slow scholarship: A feminist politics of resistance through collective action in the neoliberal university". In: *ACME: An International Journal for Critical Geographies* 14.4 (2015).

[196] D. Mu, A. Cuevas, L. Yang, H. Hu, X. Xing, B. Mao, and G. Wang. "Understanding the Reproducibility of Crowd-reported Security Vulnerabilities". In: *Proceedings of the 27th USENIX Security Symposium (USENIX Security)*. 2018.

[197] J. Munday. "The practice of feminist focus groups". In: *Feminist research practice: A primer* (2014).

[198] A. Murillo, A. Kramm, S. Schnorf, and A. De Luca. ""If I Press Delete, It's Gone": User Understanding of Online Data Deletion and Expiration". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[199] M. Muthukrishna and J. Henrich. "A problem in theory". In: *Nature Human Behaviour* 3.3 (2019).

[200] A. Naiakshina, A. Danilova, C. Tiefenau, M. Herzog, S. Dechand, and M. Smith. "Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[201] A. Naiakshina, A. Danilova, C. Tiefenau, and M. Smith. "Deception Task Design in Developer Password Studies: Exploring a Student Sample". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[202] A. Narayanan and B. Zevenbergen. "No encore for encore? ethical questions for web-based censorship measurement". In: *Ethical Questions for Web-Based Censorship Measurement* (2015).

[203] A. A. Neto and M. Vieira. "Towards assessing the security of DBMS configurations". In: *Proceedings of the 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 2008.

[204] A. Neupane, K. Satvat, N. Saxena, D. Stavrinos, and H. J. Bishop. "Do Social Disorders Facilitate Social Engineering?: A Case Study of Autism and Phishing Attacks". In: *Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC)*. 2018.

[205] D. C. Nguyen, D. Wermke, Y. Acar, M. Backes, C. Weir, and S. Fahl. "A Stitch in Time: Supporting Android Developers in WritingSecure Code". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[206] C. Ni, E. Smith, H. Yuan, V. Larivière, and C. R. Sugimoto. "The gendered nature of authorship". In: *Science advances* 7.36 (2021).

[207] nod.org. *How Remote Work Has Made Working Accessible for Millions of People*. Feb. 9, 2022. URL: https://web.archive.org/web/20220713230312/https://www.nod.org/how-remote-work-has-made-working-accessible-for-millions-of-people/ (visited on 07/13/2022).

[208] oaic.gov.au. *Notifiable Data Breaches scheme 12-month insights report*. May 13, 2019. URL: https://web.archive.org/save/https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-scheme-12-month-insights-report (visited on 05/28/2019).

[209] M. Oates, Y. Ahmadullah, A. Marsh, C. Swoopes, S. Zhang, R. Balebako, and L. F. Cranor. "Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration". In: *Proceedings of the 18th Privacy Enhancing Technologies Symposium (PETS)*. 2018.

[210] R. Oldenziel. *Making technology masculine: men, women and modern machines in America, 1870-1945*. Amsterdam University Press, 1999.

[211] D. Oliveira, M. Rosenthal, N. Morin, K.-C. Yeh, J. Cappos, and Y. Zhuang. "It's the Psychology Stupid: How Heuristics Explain Software Vulnerabilities and How Priming Can Illuminate Developer's Blind Spots". In: *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC)*. 2014.

[212] D. S. Oliveira, T. Lin, M. S. Rahman, R. Akefirad, E. Donovan, E. Perez, R. Bobhate, L. A. DeLong, J. Cappos, and Y. Brun. "API Blindspots: Why Experienced Developers Write Vulnerable Code". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[213] J. S. Olson and G. M. Olson. "Bridging Distance: Empirical studies of distributed teams". In: *Human-Computer Interaction and Management Information Systems: Applications. Advances in Management Information Systems*. 2014.

[214] W. J. Orlikowski and J. J. Baroudi. "Studying Information Technology in Organizations: Research Approaches and Assumptions. I Michael D. Myers & David Avison (Red.)" In: *Qualitative Research in Information Systems* (1990).

[215] C. Y. Park, C. Faklaris, S. Zhao, A. Sciuto, L. Dabbish, and J. Hong. "Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[216] A. A. Payne and K. Welch. "Restorative justice in schools: The influence of race on restorative discipline". In: *Youth & Society* 47.4 (2015).

[217] T. C. Peck, L. E. Sockol, and S. M. Hancock. "Mind the gap: The underrepresentation of female participants and authors in virtual reality research". In: *IEEE transactions on visualization and computer graphics* 26.5 (2020).

[218] C. Perrow. *Normal accidents: living with high-risk technologies*. New York, NY, Basic Books, 1984.

[219] E. S. Poole, M. Chetty, T. Morgan, R. E. Grinter, and W. K. Edwards. "Computer help at home: methods and motivations for informal technical support". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2009.

[220] A. van Poortvliet. "Risks, Disasters and Management: A Comparative Study of Three Passenger Transport Systems". PhD thesis. TU Delft, 1999.

[221] I. Pupulidy. *Understanding and Adding to the Investigation Toolbox*. Apr. 22, 2017. URL: /web/20230406150559/https://safetydifferently.com/understanding-and-adding-to-the-investigation-toolbox/ (visited on 04/06/2022).

[222] Y. Qian and W. Fan. "Men and women at work: Occupational gender composition and affective well-being in the United States". In: *Journal of Happiness Studies* 20.7 (2019).

[223] A. B. Raposo, L. P. Magalhães, I. L. M. Ricarte, and H. Fuks. "Coordination of collaborative activities: A framework for the definition of tasks interdependencies". In: *Proceedings of the Seventh IEEE International Workshop on Groupware (CRIWG)*. 2001.

[224] F. Y. Rashid. *Digging Deep into the Verizon DBIR*. May 13, 2019. URL: https://web.archive.org/save/https://duo.com/decipher/digging-deep-into-the-verizon-dbir (visited on 03/27/2023).

[225] Y. Rashidi, T. Ahmed, F. Patel, E. Fath, A. Kapadia, C. Nippert-Eng, and N. M. Su. ""You Don't Want to Be the Next Meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[226] J. Reason. "Achieving a safe culture: theory and practice". In: *Work & Stress* 12.3 (1998).

[227] E. M. Redmiles, Y. Acar, S. Fahl, and M. L. Mazurek. *A summary of survey methodology best practices for security and privacy researchers*. Tech. rep. 2017.

[228] E. M. Redmiles, S. Kross, and M. L. Mazurek. "How well do my results generalize? Comparing security and privacy survey results from mturk, web, and telephone samples". In: *Proceedings of the 40th IEEE Symposium on Security & Privacy (S&P)*. 2019.

[229] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. "I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security". In: *Proceedings of the 37th IEEE Symposium on Security & Privacy (S&P)*. 2016.

[230] E. M. Redmiles, Z. Zhu, S. Kross, D. Kuchhal, T. Dumitras, and M. L. Mazurek. "Asking for a Friend: Evaluating Response Biases in Security User Studies". In: *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2018.

[231] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman. "An Experience Sampling Study of User Reactions to Browser Warnings in the Field". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2018.

[232] L. Reinfelder, R. Landwirth, and Z. Benenson. "Security managers are not the enemy either". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2019.

[233] P. Rheingans, E. D'Eramo, C. Diaz-Espinoza, and D. Ireland. "A model for increasing gender diversity in Technology". In: *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE)*. 2018.

[234] T. Riebe, M.-A. Kaufhold, and C. Reuter. "The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study". In: *Proceedings of the ACM on Human-Computer Interaction (CSCW2)*. 2021.

[235] S. Ruoti, N. Kim, B. Burgon, T. van der Horst, and K. Seamons. "Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes". In: *Proceedings of the 9th Symposium On Usable Privacy and Security (SOUPS)*. 2013.

[236] S. Ruoti, T. Monson, J. Wu, D. Zappala, and K. Seamons. "Weighing Context and Trade-offs: How Suburban Adults Selected Their Online Security Posture". In: *Proceedings of the 13th Symposium On Usable Privacy and Security (SOUPS)*. 2017.

[237] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon. "Biometric-rich Gestures: A Novel Approach to Authentication on Multi-touch Devices". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2012.

[238] E. Salas, C. Prince, D. P. Baker, and L. Shrestha. "Situation awareness in team performance: Implications for measurement and training". In: *Human Factors* 37.1 (1995).

[239] N. Sambasivan, G. Checkley, A. Batool, N. Ahmed, D. Nemer, L. S. Gaytán-Lugo, T. Matthews, S. Consolvo, and E. Churchil. ""Privacy is Not for Me, It's for Those Rich Women": Performative Privacy Practices on Mobile Phones by Women in South Asia". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

[240] M. Schwarz, M. Lipp, and D. Gruss. "JavaScript Zero: Real JavaScript and Zero Side-Channel Attacks". In: *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS)*. 2018.

[241] U. Sekaran and R. Bougie. *Research methods for business: A skill building approach*. John Wiley & Sons, 2016.

[242] S. Shah. *7 Biases to avoid in qualitative research*. Jan. 3, 2019. URL: https://web.archive.org/save/https://www.editage.com/insights/7-biases-to-avoid-in-qualitative-research (visited on 05/11/2023).

[243] A. Shell-Gellasch. "Improbable Warriors: Women Scientists and the US Navy in World War II". In: *Mathematics and computer education* 36.3 (2002).

[244] D. Shin and R. Lopes. "An Empirical Study of Visual Security Cues to Prevent the SSLstripping Attack". In: *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC)*. 2011.

[245] M. Shirvanian and N. Saxena. "CCCP: Closed Caption Crypto Phones to Resist MITM Attacks, Human Errors and Click-Through". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[246] S. Silva and M. Kenney. “Algorithms, platforms, and ethnic bias”. In: *Communications of the ACM* 62.11 (2019).

[247] L. Simko, L. Zettlemoyer, and T. Kohno. “Recognizing and Imitating Programmer Style: Adversaries in Program Authorship Attribution”. In: *Proceedings of the 18th Privacy Enhancing Technologies Symposium (PETS)*. 2018.

[248] M. W. Skirpan, T. Yeh, and C. Fiesler. “What’s at Stake: Characterizing Risk Perceptions of Emerging Technologies”. In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2018.

[249] J. Slupska, S. D. Duckworth, L. Ma, and G. Neff. “Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity”. In: *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 2021.

[250] C. Smith. *The hidden history of Bletchley Park: A social and organisational history, 1939–1945*. Springer, 2015.

[251] M. Smith. “The Wrens of Bletchley Park”. In: *XRDS: Crossroads, The ACM Magazine for Students* 21.3 (2015).

[252] J. Smithson. “Focus groups”. In: *The Sage handbook of social research methods* 357 (2008).

[253] C. R. de Souza, C. S. Pinhanez, and V. F. Cavalcante. “Information needs of system administrators in information technology service factories”. In: *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT)*. 2011.

[254] K. Spiel. ““Why are they all obsessed with Gender?”—(Non) binary Navigations through Technological Infrastructures”. In: *Designing Interactive Systems Conference (DIS)*. 2021.

[255] C. Stanworth. “Women and work in the information age”. In: *Gender, Work & Organization* 7.1 (2000).

[256] B. Stock, G. Pellegrino, F. Li, M. Backes, and C. Rossow. “Didn?t You Hear Me? – Towards More Successful Web Vulnerability Notifications”. In: *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS)*. 2018.

[257] J. Stubbs. “Domestic violence and women’s safety: Feminist challenges to restorative justice”. In: *Restorative justice and family violence* (2002).

[258] S. Stumpf, A. Peters, S. Bardzell, M. Burnett, D. Busse, J. Cauchard, E. Churchill, et al. “Gender-inclusive HCI research and design: A conceptual review”. In: *Foundations and Trends® in Human–Computer Interaction* 13.1 (2020).

[259] R. Suddaby. “From the editors: What grounded theory is not”. In: *Academy of Management Journal* 49.4 (2006).

[260] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan. "A Human Capital Model for Mitigating Security Analyst Burnout". In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 2015.

[261] S. C. Sundaramurthy, J. McHugh, X. Ou, M. Wesch, A. G. Bardas, and S. R. Rajagopalan. "Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations". In: *Proceedings of the 12th Symposium On Usable Privacy and Security (SOUPS)*. 2016.

[262] P. Swuste, C. van Gulijk, and W. Zwaard. "Safety metaphors and theories, a review of the occupational safety literature of the US, UK and The Netherlands, till the first part of the 20^{th} century". In: *Safety science* 48.8 (2010).

[263] M. Tahaei and K. Vaniea. "A Survey on Developer-Centred Security". In: *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 2019.

[264] J. Tamarit and E. Luque. "Can restorative justice satisfy victims' needs? Evaluation of the Catalan victim–offender mediation programme". In: *Restorative Justice* 4.1 (2016).

[265] L. M. Tanczer. "Hacktivism and the male-only stereotype". In: *New Media & Society* 18.8 (2016).

[266] F. W. Taylor. *The principles of scientific management*. New York: Harper & Brothers, 1911.

[267] L. Thomas. "Actress Hedy Lamarr, Inventor: A Public Image Reframed". PhD thesis. University of Saskatchewan, 2022.

[268] T. W. Thomas, M. Tabassum, B. Chu, and H. Lipford. "Security During Application Development: An Application Security Expert Perspective". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2018.

[269] S. R. C. Thomas A. Limoncelli Christina J. Hogan. *The Practice of System and Network Administration: Volume 1: DevOps and other Best Practices for Enterprise IT (3rd Edition)*. Addison-Wesley, 2017.

[270] Y. Tian, N. Zhang, Y.-H. Lin, X. Wang, B. Ur, X. Guo, and P. Tague. "Smartauth: User-centered Authorization for the Internet of Things". In: *Proceedings of the 26th USENIX Security Symposium (USENIX Security)*. 2017.

[271] C. Tiefenau, M. Häring, K. Krombholz, and E. von Zezschwitz. "Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators". In: *Symposium on Usable Privacy and Security (SOUPS)*. 2020.

[272] M. Tischer, Z. Durumeric, F. Sam, S. Duan, A. Mori, E. Bursztein, and M. Bailey. "Users Really Do Plug in USB Drives They Find". In: *Proceedings of the 37th IEEE Symposium on Security & Privacy (S&P)*. 2016.

[273] D. Todd. *Top 10 Data Breaches of All Time*. Mar. 4, 2022. URL: http://web.archive.org/web/20220516152124/https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time (visited on 05/16/2022).

[274] S. Travaglia. *Bastard Operator from Hell*. Plan Nine Publishing, 2001.

[275] E. Tseng, M. Sabet, R. Bellini, H. K. Sodhi, T. Ristenpart, and N. Dell. "Care Infrastructures for Digital Security in Intimate Partner Violence". In: *CHI Conference on Human Factors in Computing Systems*. 2022.

[276] J. Ubacht. "A Conceptual Framework for Regulatory Practice in Mobile Telecommunications Systems". PhD thesis. TU Delft, 2020.

[277] Unknown. *What the Client Wants*. URL: https://web.archive.org/web/20220708162603/https://lawprofessors.typepad.com/.a/6a00d8341bfae553ef0168e74326d5970c-500wi (visited on 07/08/2022).

[278] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. ""I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab". In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 2015.

[279] utwente.nl. *Communication Theories*. 2003–2004. URL: https://web.archive.org/save/https://www.utwente.nl/en/bms/communication-theories/ (visited on 03/27/2023).

[280] A. H. Van de Ven. "Nothing is quite so practical as a good theory". In: *Academy of management Review* 14.4 (1989).

[281] B. Van der Klaauw and A. Dias da Silva. "Wage dynamics and promotions inside and between firms". In: *Journal of Population Economics* 24.4 (2011).

[282] N. F. Velasquez and S. P. Weisband. "System administrators as broker technicians". In: *Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology (CHIMIT)*. 2009.

[283] M. Vining. "Women Join the Armed Forces: The Transformation of Women's Military Work in World War II and After (1939–1947)". In: *A Companion to Women's Military History*. 2012.

[284] M. Vizard. *McAfee Survey Finds IT at Cybersecurity Fault Most*. May 3, 2019. URL: https://web.archive.org/save/https://securityboulevard.com/2019/05/mcafee-survey-finds-it-at-cybersecurity-fault-most/ (visited on 05/28/2019).

[285] R. H. Von Alan, S. T. March, J. Park, and S. Ram. "Design science in information systems research". In: *MIS quarterly* 28.1 (2004).

[286] D. Votipka, R. Stevens, E. M. Redmiles, J. Hu, and M. L. Mazurek. "Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes". In: *Proceedings of the 39th IEEE Symposium on Security & Privacy (S&P)*. 2018.

[287] K. Vredenburg, J.-Y. Mao, P. W. Smith, and T. Carey. "A survey of user-centered design practice". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2002.

[288] J. Wajcman. “From women and technology to gendered technoscience”. In: *Information, Community and Society* 10.3 (2007).

[289] R. Wash, E. Rader, K. Vaniea, and M. Rizor. “Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences”. In: *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS)*. 2014.

[290] K. E. Weick. “Organizational culture as a source of high reliability”. In: *California management review* 29.2 (1987).

[291] K. E. Weick. *Sensemaking in organizations*. Vol. 3. SAGE, 1995.

[292] R. Werlinger, K. Hawkey, K. Muldner, P. Jaferian, and K. Beznosov. “The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?” In: *Proceedings of the 4th Symposium On Usable Privacy and Security (SOUPS)*. 2008.

[293] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov. “Preparation, detection, and analysis: the diagnostic work of IT security incident response”. In: *Information Management & Computer Security* (2010).

[294] D. Wermke, N. Huaman, Y. Acar, B. Reaves, P. Traynor, and S. Fahl. “A Large Scale Investigation of Obfuscation Use in Google Play”. In: *Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC)*. 2018.

[295] C. West and D. H. Zimmerman. “Doing gender”. In: *Gender & society* 1.2 (1987).

[296] M. West, R. Kraut, and H. Ei Chew. *I’d blush if I could: closing gender divides in digital skills through education*. 2019.

[297] R. D. White Jr. “The micromanagement disease: Symptoms, diagnosis, and cure”. In: *Public Personnel Management* 39.1 (2010).

[298] A. Whitten and J. D. Tygar. “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.” In: *Proceedings of the 8th USENIX Security Symposium (USENIX Security)*. 1999.

[299] who.int. *WHO Director-General’s opening remarks at the media briefing on COVID-19*. Mar. 11, 2022. URL: https://web.archive.org/save/https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 (visited on 04/05/2022).

[300] S. Wilkinson. “Focus groups: A feminist method”. In: *Psychology of women quarterly* 23.2 (1999).

[301] J. Wolbers, K. Boersma, and P. Groenewegen. “Introducing a fragmentation perspective on coordination in crisis management”. In: *Organization Studies* 39.11 (2018).

[302] C. C. Wood and W. W. Banks Jr. “Human error: an overlooked but significant information security problem”. In: *Computers & Security* 12.1 (1993).

[303] wrens.org.uk. *Post-war WRNS*. URL: https://web.archive.org/web/20220715164230/https://wrens.org.uk/about-us/history/ (visited on 06/07/2022).

[304] S. Xiao, C. Cheshire, and N. Salehi. "Sensemaking, support, safety, retribution, transformation: A restorative justice approach to understanding adolescents' needs for addressing online harm". In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 2022.

[305] J. Xie, H. Lipford, and B.-T. Chu. "Evaluating Interactive Support for Secure Programming". In: *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2012.

[306] K. Yakdan, S. Dechand, E. Gerhards-Padilla, and M. Smith. "Helping Johnny to Analyze Malware: A Usability-Optimized Decompiler and Malware Analysis User Study". In: *Proceedings of the 37th IEEE Symposium on Security & Privacy (S&P)*. 2016.

[307] J. B. Yoder and A. Mattheis. "Queer in STEM: Workplace experiences reported in a national survey of LGBTQA individuals in science, technology, engineering, and mathematics careers". In: *Journal of homosexuality* 63.1 (2016).

[308] A. Zanutto, B. Shreeve, K. Follis, J. Busby, and A. Rashid. "The Shadow Warriors: In the no man's land between industrial control systems and enterprise IT systems". In: *Proceedings of the 13th Symposium On Usable Privacy and Security (SOUPS)*. 2017.

[309] L. Zhang, S. Tan, and J. Yang. "Hearing Your Voice is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[310] F. Zhu, S. Carpenter, A. Kulkarni, and S. Kolimi. "Reciprocity Attacks". In: *Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS)*. 2011.

[311] V. Zimmermann and K. Renaud. "Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset". In: *International Journal of Human-Computer Studies* 131 (2019).

[312] Y. Zou, A. H. Mhaidli, A. McCall, and F. Schaub. ""I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions After the Equifax Data Breach". In: *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*. 2018.

A

Appendix for Chapter 4

A.1. Informed Consent Form

The consent form was sent to the participants before the interview and the participants were asked if they have any questions regarding this prior to recording the interview as well.

Taking part in the study

1. I have read and understood the study information dated DD/MM/YYYY, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.
2. I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.
3. I understand that taking part in the study involves one-on-one recorded interviews accompanied with written notes, remotely conducted. The recording will be transcribed and will be stored without any personally identifiable information.

Use of the information in the study

1. I understand that information I provide will be used for academic reports and scientific publications.
2. I understand that personal information collected about me that can identify me, such as e.g. my name or workplace, will not be shared beyond the study team.
3. I agree that, with my approval, my information can be anonymously quoted in research outputs.

A

A.2. Interview Questions

Interview questions were read out to the participants and were displayed on the screen during the interview.

1. Can you describe a normal work day in the past 1-2 weeks?
   - number of tasks
   - nature of tasks
   - prioritization of tasks
2. Can you describe a normal work day in the last weeks of March 2020?
   - number of tasks
   - nature of tasks
   - prioritization of tasks
3. Can you describe a normal work day in February 2020 (before the lockdown)?
   - number of tasks
   - nature of tasks
   - prioritization of tasks
4. Did any of your routine tasks like patching, backups, reviews etc. change since mid-March (or before)?
5. Do you have an opinion about how these changes in your work may have impacted the security of systems?

A.3. Recruitment Flyer

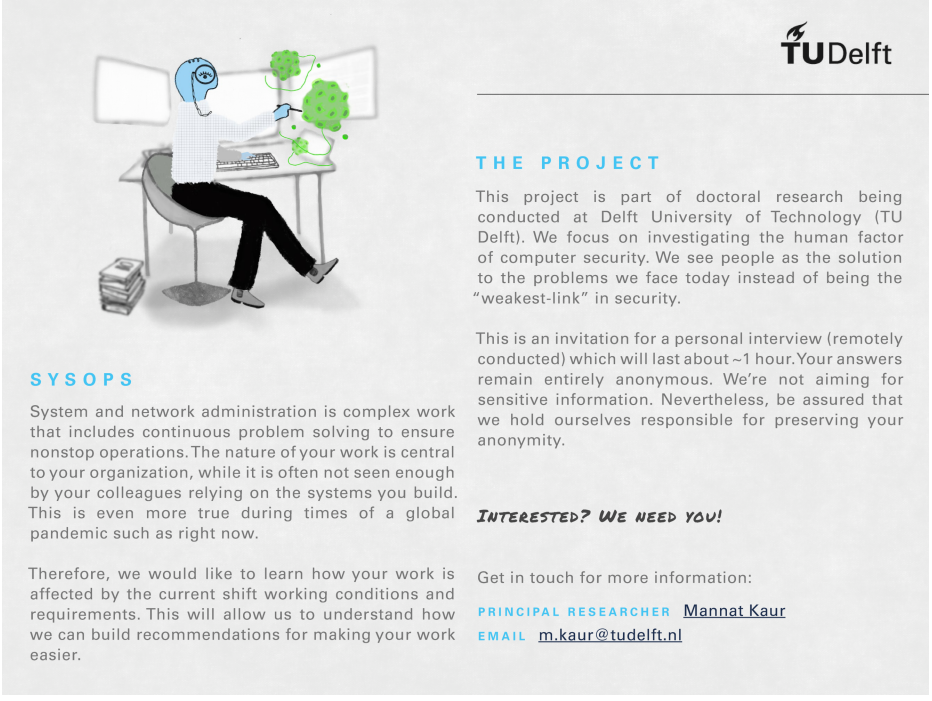


Figure A.1: Flyer for participant recruitment

A.4. Codebook

	Operational		Interactions		Characteristics		Prioritization	
Sysadmin Tasks	Maintenance	10	w/ Colleagues	35	Used to remote working	15	Impact on the user	30
	All is working	6	w/ Users	19	Working odd hours	9	"I decide"	10
	Improvement	5	w/ Vendors	6	Working fast	4	Deadlines	10
	Configuration	4	w/ Other departments	4	Changes day-to-day	3	Incidents/security	5
	Development	4			Unplanned work	2	Requests from others	15
	Security	3						
	Managing clusters	3						
	Monitoring	2						
	Implementing projects	2						

	WFH Effects		As Part of Work		Security		In-Person	
Social Interactions	Informal interactions difficult	17	Affects work	7	Impact of office setting	2	More effective	6
	More coordination needed	5	Not work related	6			Fewer meetings	2
	Interactions more work-focused	3	Miss the social aspects	5				
	More communication	5						
	Learning patience	5						
	Lack of informal interactions lowers work effectiveness	2						
	Async communication is more effective	2						

	Routine Tasks		Immediate Effects		Other Effects		Challenges	
Lockdown Effects	More planning	8	more tasks/work done	20	WFH necessitates process	4	Delays	8
	Takes longer to do reviews	2	Helping others	7	Strictly enforcing pre-existing regulation	4	Capacity issues	5
	Takes longer for driver updates	1	More time available	6	Increase in knowledge documentation	5	Hard to stop working when WFH	4
	Takes longer to patch	1	New daily meetings	6	Work driven by processes, not informal conversations	3		
	Security reviews moved online	1	Coordination is difficult	4	More time taken to finish tasks	3		
	Change in security maintenance	1	Less work	3	Accelerating existing projects	2		
	Cannot deploy new software	1	Budget cuts / layoffs	2	More use of existing resources	2		
	Backup tapes changed weekly instead of daily	1	National security concerns	2	Change in the kind of user requests	6		
			Change freeze	2	Can research/study when WFH	2		
			Ensure security	1	Less micro-management	3		
			Change in policy	1	Fewer constraints from users	2		
					Increase in working outside office time	2		
					Negative health effects	2		
					More work due to more time	2		
					Higher productivity	2		

	Lockdown Effects		Perception		Practices	
Security	Unaffected	13	Management's perspective	6	Reactive security	4
	Increased security awareness	9	Influenced by media	3	Compromise	3
	Increased security communication	7			Redundancy	4
	More concerns from users	4			Automation	4
	More concerns from management	3			ITIL based	2
	Normalized talking about security	2				
	Increased awareness of rules	2				
	Use of more online tools	7				
	Use of private hardware and network by users	5				
	New attack vectors	3				
	Increase in COVID-19 related scams	4				
	Improved security	5				
	Decreased security	3				

Table A.1: Overview of the codebook

B

Appendix for Chapter 5

B.1. Informed Consent Form

We supplemented the informed consent form with the code of conduct (see Appendix B.5) for the study and a brief project description (see Appendix B.2). We also solicited participants' information in this form: job title, job sector, job country, years of experience and gender. We shared the consent form with the participants when they expressed interest in participating and asked for further information about the study. The participants had to choose a yes or no box for each of the items listed below and sign the consent form.

Taking part in the study

1. I have read and understood the study information (in this form) dated DD/MM/YYYY, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.
2. I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.
3. I have read the 'code of conduct for the focus group' (next page) dated DD/MM/YYYY or it has been read to me. I have been able to ask questions and my questions have been answered to my satisfaction.
4. I understand that taking part in the study involves participating in three focus groups via texts which will be recorded.

Use of the information in the study

1. I understand that information I provide will be used for scientific reports and publications.

2. I understand that personal information collected about me that can identify me, such as my name, email or gender, will not be shared beyond the study team.

3. I understand that I can request access to and rectification or erasure of my personal data.

4. I agree that my information (such as the text messages) will be anonymously stored for analysis and can be anonymously quoted in research outputs.

Future use and reuse of the information by others

I understand that once the research project is over (estimated end date DD/MM/YYYY), all my information (personal and anonymized) will be deleted within 1 month after the project and only aggregated metadata will be archived.

B.2. Project Description in the Consent Form

The issue: STEM fields continue to be dominated by cis men (and a masculine culture) and people of other genders commonly face barriers to enter and remain in the field. Similarly in the field of system and network administration, gender diversity remains a goal with a long way to go and most existing scientific literature does not take gender into account.

Our study: We aim to address this knowledge gap by engaging with a group of sysadmins who are not cis men. Through an online focus group we will gather your experiences and views in regards to your system administration work. Our findings will highlight the diverse perspectives in the sysadmin community. These are important for moving towards a more gender-inclusive and just work environment within the field.

Your participation: You will participate in one online focus group meeting which will take place on a self-hosted web-based IRC service and will last about 90 minutes. These meetings will be scheduled in consultation with you and the other participants. Each meeting will contain 3-4 participants. We will do our best to ensure that your anonymity is maintained when participating in these meetings, throughout and after the research process.

Researchers: The focus groups will be facilitated by one PhD researcher (myself). I am interested in feminist research approaches and am investigating the human aspects of system operations. A second PhD researcher will assist.

(We included the names and affiliations of all the author in the consent forms).

B.3. Interview Protocol

First, the code of conduct (see Appendix B.5) was shared in the group chat. Next we introduced the facilitators using our names and pronouns and asked the participants to introduce themselves without names by sharing

- brief description of your day-to-day work,
- your work experience in years and
- gender distribution of the team within which you work.

We then encouraged the participants interact with each other during the focus group (for example, by agreeing or adding to each other's comments) by explaining that it would be helpful for the research if we build on each other's experiences and have discussions. The focus groups lasted 90 minutes and we planned to spend around 30 minutes per each **main question**. The list of sub-questions accompanying each main question helped us navigate the group discussions without straying too far from our research topic.

1. **What do you find easy to do in your work? And why?**
   - What do you feel enabled to do?
   - What enables you?
   - (if gender not mentioned) What is the easiest part of your work considering you work in a cis-men dominated field?
   - What social, organizational or environmental factors enable you to do your work?
   - What made you work and stay in this field/job? What makes you feel welcome?
2. **What do you find difficult to do in your work? And why?**
   - Examples of the kind of difficulties?
   - Why do you think these obstacles exist? Your reasoning?
   - (if gender not mentioned) Do you face any obstacles considering you work in a cis-men-dominated field?
   - (if gender not mentioned) Have you had any negative experiences considering you work in a cis-men-dominated field?
   - How do these obstacles affect your work?
3. **How do you overcome the difficulties you face at work?**
   - What social, organizational or environmental factors help you to overcome obstacles you face in your work?
   - What help (if any) do your get from your workplace?
   - (if gender not mentioned) Are there any measures in place to address your needs at work considering you work in a cis-men-dominated field?
   - What would you do/change to make your work better (for a more just and inclusive workplace)?

In the end, we thanked the participants for sharing their experiences and volunteering their time. We invited them to share any final comments and reminded them that the chat forum was open for the next two weeks in case they thought of adding any more comments.

B.4. Image Shared by a Participant During Focus Group 4

The following image was shared by Participant P9 to illustrate what it is like to coordinate with several stakeholders and to *"get them all to the same picture"*

(P9). Interestingly, variations of this image have been around since 1970s [155] in reference to the project management culture in the IT domain commenting on intra-organizational and inter-departmental communication, and client interactions.

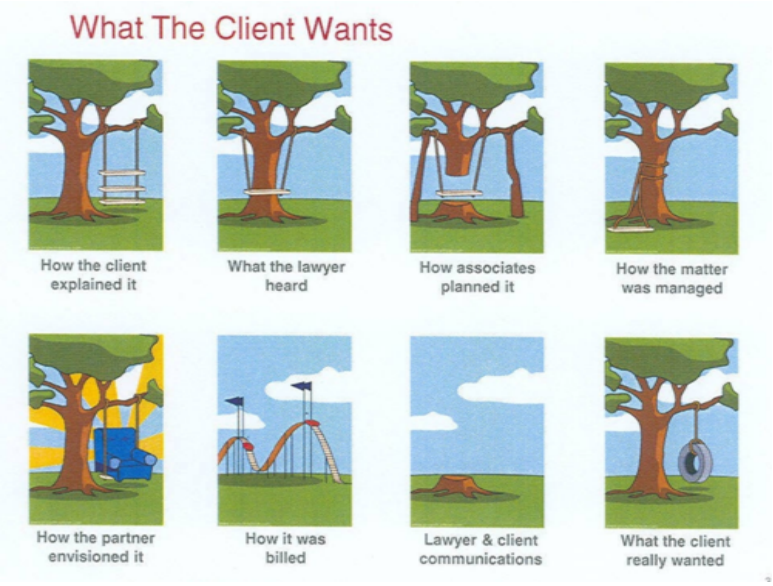


Figure B.1: Image shared to illustrate the experience of working with several stakeholders [277]

B.5. The Code of Conduct

1. The topic will be revealed during the focus group meeting.
2. One PhD researcher acts as a neutral facilitator and a second PhD researcher assists.
3. You can respond directly to the discussion topic and to other participants' messages. You can also respond in the group chat after the meeting in case you think of something later (in the next 2 weeks).
4. You can ignore a question if you do not feel comfortable in responding.
5. You can leave the group if you feel uncomfortable or do not wish to participate anymore.
6. We reserve the right to remove anyone from the group in case of the following:
   (a) Disrespectful communication towards others in the group
   (b) Verbal or written abuse towards others in the group
   (c) Bullying or intimidation
   (d) Harassment or discrimination (gender, racial, sexual etc.)

B.6. Codebook

Nature of Work							
Team gender distribution	16	Fulfill many roles	5	Difficulties of tech/startup culture	2	Engaging with users is key	
Technical work is easy/easier	12	Coordination related tasks in sysadmin work	4	Communication with users is easy	2	Easier to work with younger people	
Socializing with cis men	12	Less women in sysadmining (vs. UX/UI, dev, webdesign)	4	Flat hierachies lead to autonomy in sysadmin work		Experience makes sysadmin work easy	
Gender affects sysadmin work	8	Sysadmin processes ignored by organization	3	Sysadmin work can be lonely		Self-taught sysadmin	
Support tasks in sysadmin work	7	Hierachy in sysadmin work: Hard to say no to seniors	3	Dealing with many stakeholders		Changing jobs may often contribute to unchanging workplace conditions	
Sysadmin work job description	6	Flat hierachies enable sysadmin work	2				
Care Aspects							
(Lack of) community support in the workpalce	19	(Lack of) care culture in IT	4	Identity and empathy	3	Empathy and user communication	
Visibility Aspects: *Gender Visibility Impact*							
Strategies to cope with sexism	22	Negative effects on health	7	Strategies to overcome gender bias at work	3	Less gender in remote work	
Sexism in the workplace	12	Coping strategies affect sysadmin work	6	Takes longer to do tasks	3	Less socializing in remote work	
Lack of respect due to gender	12	Involuntary trail-blazer	4	Not wanting to ask for accomodations	2	(in) effectiveness of coping	
Having to do extra due to gender	11	(Negative) effects of extra work	4	Gender and social skills	2	Misgendering non-men sysadmins	
Having to prove oneself to others	10	Power of choosing where to work	3	Hard to speak up about needs			
Visibility Aspects: *Invisibility in Sysadmin Work*							
Experience provides visibility	2	Sysadmin work s undermined					
Routine Tasks							
Workplace better than others	7	Why stay in a men-dominated field	6	Space for low motivation in a fast-paced productivity culture	2	Performative inclusion in the workplace	
Process for gender equity	6	Just culture	2				

Table B.1: Overview of the codebook

Curriculum Vitæ

Mannat Kaur

Bio

Mannat is currently a postdoctoral researcher at the Max Plank Institute for Informatics (MPI-INF) in the Internet Architecture (INET) group, combining quantitative internet measurement data with qualitative feminist perspectives. Mannat's primary interest lies in comprehending the ways in which inequities manifest in digital infrastructures and in the work environments of those who manage these digital infrastructures. Mannat's research aims to understand these social dynamics, their impact, and their connection to workplace culture and organizational security in order to find ways to move towards more equitable sociotechnical realities.

Mannat holds a Bachelor's degree in Mechanical Engineering and a Master's degree in Aerospace Engineering. During their master thesis work, they gravitated towards understanding and analyzing human interaction in the context of sociotechnical system safety. They mathematically modelled & simulated an aviation accident using agent-based frameworks to better understand the coordination between agents, humans or otherwise. Through a variability analysis, they showed the ineffectiveness of the "human error" perspective. They grew curious about the critical role played by people in ensuring the safety and security of essential systems.

Their PhD research provided an opportunity to investigate this further and, together with their supervisor Dr.-Ing. Tobias Fiebig and promoter Prof. dr. ir. Marijn Janssen, they delved deeper into the experiences of the people (sysadmins) who ensure continuous system operations everyday. First, the state of knowledge of human factors research in the computer security domain was extensively reviewed which showed that sysadmins are an understudied population of expert users. Working with Dr. Simon Parkin, they studied what the work of sysadmins looks like and how this work was affected by COVID-19. Most recently, they collaborated with Dr. Yasemin Acar and Ir. Harshini Sri Ramulu to study the gendered experiences of system administrators working in a men-dominated profession.

EDUCATION

2010–2014 Bachelor of Engineering (BE) in Mechanical Engineering
Reva Institute of Technology and Management (RITM), VTU
Final Project: Optimization of a Quadcopter for a Stable Flight

2014–2017 Master of Science (MSc) in Aerospace Engineering
Specialized in Air Transport and Operations
Delft University of Technology (TU Delft)
Thesis: Causes, Identification and Repair of Loss of Common Ground in Coordination in Air Traffic Management
Supervisor: Dr. Alexei Sharpanskykh
Chair: Prof. dr. ir. Henk Blom

2018–2023 PhD Human Factors in Computer Security
Delft University of Technology (TU Delft)
Thesis: Towards Safe and Just Work Environments for System Administrators
Supervisor: Dr. -Ing. Tobias Fiebig
Promotor: Prof. dr. ir. Marijn Janssen

2023–present Postdoc Human Factors and Equitable Digital Infrastructure
Max Plank Institute for Informatics, INET group
Supervisor: Prof. Anja Feldmann, Ph.D.

AWARDS

Oct 2023 **CSCW Recognition Award for Contribution to Diversity and Inclusion** for the paper:
M. Kaur, H. Sri Ramulu, Y. Acar, T. Fiebig, *"Oh yes! over-preparing for meetings is my jam :)": The Gendered Experiences of System Administrators*, In Proceedings of the ACM on Human-Computer Interaction 7, Computer-Supported Cooperative Work CSCW1, Article 141 (2023)

List of Publications

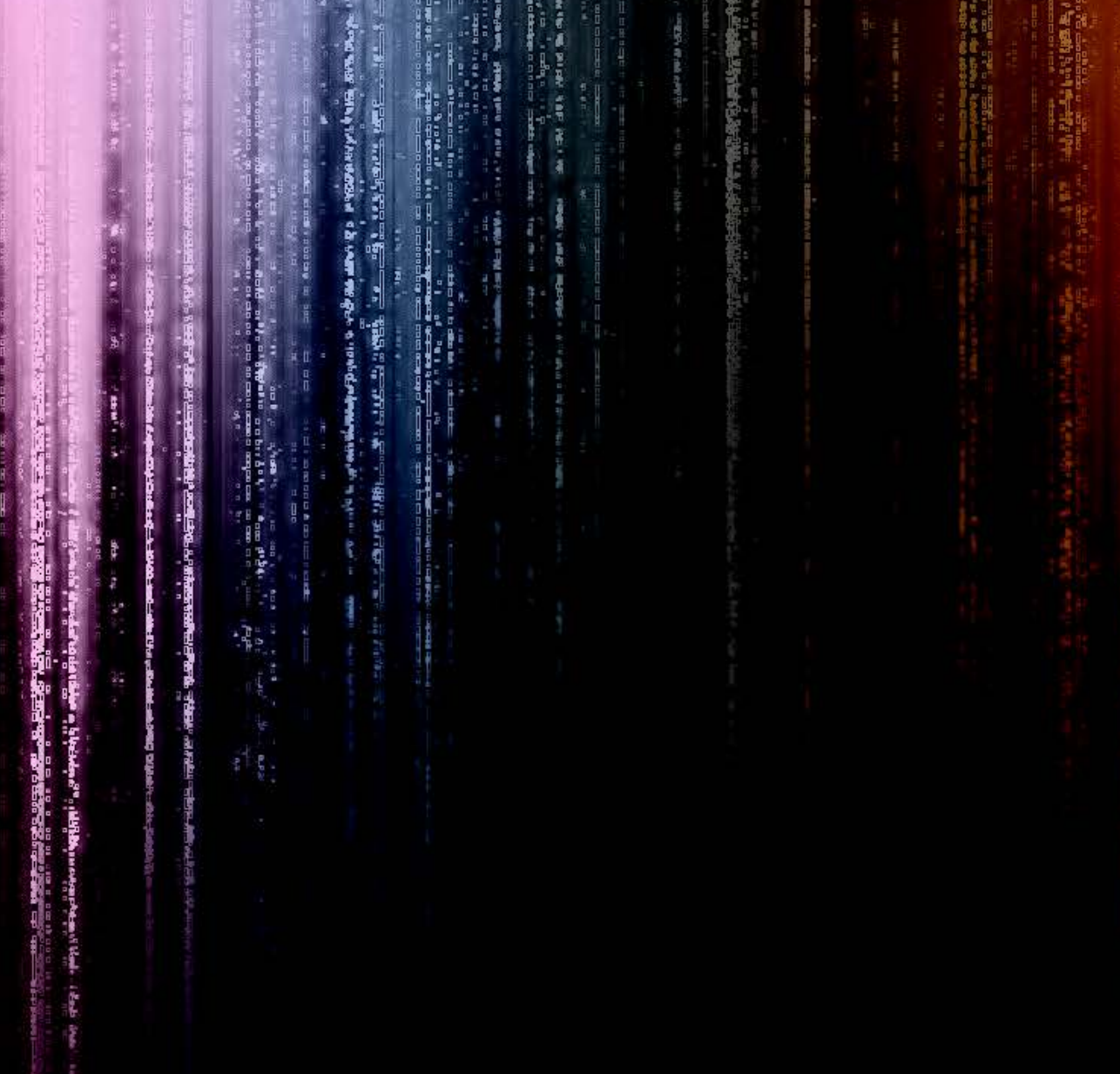
5. **M. Kaur**, H. Sri Ramulu, Y. Acar, T. Fiebig, *"Oh yes! over-preparing for meetings is my jam :)": The Gendered Experiences of System Administrators*, In Proceedings of the ACM on Human-Computer Interaction 7, Computer Supported Cooperative Work CSCW1, Article 141, 38 pages (2023).

4. **M. Kaur**, S. Parkin, M. Janssen, T. Fiebig, *"I needed to solve their overwhelmness": How System Administration Work was Affected by COVID-19*, In Proceedings of the ACM on Human-Computer Interaction 6, Computer Supported Cooperative Work CSCW2, Article 390, 30 pages (2022).

3. **M. Kaur**, M. van Eeten, M. Janssen, K. Borgolte, T. Fiebig, *Human Factors in Security Research: Lessons Learned from 2008-2018*, arXiv pre-print, 23 pages (2021).

2. **M. Kaur**, R. J. De Boer, A. Oates, J. Rafferty, S. Dekker, *Restorative Just Culture: A Study of the Practical and Economic Effects of Implementing Restorative Justice in an NHS Trust*, MATEC Web of Conferences 273, 01007, 9 pages (2019).

1. S. Hussain, A. Puttabakula, **M. Kaur**, R.B.S. Gowda, *Optimization of a Quad Rotor Aircraft for a Stable Flight*, Journal on Science Engineering & Technology JSET, Vol. 1, No. 2, 10 pages (2014).



Abstract: This dissertation is a qualitative exploration into system administration work, encompassing a comprehensive review of existing literature, an in-depth interview investigation, and a focus group study. It culminates in a set of recommendations for moving toward safe and equitable work environments for system administrators.

Author bio: Mannat Kaur was born in India in September 1992. Their academic journey began with a bachelor's degree in mechanical engineering, which they earned in 2014 from RITM Bangalore, India. Specializing in control and operations, they pursued their Master of Science in aerospace engineering at TU Delft, the Netherlands, completing it in 2017. Their research interests revolve around human factors, and they are inspired by feminist research methodologies and approaches.