“I needed to solve their overwhelmness”: How System Administration Work was Affected by COVID-19

MANNAT KAUR, SIMON PARKIN, and MARIJN JANSSEN, TU Delft
TOBIAS FIEBIG, Max-Planck-Institut für Informatik, Forschungsgruppe Internet Architecture (INET)

The ongoing global COVID-19 pandemic made working from home – wherever working remotely is possible – the norm for what had previously been office-based jobs across the world. This change in *how* we work created a challenging situation for system administrators (sysadmins), as they are the ones building and maintaining the digital infrastructure our world relies on.

In this paper, we examine how system administration work changed early in the pandemic from sysadmins' personal perspectives, through semi-structured interviews and thematic analysis. We find that sysadmins faced a two-sided crisis: While sysadmins' own work environment changed, they also had to react to the new situation and facilitate stable options to work online for themselves and their colleagues, supporting their users in adapting to the crisis. This finding embeds into earlier work 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.

Furthermore, while we find that sysadmins *perceived* no major changes in the way they work, by consecutively probing our interviewees, we find that they *did* experience several counter-intuitive effects on their work. This includes 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, we identify changes in sysadmins' coordination patterns. From these we derive recommendations for how system administration work can be coordinated, ranging beyond the immediate pandemic response and the transition to any 'new normal' way of working.

CCS Concepts: • **Human-centered computing** → **Empirical studies in HCI**.

Additional Key Words and Phrases: human factors, qualitative study, system administration, sysadmin, sysops, interviews, system operations, COVID-19

ACM Reference Format:
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. *ACM CSCW*, 30 pages.

1 INTRODUCTION

When the World Health Organization declared the COVID-19 outbreak as a pandemic on 11th March 2020 [54], 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.

Authors' addresses: Mannat Kaur, m.kaur@tudelft.nl; Simon Parkin, s.e.parkin@tudelft.nl; Marijn Janssen, M.F.W.H.A. Janssen@tudelft.nl, TU Delft, P.O. Box 5015, Delft, 2628 BX; Tobias Fiebig, tfiebig@mpi-inf.mpg.de, Max-Planck-Institut für Informatik, Forschungsgruppe Internet Architecture (INET), Campus E14, Saarbrücken, 66123.

While the onset of COVID-19 was a disruptive event for everyone, we investigate how this challenge affected system administrators[1] 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 paper, 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 [9].

Contributions: In summary, we make 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 [11], providing evidence of the connection between IT (security) work and notions of care and responsibility [29], 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 paper is arranged as follows: We first introduce Background literature on sysadmins' work, coordination, and existing frameworks for handling crisis situations in Section 2. Informed by existing approaches, we next present our Methodology in Section 3, where we also detail our analysis approach and ethical considerations. We then present the Results of our analysis

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

in Section 4, going on to frame our study alongside Related Work (Section 5), before a Discussion of the implications of our results (Section 6); 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 7.

2 BACKGROUND

In this section, we discuss the activities of system administration, as the work that sysadmins do. We provide an overview of prior work on coordination where it relates to sysadmin work, and expand upon this to consider coordination *during a crisis*. We also describe a model of coordination and communication [11] – referred to here as 'the co-ladder model' – which we use as a lens to analyze sysadmins' coordination in response to the COVID-19 related lockdowns. Later in discussion (Section 6) we revisit this model to further contextualize and reflect on our findings.

2.1 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, where this work is attributed to *system administrators*, or *'sysadmins'*. 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."* [36].

Consolidating these definitions points 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*. In a crisis, sysadmins must facilitate other employees' adaptations by adapting the IT systems available to them. In so doing, 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 [5]. 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.

System Administration and DevOps. Since the early 2000s the concept of 'DevOps' has grown out of the concept of 'Site Reliability Engineers', first prominent at Google [4]. DevOps, a word-merger between development and operations, is often (mis)understood as something *different* than classical system administration [36]. 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 [14, 34]. 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) [14, 34, 36]; formalize already existing practices (making outcomes and changes' impact measurable) [36], and; incorporate lessons learned from safety science on preventing errors (a just error culture and blameless post-mortems, for example) [14, 18, 34].

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 [36]—but has to gradually change the culture of its operations. Hence, parts of how DevOps 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 just error culture. In sum, we consider professionals working as DevOps to be within scope as sysadmins for the purpose of this paper.

2.2 Coordination in System Administration

Several prior studies have highlighted the collaborative nature of system administration work [3, 15, 23, 51, 52]. Sysadmins have to constantly communicate with other sysadmins to *coordinate* tasks, i.e., *"work that needs to be done"* [51]. Coordination—according to Malone and Crowston—is *"the act of managing interdependencies between activities performed to achieve a goal"* [40]. Naturally, coordination also requires multiple actors to be involved for coordination to occur *between* them [40], where sysadmins coordinate their activities as a team [17]. Tasks can be discrete activities or consist of interdependent sub-tasks [45], 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 [36]. A common flashpoint for this coordination is, for example, the rollout of software updates, which can necessitate computer restarts, which must not impact productive work [49].

There is both *implicit* and *explicit* coordination, with explicit coordination being the most commonly *recognized* form of coordination [19]. This manifests when actors in a team *explicitly* exchange information about their tasks in order to coordinate them [19]. 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' [19].

Implicit coordination occurs when teams exhibit coordinated behavior *without* any explicit exchange of information [19]. 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 [33], or similarly exhibit seemingly the same awareness of a situation [48]. 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 also anticipate their actions as well [19]. 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.

2.3 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"* [10]. 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 [7].

To navigate the complex space of sysadmin 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. [11]. This model is also called the co-ladder model, because of its shape of (multiple) ladders placed next to each other, see Figure 2. We regard an anomaly in planning as an event that is both *abnormal* and *unexpected* [20]. 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."*.

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 [26]. 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"* [11].

We chose the co-ladder model for our analysis as opposed to the 4-phase model by Boin and Bynander [7] or the theoretical coordination framework by Christensen and Ma [12]. 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. [55], usually deal with concrete fast-response emergency scenarios (similar to the model of Boin and Bynander [7]), 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.

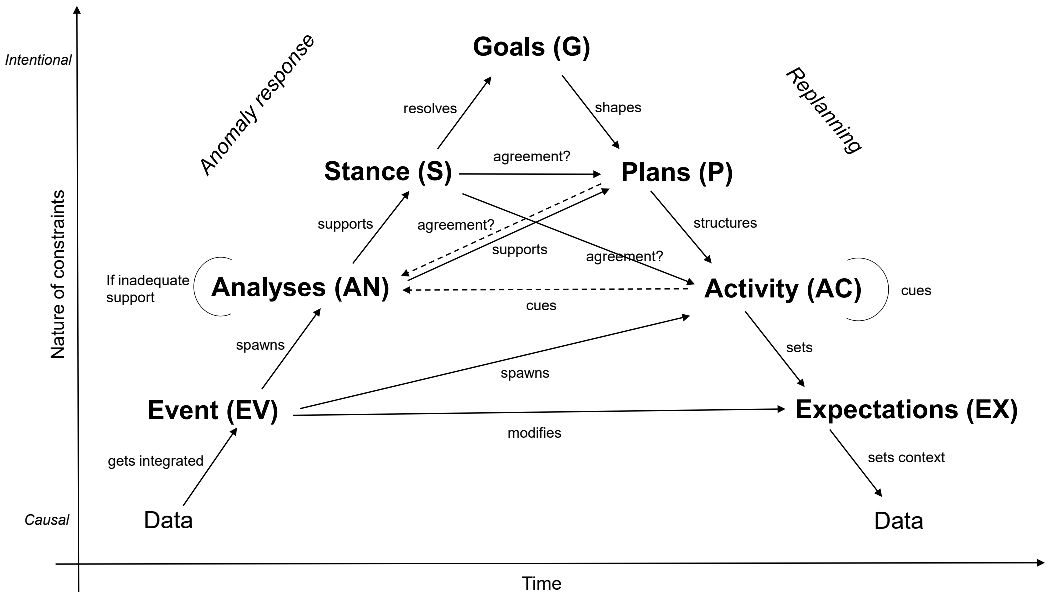


Fig. 1. Model of coordination and communication for distributed anomaly response and replanning (Co-Ladder Model), reproduced from Chow et al. [11].

We provide an overview of the Chow et al. model in Figure 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 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. [11] 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 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

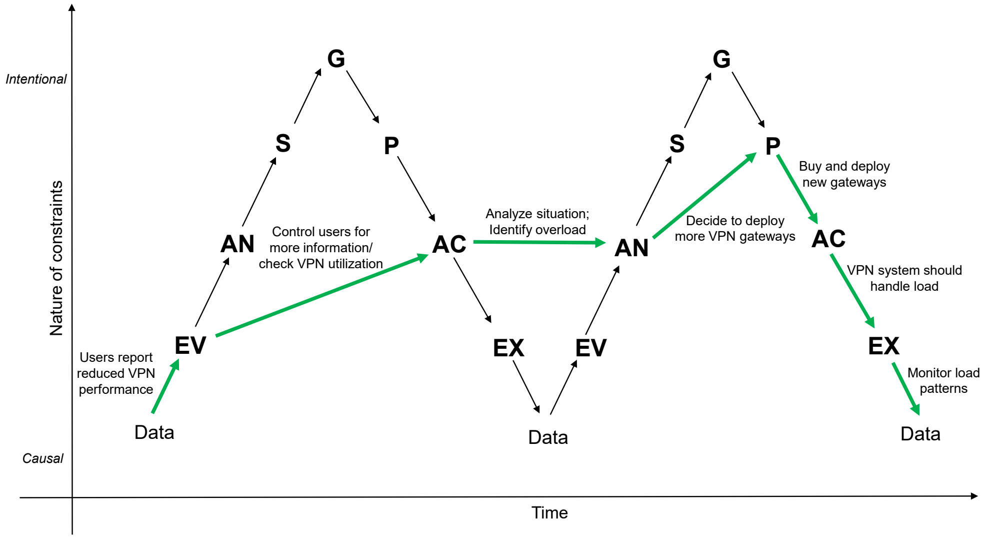

Intentional
Causal
Nature of constraints
Time
G
S
P
AN
AC
EV
EX
Data
Users report reduced VPN performance
Control users for more information/ check VPN utilization
Analyze situation; Identify overload
G
S
P
AN
AC
EV
EX
Data
Decide to deploy more VPN gateways
Buy and deploy new gateways
VPN system should handle load
Monitor load patterns
Data

Fig. 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).

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.

3 METHODOLOGY

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

3.1 Modelling Coordination Within System Administration

The Chow et al. / 'co-ladder' model [11], 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 3.2). We structured the engagements accordingly, as described in Section 3.3.

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.

3.2 Pre-Study

In early 2020, before COVID-19 emerged as a global crisis, one of the authors began an observational study in a team of six Linux administrators, similar to the work of Barrett et al. [3]. In total, the author 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.

3.3 Interview Protocol

For the interview questions, our main focus is on the day-to-day tasks of sysadmins, following our description in Section 2.1. Given the diverse nature of sysadmin 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 2.3). Here it is important to relate to the terminology used by participants [1], and rather than introduce these terms from the co-ladder model, instead be careful not to introduce the researchers’ terms into the interviews themselves [30]. 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 sysadmin 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 [1]). 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.

3.4 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.

3.5 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. [46] and Dietrich et al. [18]. Additionally, we recruited via social media posts (Twitter, LinkedIn) to attract self-described sysadmins. See Figure 4 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. [18]. In total, we recruited 22 participants for interviews, see Table 1.

Table 1. Overview of participants' working location, work experience, and their employers business sector.

ID	Sector	Experience	Location	ID	Sector	Experience	Location
P1	IT	2 years	Netherlands	P13	Telecommunication	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	United Kingdom
P11	Education	5 years	Netherlands	P23a	Manufacturing industry	16 years	Germany
P12	Education	10 years	Austria	P24a	IT	4 years	Canada

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.

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. [18]. We do not list our participants' specific job titles. We found, in line with existing understanding in Section 2, 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 2, and further consider roles during our result analysis.

3.6 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 [9]. Note that *"data are not coded in an epistemological vacuum"* [8], and we inform our work with existing theory (Section 2) to place our work within the existing research in the field (Section 6). 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."* [9]. 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 [8], one author 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. [41]. In total we developed 93 codes split over four main themes and 15 subgroups, as in Table 2.

4 RESULTS

In this section, we first discuss what our sysadmin participants report doing as their work (Subsection 4.1 – 'Sysadmin Tasks' in Table 2) – leading to tasks in activities they have to perform for their jobs, associated responsibilities, and underlying goals. In Subsection 4.2, 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 2. In Subsection 4.3, the lockdown-induced changes on sysadmins' coordination activities are presented, drawing from 'Lockdown Effects' and 'Social Interactions' in Table 2, while also contextualizing the need for these changes under the premise of 'Security'.

4.1 Sysadmins' Tasks and Responsibilities

Our participants' reported tasks and responsibilities broadly in line with our initial description of what sysadmins do (Section 2.1), 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. [29], 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.

Table 2. Overview of our code-book.

	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						

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 sysadmin work can nonetheless mean that the job of system administration is *"quite [an] invisible one"* (P12). Limoncelli et al. [34] 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. [3] 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! Yeah! 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 [31]. 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 community nature of the sysadmin workforce, as also reported by Dietrich et al. [18].

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 sysadmin work: **helping people** (users and colleagues) and **coordination processes** (formal and informal).

4.2 Supporting Others: Lockdown-Induced Task and Responsibility Changes

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 [sic]"*, 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 [28]). 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 Virtual Private Network (VPN) access, and 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 4.3.4).

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. [44]. 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 [43].

4.3 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 4.1), 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 [43], 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 sysadmin 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 [16]. Despite all this, sixteen participants reported that they perceived the lockdown itself to not affect their tasks or how they work.

4.3.1 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 4.3.4), and as reported elsewhere [29], 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 [39]), 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. [29] 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 [29].

4.3.2 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 [16, 43] 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 [37], as a lens on their 'repair' of destabilized work processes [25], but here as another 'oscillation' in security [29] 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 [2, 53]. However, also note that informal interactions help in building trust which is essential for collaborative work [43]. 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 [43]. 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 [43], it can be difficult to establish common ground – and develop implicit coordination [19] – 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 sysadmin 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 [16] and reports therein of an increase in overall meetings in order to compensate for the lower (perceived) effectiveness of online meetings.

4.3.3 More Formal Coordination Needed for Routine Tasks. As noted in Section 2, 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 [43], 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 [29].

4.3.4 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 [18], 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 [42], 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.

5 RELATED WORK

We present related work in two parts. First, studies related to system administration and distributed work in system administration. Second, studies related to system administration during crisis situations, including the impact of COVID-19.

5.1 System Administration as Distributed Work

Early work regarding sysadmins was either descriptive, e.g., Barret et al. [3], or focused on tools and usability, e.g., Haber and Bailey [22]. Later work then started to investigate the interaction and coordination of sysadmins, for example Maglio et al. looking at distributed cognition [38], and Velasquez and Weisband who framed sysadmins as 'broker technicians' due to the high communication needs of the profession [51]. Kocksch et al. then expand beyond coordination alone, including discussion of the notion of care in system administration [29]. This general theme of moving from descriptive and tool-focused studies can also be found in the context of computer security [27], where (insufficient) coordination is an important factor in updating systems [49] and security issues [18].

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 [24]. We also connect to Bjorn et al., who find that effective remote work is a matter of organizational practices and available supporting technology [6]. 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 sysadmin work, between organizing one's own work and caring for the work of others.

5.2 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 [47], or De Souza et al., who similarly investigated sysadmins during incident response [15]. Similarly, Haber and Kandogan note that especially for security tasks and issues, sysadmins' work is 'event-driven' [21].

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.

5.3 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 [16]. 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 [13]. 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. [28] 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 [35]. Finally, from a security perspective, Lallie et al. investigate how the threat landscape on the Internet changed due to COVID-19 and associated effects [32]. While this latter study is tangential, it still documents how the environment outside of sysadmin 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.

6 DISCUSSION

In this section we discuss and contextualize our overall findings, and relate our results back to the descriptive co-ladder model (Section 2). We conclude this section with recommendations and lessons learned, and document the limitations of our work.

6.1 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' [11] to understand the changes (as referred to in Section 2.3).

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. [28]; also see our report on these findings in Section 4.2.

We found that the two main aspects of sysadmin 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 [29]), 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 [16, 43]. 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 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 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 4.3.4. While this is related to comparable effects, e.g., among information security managers [42], 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) [16], 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 on a different population of employees, e.g., by Maguire [39], 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 [39], 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 4.3.1, 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 [31]; 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 sysadmin 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. [31] 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.

The link between sysadmin 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 other 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).

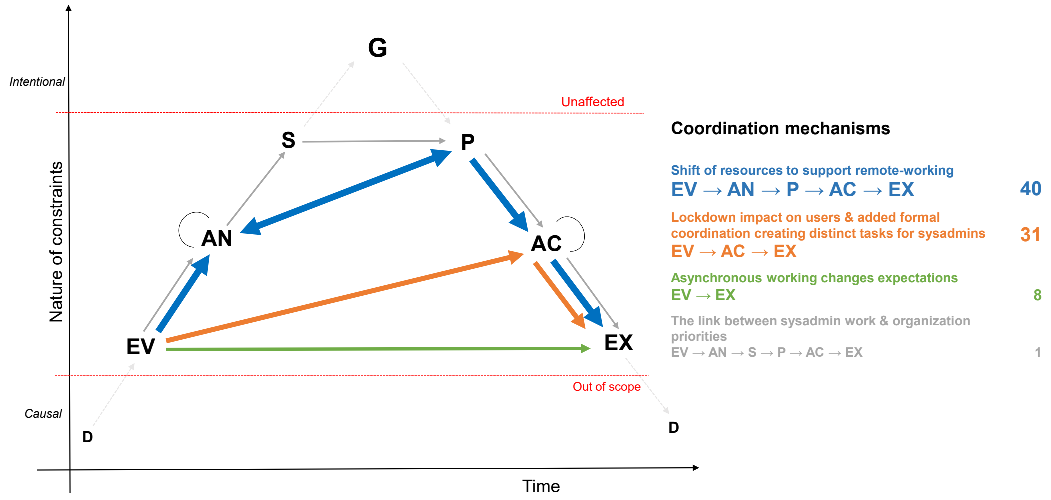

G
Intentional
Unaffected
S
P
AN
AC
EV
EX
Nature of constraints
Out of scope
Causal
D
D
Time
Coordination mechanisms
Shift of resources to support remote-working
EV → AN → P → AC → EX
40
Lockdown impact on users & added formal coordination creating distinct tasks for sysadmins
EV → AC → EX
31
Asynchronous working changes expectations
EV → EX
8
The link between sysadmin work & organization priorities
EV → AN → S → P → AC → EX
1

Fig. 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.

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 [42], it distinguishes this aspect in our population from observations in related work.

6.2 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 [22, 24]. 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. [29]), 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 sysadmin work can emerge.

6.3 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 [47], and the role of care in managing IT and IT-security in organisations [29, 31].

In contrast to the original co-ladder model [11], 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.

7 CONCLUSIONS

In this paper we present 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 sysadmin 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.

7.1 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. Furthermore, based on our findings regarding its applicability, further studies can use the co-ladder model to investigate sysadmins' distributed work and coordination.

ACKNOWLEDGMENTS

This material is based on research supported by the European Commission (EC) under grant CyberSecurity4Europe (#830929), and the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (Dutch Research Council, NWO) under grant INTERSECT (NWA.1160.18.301). Any views, opinions, findings, recommendations, or conclusions contained or expressed herein are those of the authors and do not necessarily reflect the position, official policies, or endorsements, either expressed or implied of their host institutions, or those of the EC, or NWO.

REFERENCES

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

[2] Mats Alvesson and Stefan Sveningsson. 2003. Good visions, bad micro-management and ugly ambiguity: Contradictions of (non-) leadership in a knowledge-intensive organization. *Organization studies* 24, 6 (2003), 961–988.

[3] Rob Barrett, Eser Kandogan, Paul P Maglio, Eben M Haber, Leila A Takayama, and Madhu Prabaker. 2004. 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).* 388–395.

[4] Betsy Beyer, Chris Jones, Jennifer Petoff, and Niall Richard Murphy. 2016. *Site reliability engineering: How Google runs production systems.* " O'Reilly Media, Inc.".

[5] Veroniek Binkhorst, Tobias Fiebig, Katharina Krombholz, Wolter Pieters, and Katsiaryna Labunets. 2022. 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.*

[6] Pernille Bjørn, Morten Esbensen, Rasmus Eskild Jensen, and Stina Matthiesen. 2014. Does distance still matter? Revisiting the CSCW fundamentals on distributed collaboration. *ACM Transactions on Computer-Human Interaction (TOCHI)* 21, 5 (2014), 1–26.

[7] Arjen Boin and Fredrik Bynander. 2015. Explaining success and failure in crisis coordination. *Geografiska Annaler: Series A, Physical Geography* 97, 1 (2015), 123–135.

[8] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101.

[9] Virginia Braun and Victoria Clarke. 2020. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology* (2020), 1–25.

[10] Jonathan Bundy, Michael D Pfarrer, Cole E Short, and W Timothy Coombs. 2017. Crises and crisis management: Integration, interpretation, and research development. *Journal of Management* 43, 6 (2017), 1661–1692.

[11] Renée Chow, Klaus Christoffersen, and David D Woods. 2000. A model of communication in support of distributed anomaly response and replanning. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 44:1. SAGE Publications Sage CA: Los Angeles, CA, 34–37.

[12] Tom Christensen and Liang Ma. 2020. Coordination structures and mechanisms for crisis management in China: Challenges of complexity. *Public Organization Review* 20, 1 (2020), 19–36.

[13] Rafael da Camara, Marcelo Marinho, Suzana Sampaio, and Saulo Cadete. 2020. How do Agile Software Startups deal with uncertainties by Covid-19 pandemic? *arXiv preprint arXiv:2006.13715* (2020).

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

[15] Cleidson RB de Souza, Claudio S Pinhanez, and Victor F Cavalcante. 2011. 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.* 1–10.

[16] Gianluca F Delfino and Berend van der Kolk. 2021. Remote working, management control changes and employee responses during the COVID-19 crisis. *Accounting, Auditing and Accountability Journal* (2021).

[17] Dennis J Devine. 2002. A review and integration of classification systems relevant to teams in organizations. *Group Dynamics: Theory, Research, and Practice* 6, 4 (2002), 291.

[18] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. 2018. Investigating system operators' perspective on security misconfigurations. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS).* 1272–1289.

[19] J Alberto Espinosa, F Javier Lerch, and Robert E Kraut. 2004. *Explicit versus implicit coordination mechanisms and task dependencies: One size does not fit all.* American Psychological Association, 107–129.

[20] Marisa R Grayson. 2020. Cognitive work of hypothesis exploration during anomaly response. *Commun. ACM* 63, 4 (2020), 97–103.

[21] Eben Haber and Eser Kandogan. 2007. Security administrators: A breed apart. *Proceedings of the SOUPS Workshop on Usable IT Security Management (USM)* (2007), 3–6.

[22] Eben M Haber and John Bailey. 2007. 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).*

[23] Eben M Haber, Eser Kandogan, and Paul Maglio. 2010. Collaboration in System Administration: For sysadmins, solving problems usually involves collaborating with others. How can we make it more effective? *Queue* 8, 12 (2010), 10–20.

[24] Jim Hollan and Scott Stornetta. 1992. Beyond being there. In *Proceedings of the SIGCHI conference on Human factors in computing systems.* 119–125.

[25] Ju Yeon Jung, Tom Steinberger, John L King, and Mark S Ackerman. 2021. Negotiating Repairedness: How Artifacts Under Repair Become Contingently Stabilized. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–29.

[26] Mannat Kaur. 2017. Causes, identification and repair of loss of common ground in coordination in ATM (air traffic management), *Master Thesis, TU Delft.*

[27] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. 2021. Human Factors in Security Research: Lessons Learned from 2008-2018. *arXiv preprint arXiv:2103.13287* (2021).

[28] Kevin M Kniffin, Jayanth Narayanan, Frederik Anseel, John Antonakis, Susan P Ashford, Arnold B Bakker, Peter Bamberger, Hari Bapuji, Devasheesh P Bhave, Virginia K Choi, et al. 2021. COVID-19 and the workplace: Implications, issues, and insights for future research and action. *American Psychologist* 76, 1 (2021), 63.

[29] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT security: Accountabilities, moralities, and oscillations in IT security practices. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.

[30] Kat Krol, Jonathan M Spring, Simon Parkin, and M Angela Sasse. 2016. Towards robust experimental design for user studies in security and privacy. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016).* 21–31.

[31] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J Godfrey, Heather Lipford, and Pamela J Wisniewski. 2021. Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–23.

[32] Harjinder Singh Lallie, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. Cyber security in the age of Covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security* 105 (2021), 102248.

[33] Beng-Chong Lim and Katherine J Klein. 2006. Team mental models and team performance: A field study of the effects of team mental model similarity and accuracy. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior* 27, 4 (2006), 403–418.

[34] Tom Limoncelli, Strata R Chalup, and Christina J Hogan. 2014. *The Practice of Cloud System Administration: Designing and Operating Large Distributed Systems.* Vol. 2. Pearson Education.

[35] Thomas A Limoncelli. 2020. Five Nonobvious Remote Work Techniques: Emulating the efficiency of in-person conversations. *Queue* 18, 3 (2020), 29–38.

[36] Thomas A Limoncelli, Christina J Hogan, and Strata R Chalup. 2016. *The Practice of System and Network Administration: Volume 1: DevOps and other Best Practices for Enterprise IT.* Vol. 1. Addison-Wesley Professional.

[37] Leah Maestri and Ron Wakkary. 2011. Understanding repair as a creative process of everyday design. In *Proceedings of the 8th ACM Conference on Creativity and Cognition.* 81–90.

[38] Paul P Maglio, Eser Kandogan, and Eben Haber. 2008. Distributed Cognition and Joint Activity in Computer System Administration. In *Resources, Co-Evolution and Artifacts.* Springer, 145–166.

[39] Laura MD Maguire. 2020. Managing the hidden costs of coordination. *Commun. ACM* 63, 4 (2020), 90–96.

[40] Thomas W Malone and Kevin Crowston. 1990. 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).* 357–370.

[41] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–23.

[42] Tyler Moore, Scott Dynes, and Frederick R Chang. 2016. Identifying how firms manage cybersecurity investment. *Workshop on the Economics of Information Security (WEIS)* (2016).

[43] Judith S Olson and Gary M Olson. 2014. Bridging Distance: Empirical studies of distributed teams. In *Human-Computer Interaction and Management Information Systems: Applications. Advances in Management Information Systems*. Routledge, 117–134.

[44] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E Grinter, and W Keith Edwards. 2009. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 739–748.

[45] Alberto Barbosa Raposo, Léo Pini Magalhães, Ivan Luiz Marques Ricarte, and Hugo Fuks. 2001. Coordination of collaborative activities: A framework for the definition of tasks interdependencies. In *Proceedings of the Seventh IEEE International Workshop on Groupware (CRIWG)*. 170–179.

[46] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. 2019. Security managers are not the enemy either. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 1–7.

[47] Thea Riebe, Marc-André Kaufhold, and Christian Reuter. 2021. The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–30.

[48] Eduardo Salas, Carolyn Prince, David P Baker, and Lisa Shrestha. 1995. Situation awareness in team performance: Implications for measurement and training. *Human Factors* 37, 1 (1995), 123–136.

[49] Christian Tiefenau, Maximilian Häring, Katharina Krombholz, and Emanuel von Zezschwitz. 2020. Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators. In *Symposium on Usable Privacy and Security (SOUPS)*. 239–258.

[50] US National Institute of Standards and Technology (NIST). 2021. System administrator (SA). NIST Information Technology Laboratory: Computer Science Resource Center (CSRC) https://csrc.nist.gov/glossary/term/system_administrator. Accessed: 2021-07-08.

[51] Nicole F Velasquez and Suzanne P Weisband. 2009. System administrators as broker technicians. In *Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology*. 1–8.

[52] Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. 2010. Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security* (2010).

[53] Richard D White Jr. 2010. The micromanagement disease: Symptoms, diagnosis, and cure. *Public Personnel Management* 39, 1 (2010), 71–76.

[54] WHO. [n.d.]. *WHO Director-General's opening remarks at the media briefing on COVID-19*. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[55] Jeroen Wolbers, Kees Boersma, and Peter Groenewegen. 2018. Introducing a fragmentation perspective on coordination in crisis management. *Organization Studies* 39, 11 (2018), 1521–1546.

A APPENDIX

A.1 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 (right after lockdown)?
  - 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.2 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.

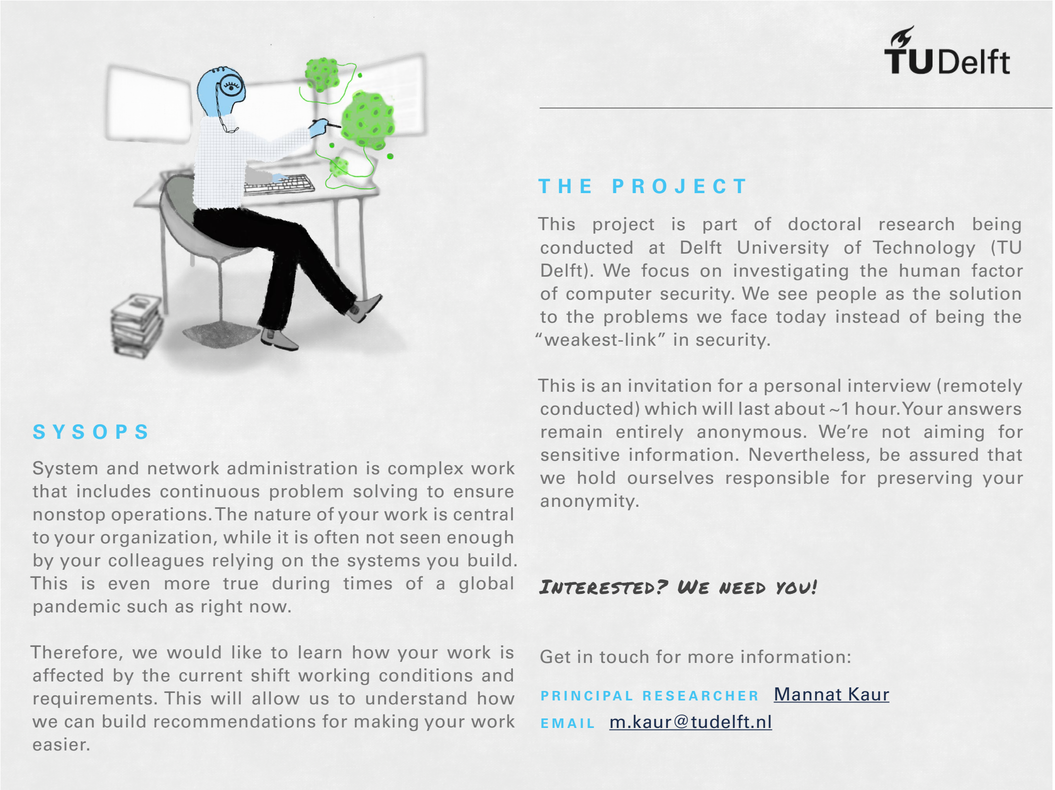
Taking part in the study

(1) I have read and understood the study information dated / /2020, 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.3 Recruitment Flyer



SYSOPS

System and network administration is complex work that includes continuous problem solving to ensure nonstop operations. The nature of your work is central to your organization, while it is often not seen enough by your colleagues relying on the systems you build. This is even more true during times of a global pandemic such as right now.

Therefore, we would like to learn how your work is affected by the current shift working conditions and requirements. This will allow us to understand how we can build recommendations for making your work easier.

THE PROJECT

This project is part of doctoral research being conducted at Delft University of Technology (TU Delft). We focus on investigating the human factor of computer security. We see people as the solution to the problems we face today instead of being the "weakest-link" in security.

This is an invitation for a personal interview (remotely conducted) which will last about ~1 hour. Your answers remain entirely anonymous. We're not aiming for sensitive information. Nevertheless, be assured that we hold ourselves responsible for preserving your anonymity.

INTERESTED? WE NEED YOU!

Get in touch for more information:

PRINCIPAL RESEARCHER Mannat Kaur
EMAIL m.kaur@tudelft.nl

Fig. 4. Flyer for participant recruitment.