Securing Vital Power Against Uncertainties

Standards and Standardisation, Forecasting, and Training as Power Grid Security Techniques

Leonard Schliesser

Thesis in pursuit of the qualification of

Doctor of Philosophy (PhD)

Department of Geography

Durham University

2024

Abstract

Modern societies depend on a stable and uninterrupted electricity supply. Power grids function as infrastructural life-support systems. Their complexity, interdependence, and tight coupling generate systemic uncertainty: failures can occur unexpectedly and escalate rapidly, while every security intervention can reflexively be either excessive or insufficient. Blackouts are rarely caused by a single discrete event, but rather by cascading failures within a stressed system. Securing the grid, then, means intervening before uncertainty materialises into a potential catastrophe.

This thesis investigates how security is enacted in the German electricity transmission system. Yet the interconnected grid and its security defy national boundaries. Drawing on multi-sited ethnographic fieldwork with a Transmission System Operator (TSO) and a regional security coordinator (RSC), it examines how everyday operations contain, reduce and manage uncertainty. The study focuses on three key security techniques—standards and standardisation, forecasting, and training—which each target distinct uncertainties and futures. The aim is to understand how security emerges not from eliminating threats, but from rendering uncertainties actionable through technical and embodied routines.

The analysis demonstrates how standards rely on imagined futures to inform present actions, how forecasting models generate probabilistic predictions of grid behaviour, and how training creates uncertainty managers. These techniques do not operate in isolation. Their layered application constitutes a form of anticipatory security that manages uncertainty across spatial and temporal scales. Power grid security, the thesis argues, is not reactive but generative: it creates, includes and excludes specific futures.

The thesis contributes to Critical Security Studies by theorising power grid security as a form of everyday biopolitics. It shows how infrastructures are made secure through mundane yet vital forms of labour that modulate uncertainty, rather than eliminate it. These findings have broader implications for understanding how security is enacted in other infrastructural systems shaped by complexity, interdependence, and systemic uncertainty.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACER	Agency for the Cooperation of Energy Regulators
aFRR	Frequency Restoration Reserve with automatic activation
AMICA	Advanced Multisite Integral Congestion Assessment
BNetzA	Bundesnetzagentur - German Federal Network Agency
CCR	Capacity Calculation Region
CF	Contingency Failure
CGM	Common Grid Model
CGS	Critical Grid Situation
CNEC	Critical Network Element with Contingency
CORE FB MC	CORE (Capacity Calculation Region) Flow-Based Market Coupling
D-1	Day ahead
D-2	Two Days ahead
DACF	Day Ahead Congestion Forecast
DEF	Data Exchange Format
ENTSO-E	European Network of Transmission System Operators for Electricity
FCR	Frequency Containment Reserve
FRM	Flow Reliability Margin

GSK	Generation Shift Key
HRO	Highly Reliable Organisation
IDCF	Intra-Day Congestion Forecast
IGM	Individual Grid Model
LF	Load Flow
LTA	Long-Term Allocated Capacities
mFRR	Frequency Restoration Reserve with manual activation
NRAO	Non-Costly Remedial Action Optimisation
OM	Operational Manager (at TSCNET)
OPC	Outage Planning Coordination
OPI	Outage Planning Incompatibilities
PTDF	Power Transfer Distribution Factor
RAM	Remaining Available Margin
RAO	Remedial Action Optimisation
RSC	Regional Security Coordinator
SDAC	Single Day-ahead Coupling
SO GL	System Operation Guidelines
STA	Short Term Adequacy
TSO	Transmission System Operator
UCTE	Union for the Coordination of the Transmission of Electricity
UPS	Uninterrupted Power Supply
WOPT	Weekly Operational Teleconference
Y-1	Year ahead

Statement of Copyright

Acknowledgements

The work presented in this thesis is my own. Nevertheless, this PhD would not have been possible or completed without the help and support of others. I would like to extend my gratitude to my supervisors for their sustained guidance, support and patience. Without their encouragement, I would probably not have started a PhD in the first place.

Thank you to the Economic and Social Research Council (ESRC) and NINE DTP for their stipend. Your financial support allowed me to conduct this PhD. Similarly, I would like to extend my sincere gratitude to my Geography Department. Without their infrastructure, especially the Gordon Manley Room, Skylab and their staff the PhD experience would have been a very different one.

Supplied with funds and excellent supervisors, I would like to thank the regional security coordinator, TSCNET, and the transmission grid operator, TransnetBW. Despite the COVID-19 pandemic, you offered me access to your organisation and personnel. You allowed me to shadow the operators and OMs on shift—special thanks to those who welcomed me to their control and coordination rooms. We spent a lot of time together, and I am grateful for the stories and insights you shared, all while being patient in explaining the details of grid operation that I lacked as a Geographer.

To my family, friends and colleagues, thank you for your support throughout these years. Thank you for your encouragement, wit and patience with me. Thank you for the stimulating conversations about various topics and the challenging sessions on my writing and lines of argumentation. I learnt a lot from you and am glad to have you by my side. With you, the PhD experience was more colourful.

Finally, I am immensely grateful to have met my wife on this journey. Your love and care gave me the strength and motivation I needed during the final stretch. Thank you for your patience and endurance. You now have a great deal of knowledge about the power grid and why it's essential to be prepared.

Dedication

There is no glory in pre-emption, prevention, preparedness or precaution. Nevertheless, silent professionals in critical infrastructure providers, emergency services and the armed forces constantly ensure and safeguard our lives and lifestyles.

Thank you for your service.

Preface: The Emsland Case

On the 4th of November 2006, what should have been a relatively routine operation on the transmission grid severely compromised its security. A cruise ship built in the Papenburg shipyard (NW Germany) had to transition underneath a transmission line on its way to the open ocean. As a precaution, this transmission line was switched off. Multiple preceding analyses by the responsible transmission system operators (TSOs) did indicate a tight but manageable impact of this temporary loss of this transmission line on the overall grid. Yet, after it was turned off by the TSO, the situation escalated as circuits unexpectedly overloaded. What followed happened in milliseconds. Cascading overloads tripped and disconnected strings of transmission lines hundreds of kilometres away from the original failure. The synchronous continental European power grid was severed, splitting it into three regions. In Western Europe, the grid collapsed due to severe under-frequency. There was not enough electricity, and the demand was too high. Subsequently, around 15 million households were blacked out for around two hours. Although also affected by under-frequency, the South-Eastern area of Europe did not suffer significant outages. The imbalance between demand and generation remained above the threshold for load shedding. In the North-Western area, the problem was inverted. While no lights went off, it suffered from severe over-frequency, excessive generation, and insufficient demand. The collapse of the now-split European grid was only averted through skilful management and sheer luck. If the TSOs had been unable to black start the grid in the Western area, manage it in the North and South-Eastern parts and re-synchronise them timely, a prolonged blackout of the entirety of continental Europe would have ocurred. This would be a catastrophe. (UCTE 2006)

While the political and public aftermath was relatively mild, the Emsland Case was a watershed event for the European power industry and the transmission system operation. The official post-event report of the Union for the Co-ordination of Transmission of Electricity (UCTE 2006) specified not only human error and a lack of operator training as causes for this near catastrophe, but also more wide-ranging systemic and structural issues of un-coordination and insufficient standardisation. “From that moment on it was definitely clear that different coordination duties were necessary […]”, said Uwe Zimmermann, a managing director of the regional security coordinator (RSC), TSCNET, which was cited in an introductory presentation I received during my three-month internship there (Fieldnotes 090921). It is worth mentioning that the TSO Security Cooperation (TSC) was founded in 2008 and then superseded by TSCNET in 2014 (TSCNET 2022). Furthermore, in response of this event, the European Commission prepared the ‘Third Energy Package’, which incorporated most of the UCTEs' recommendations. With its directives and regulations, the European Union's Third Energy Package (2009) and its update, the Fourth (2019), define and shape the basic structure of the power industry and the energy market in Europe today.

This thesis is dedicated to the security of the energy infrastructure that facilitates the circulation of electrical flows. The primary focus of this thesis is to examine the power grid as an uncertain artefact that requires constant securing to ensure its uninterrupted functioning as a life support system. As a starting point for this thesis, which explores power grid security, the Emsland Case showcases how and what might happen if the grid fails. It highlights the fragility of electric flows that require constant management. In the everyday, the blackout as a potential catastrophe is already present in embryonic form. While in this case, the catastrophe was averted, the Emsland Case provides insights and a reference for all empirical chapters. Standardisation, forecasting and training will be introduced as security techniques developed by the TSOs, which all relate to the Emsland Case and were partially constituted in its aftermath. Without them, TSCNET might not have been founded, as its mandate to forecast and coordinate directly originates from the UCTE’s recommendation and the European Union’s Third Energy Package.

1. Introduction

To keep 'the lights on' is not trivial, requiring a constant balancing act 24/7, 365 days a year. A stable equilibrium does not exist in the power grid, because electrical generation needs to be matched with the momentary demand yet always falls short or exceeds it[1]. However, this is permissible within a specific bandwidth and scale. Nevertheless, any 'too much' or 'too little' exceeding this bandwidth threatens the security of the electrical supply. While a local and short-lived power outage, for most, is nothing more than a nuisance, when prolonged and widespread, it becomes a blackout with potentially catastrophic consequences. Through the still increasing dependence on the uninterrupted flow of electricity, Western societies, such as the German population, become vulnerable in its absence.

In grappling with why 'the lights stay on', this thesis explores how the contemporary German power grid, as a complex infrastructure, and the electrical flows it enables are secured in the everyday. It engages security as a duality of ensuring a specific flow (electricity) that manifests in a wider concern for the security of the infrastructure (power grid) that enables it.

This thesis understands that the power grid secures and enables life while simultaneously requiring constant securing. Like the medium to be secured, security here is inherently unstable, constantly under threat from external factors (changes of demand and generation) and from itself when there is too much or too little. Security here is a "paradox" (Der Derian 1992, Esposito 2011), a "wicked problem" (Rittel & Webber 1973), as in it, we find insecurity. In attempting to secure the flow of electricity, any action intended to do so (beyond a certain threshold) has the reflexive potential to stimulate insecurity and bring about what it wants to foreclose. If, for example, a reaction to a frequency deviation is too little or too much, it escalates this deviation and, in the extreme, could lead to a cascade towards system collapse and blackout.

If security is understood as control or faith in a secure, stable and predictable environment (Heinzen 2004, Grosz 2004), then insecurity equals uncertainty. The electrical infrastructure, as well as its medium, are constantly changing and, therefore, are "meta-stable" (Massumi 2009: 176, cf. Star 1999). Due to varying electricity generation, demand, and market patterns, the frequency changes continuously at different rates. As components of the transmission grid are retired, added, or taken offline for maintenance, the grid only appears to be stable. In the everyday this meta-stability is barely noticed as power is constantly available with the flip of a switch. Nevertheless, due to its complexity, its "tight coupling" (Perrow 1984: 4) and interdependencies, the possibility of escalating and cascading failure is always latently present. Complete control under these conditions of meta-stability and in this complex infrastructure is generally impossible and can only be achieved in small, well-defined pockets. Power grid security thus becomes the management of uncertainty.

The objective of this thesis is to understand how uncertainty is managed in the German power grid. Two research questions spearhead this inquiry and aim to generate new empirical insights into how the electricity grids operate and are secured. They first ask how uncertainty is managed in everyday

[1] The balance of demand and generation is the most prominent issue for power grid security and will be the focus of this thesis. Yet, reactive power would be another metric that requires constant balancing to uphold voltage stability. Due to its technical complexity, it will not be a focus of this thesis and is named here for completeness.

transmission grid operations. Second, it asks, what techniques are deployed in the transmission grid to secure against and manage uncertainty?

In addressing these questions, this thesis makes a primary contribution to the field of Critical Security Studies (CSS). It furthermore contributes more broadly to interdisciplinary debates in infrastructure studies, human geography and to the study of socio-technical systems. It contributes to CSS by offering an empirically rich analysis of how security is enacted in the everyday operation of a critical infrastructure, specifically the German electricity transmission grid.

This thesis does not explore how ordinary people experience security or infrastructure failure, but rather how a small group of specialised actors — transmission grid operators and regional security coordinators — practice and enact security in their routine work. It thus follows a strand of CSS that examines how security is constituted through mundane practices, tools, and anticipatory rationalities that are often hidden from public view but foundational to infrastructural resilience (Anderson & Gordon 2017, Nyman 2021). The everyday, in this context, is not a subjective experience but a spacetime of technopolitical governance, where futures are modelled, failures are imagined, and uncertainties are managed.

As CSS has tended to focus on the discursive construction of security threats (Campbell 1998b), practices of exceptionalism (Agamben 2005), or the role of sovereign and biopolitical power in governing life (Dillon & Lobo-Guerrero 2008). While these interventions have been crucial in expanding the field beyond traditional state-centred threat logics, they often foreground the spectacular, the publicly visible, and the discursively constituted. In contrast, this thesis draws attention to the technical, procedural, and practices, through which security is achieved and maintained in mundane, unspectacular ways.

By focusing on standards and standardisation, as well as forecasting and training as security techniques, this thesis demonstrates how security is not only about responding to threats, but also about the anticipatory governance of uncertainty. In doing so, it contributes to a growing literature on anticipatory security (Amoore 2014, Anderson 2010a, Anderson & Gordon 2017, Aradau & van Munster 2011). While oftentimes operating in the mundane everyday, and in technical ways, these anticipatory security techniques are biopolitical. They shape who and what is protected and for how long. This thesis thereby advances a strand of Critical Security Studies that is concerned with the everyday, infrastructure and the dispersed practices and temporalities of security and securing (Anderson 2010a, Aradau & van Munster 2011). It contributes to calls within CSS for more grounded, ethnographic accounts of how security is practised (Mc Cluskey et al. 2022) beyond high politics and exceptional events (Adey et al. 2015).

In addition to this contribution to CSS, the thesis also engages with and contributes to interdisciplinary debates in infrastructure studies, human geography, and the study of socio-technical systems. It builds on work that conceptualises infrastructures as relational, contingent, and always in the making (Larkin 2013, Star 1999). This work is extended by demonstrating how a particular infrastructure is secured by managing uncertainties. In doing so, it bridges theoretical debates in CSS with empirical insights from infrastructure studies and science and technology studies (STS). This contributes to an emerging body of work that understands security not just as a response to risk, but as a condition of (infrastructural) life (Aradau & Van Munster 2007, 2011, 2012, Collier & Lakoff 2015, 2021, Howe et al. 2015, Lundborg & Vaughan-Williams 2011, Easterling 2016).

To operationalise the aim of understanding power grid security and answering the thesis research questions, this thesis engages with how specific actors around the German electricity transmission networks manage uncertainty to ensure that 'the lights stay on'. These are the regional security coordinator (RSC) TSCNET, and the transmission system operators (TSOs). While the TSOs are legally responsible for upholding the security of the electricity supply, TSCNET is regionally coordinating the TSOs' actions to enhance grid security (TSCNET 2022, European Commission 2017a). They engage with uncertainty in the everyday, both for the everyday and the extreme: the blackout. In the seemingly mundane everyday, they incubate and prepare their ability to secure and ensure the uninterrupted flow of electricity against its potential catastrophic disruption.

In answering the research questions, this thesis describes and discusses how three mostly overlooked techniques, namely i) standards and standardisation, ii) forecasts, and iii) training, are deployed by TSOs and the RSC to secure against and manage uncertainty. In examining how these techniques 'work on uncertainty', 'relate to a future' and 'secure by', their individual contribution to power grid security will be highlighted. However, this thesis argues that only in combination are they able to secure against different uncertainties threatening the power grid and electricity flows.

Securing the contemporary German power grid was approached primarily through a research design utilising ethnography and participatory observations. In addition, these were flanked by a document review and interviews. The qualitative methodology and ethnographic focus were chosen as they allowed for locating, making visible and problematising where and how the flow of electricity is secured in the everyday. As an infrastructure, the functioning power grid is mostly transparent in the everyday (Star 1999) while it is operated and secured primarily by those working in the 'shadows' and shielded from public eyes and access.

The empirical research was conducted throughout 9 months from April to December 2021. This duration of fieldwork was necessary as I conducted security research in a critical infrastructure and during the global COVID-19 pandemic. Besides the difficulty of gaining access, building trust, and relationships with the actors I wanted to engage with, I had to wait out COVID-19 waves. During these times, access to the personnel of TSOs and the RSC, TSCNET, was not permitted as they were deemed critical for continued grid operation. Yet, ethnography and participatory observations were possible from September to November 2021 and between COVID-19 waves. In this timeframe, I conducted a three-month ethnographic study with the regional security coordinator (RSC) TSCNET. Spottier participatory observations were conducted at the German 'transmission system operator' (TSO) Transnet BW.

The following two sections on infrastructure security and understanding power grid security broadly introduce and explain why and when infrastructures and the power grid become critical and in need of security. Understanding infrastructural security requires understanding how infrastructure became critical and embeds power grid security into a broader narrative of critical infrastructure security (Aradau 2010, Collier & Lakoff 2008, LaPorte 2007, Brown et al. 2006). Infrastructural criticality is engaged as being constructed, relational, contextual, and resulting from growing individual and collective dependence on infrastructural services (Collier & Lakoff 2008, Star & Ruhleder 1996). Regarding its security, two broad narratives of critical infrastructure securitisation follow. One positions critical/vital system security as the development of military thinking that, over time, was adopted by civilian entities. The other engages specifically with the German context and describes critical infrastructure protection as a core task of the nation-state.

Following the general introduction of infrastructure security, an overview of the challenge and stake of power grid security, the blackout, is introduced. An overview of the disruption that potentially threatens the power grid aids in understanding the security regime and individual techniques necessary to secure the grid. Understanding how the grid can fail underlines why this thesis focuses on how the power grid is secured and potentially dangerous uncertainty managed in the everyday. Finally, the introduction concludes with an outline of the overall thesis.

1.1 Infrastructure Security

The power grid is a specific type of infrastructure that enables the flow of electricity. Understanding and engaging with the questions of what infrastructure is, how it became critical, and how it is an object of security, lays the foundation for the central discussion of this thesis: power grid security and how uncertainty is managed.

This section traces the origin of infrastructure as a term and a relational concept. It follows how infrastructures became 'critical' and provides two different conceptualisations of infrastructure security. Drawing from Collier's and Lakoff's (2015) idea of "vital system security" and Forsthoff's/Folker's (1938, 2017b) "existential provisions" allow for the realisation of the growing importance of infrastructure. This background narrative of infrastructural security showcases a tension between security techniques positioned to secure infrastructures against extremes and in the everyday. As references that inform the empirical discussion, Collier and Lakoff's and Folkers work point towards the need to secure against uncertainty in different ways. Furthermore, their narratives highlight how infrastructural security is co-produced between the state and the private sector and primarily performed in the everyday. This focus on the everyday provides an opportunity to link this thesis to ongoing debates within geography and Critical Security Studies, and the biopolitical perspective chosen.

'Infrastructure' is a derivative of a French engineering term. In the late 19th and early 20th century, it was first used to describe the work that was required "beneath" railroad tracks or "prior to" (Carse 2016: 29) the erection of superstructures. This specialised meaning took on new meaning and morphed into a broadly used term by the late 20th century (Carse 2016). Growing from embryotic technological advancements, they consolidate as 'infrastructures' at a point where one standardised way of erecting, operating and imagining them becomes hegemonic (Larkin 2013, Hughes 1983). Through this, infrastructures become the foundation or "installed basis" (Star 1999) for other technologies. They become "things and also the relation[s] between things" (Larkin 2013: 329), while being material as much as immaterial. Meaning, infrastructures are the material, built networks that enable circulation and flow through space and time (of electricity, power, water, information, and ideas, etc.) while being networks of links and relations, information and knowledge, resilience, and vulnerability.

Infrastructures are relational and influenced by their surroundings as much as they are "world-making" (Carse 2016: 31). They are connected and shaped by military, political, economic and social endeavours (Star & Ruhleder 1996). Similarly, Nolte (2022: 45) writes, "[…] that the criticality of an infrastructure is assigned to it in a process of securitisation". Infrastructures and their criticality take form through routinised practices (Berlant 2016, Engeström 1990: cited in, Star & Ruhleder 1996) while simultaneously being a constantly changing "practice" (Lawhon et al. 2018: 725, McFarlane &

Silver 2017). Thus, the moment of the designation of infrastructure as such or as critical is never singular or neutral but always a politically negotiated plural (Larkin 2013, McFarlane & Rutherford 2008, Latour 1988).

While infrastructures have existed since ancient times — the Roman road networks, medieval castles and cathedrals, or the fortresses of de Vauban – it was only through the relationship between liberal ideas, practices and the quality of infrastructural networks that infrastructures and their failure became loaded with political significance (Otter 2007, McFarlane & Rutherford 2008, Harvey & Knox 2012). As powerful (political) promises (homogenous secured access and affordability) and visions (progress through modernisations) (Bridge et al. 2018, Luque-Ayala & Marvin 2016, Schwenkel 2015, Harvey & Knox 2012, Graham & Marvin 2001), infrastructures were increasingly imagined to become 'organic parts' of our everyday life (Graham & Marvin 2001: 74). Their catastrophic failure then started to threaten not only lives and lifestyles, but connected to it also the legitimacy of the state and its most basic promise of protection: the survival of its population (Anderson 2021, Petermann et al. 2011a, Harvey & Knox 2012, Neyrat 2016).

Infrastructure, as a relational concept (Star & Ruhleder 1996), is not critical in itself, but it becomes critical, vital, or essential through processes of labelling and construction. Simultaneously, however, infrastructures today carry very real relationships of dependence of lives and lifestyles on their uninterrupted service provision. The designation of infrastructural criticality is, primarily, a political act. Under the "mantel of criticality", writes Steele et al. (2017: 76) and relating to Bijker (1995) "socio-economic and political interests congeal". Like labelling and designating networks as infrastructure (Goode 2014), calling infrastructure critical attaches ideas, ideals and hopes to them (Wakefield 2018, McFarlane & Rutherford 2008, Barry 2001). Critical, vital, or essential are labels assigned to infrastructures to signal their importance for specific populations and purposes. These labels then help to justify socio-political security regimes that promise the continuity of certain infrastructural services. Understanding infrastructural criticality entails asking for whom infrastructures became and are critical, in what ways, when, and at what scale (cf. Steele et al. 2017).

While Foucault (1984) recognised the political significance of infrastructure at the onset of the Industrial Revolution in the 18th century, it was only after these early infrastructures were established as the "installed basis" for follow-on infrastructures (Star 1999) that their dysfunction became a reflexive risk (Steele et al. 2017, Collier & Lakoff 2008). Infrastructural criticality turned into a reflexive security concern as infrastructure networks grew together during the early and mid-20th century, and an ever-larger part of the population became reliant and dependent on their services. 'Infrastructural services' here highlight that what renders an infrastructure critical primarily relies on the service (electricity, water, communication, etc.) they continuously and efficiently supply and enable.

The moment's infrastructures become critical, are heterogeneous. Infrastructural criticality becomes (acute) in instances of 'too much or too little' eventfulness (Anderson & Gordon 2017) or flows (power, water, etc.). This eventfulness and flow can be problematic in the nodes where they are controlled and in the 'in-between', as Forman (2018) points out using the example of gas networks. The excess or insufficiency of eventfulness or flows can originate from within or outside the infrastructure, local or global. Criticality can arise from unanticipated (technical) failures, (human) errors (Reason 1990, Carnes 2011), glitches (Berlant 2016), or natural disasters, as well as from intentional acts of terrorism and sabotage (Coaffee et al. 2009), or as part of military strategy and warfare (Graham 2005, Edwards 2003). As a systemic function, modernist infrastructure can also 'reflexively' become critical in and

through itself (Esposito 2011, Beck 1992, Der Derian 1992). Through "tight-coupling", as Perrow (1984) coined it, a multiplicity of components and their non-linear interrelations can be the common cause of failure, escalate, or cascade (Little 2002). Even if the primary effects of failures seem mild, secondary effects can lead to potential and difficult-to-predict downstream issues (Lakoff 2020, Pescaroli & Alexander 2015, Cowen 2010).

In the understanding of Perrow (1984) and Pescaroli & Alexander (2015, 2016, 2018), the looming potential of cascading failure is a distinct attribute of critical infrastructures as complex systems. The idea and argument of the power grid being a complex, thus uncertain, infrastructure will be further explored in the following section. Regarding infrastructural security, a complex system can generally be characterised by the possibility of cascading failures as a function of the number of its components and non-linear interrelations (Perrow 1984, Pescaroli & Alexander 2015, 2018). If a complex system has a lack of "slack" (Perrow 1984), meaning a lack of redundancies and overcapacities, or contextual "magnitude of vulnerability" (Pescaroli & Alexander 2015: 65) this can lead to small events escalating or cascading to system failure. Escalating or cascading failure holds the potential to amplify and evolve emerging events over space and time, drastically. The possibility of systemic failure is two-stage. It first occurs in the directly affected infrastructure but can radiate out and cause secondary and tertiary failures in neighbouring interdependent infrastructures. As virtually all critical infrastructures critically depend on the power grid to support their functioning, the potential for escalating and cascading catastrophic failure is particularly high in the event of a blackout (Foster et al. 2004, Petermann et al. 2011b).

In the style of Perrow (1984), infrastructural failure ranges from 'normal incidents' to catastrophes. 'Normal incidence' here means unfolding 'events' that do not cross the threshold into the exceptional yet already require a deviation from 'normal' operations (Anderson & Gordon 2017, Anderson 2016). They appear regularly enough to have established routines and procedures in place to manage them, while also appearing irregularly enough to be distinct from the everyday chatter. Catastrophic disruptions to infrastructure services lie at the far end of this spectrum, such as the blackout, which is discussed in the following section.

Security, while often associated with the management of exceptional disruptions (Agamben 2005) is increasingly understood to be enacted in the everyday and realised through technical, dispersed, and anticipatory practices. Within Critical Security Studies, Aradau & van Munster (2011, 2012), Dillon & Lobo-Guerrero (2008), and Amoore (2014, 2013) show that contemporary security regimes govern not through singular moments of sovereign decision, but through techniques that manage uncertain futures. In human geography, Anderson (2010b, 2017), Anderson & Gordon (2017) and Nyman (2021) locate security in mundane routines, background infrastructures, and affective responses to indicators that something might go wrong. From the perspective of infrastructure studies, Collier & Lakoff (2015, 2021), Larkin (2013), and Star (1999) characterise infrastructure as both a relational system and a site of invisible labour that enables life to continue without interruption. Together, these scholars provide the conceptual groundwork for understanding the everyday not as residual or secondary to crisis, but as the primary spacetime of infrastructural security.

For this thesis, the everyday refers not to the experience of security by populations, but to the domain of work carried out by the transmission system operators (TSOs) and the regional security coordinator (RSC), TSCNET. It encompasses the routine, anticipatory and often invisible practices by which electrical flows are secured via standards and standardisation, forecasting and training. In the

empirical chapters, these techniques are shown to ensure the grid against disruption by acting on second- and third-order indicators such as frequency deviations, network topology, or market forecasts. As power grid complexity precludes full system knowledge (Perrow 1994), even minor interventions in the everyday may be consequential, amplifying or attenuating latent risks. The significance of these interventions is rarely public-facing and remains obscured beneath the apparent stability of 'normal' grid operation.

In contrast to the spectacular or sovereign response to crisis, the everyday is where potential exceptions are continuously anticipated and managed. Anderson & Gordon (2017) describe this process as one in which "happenings and occurrences" are shaped into "(non) events"—disturbances that, through timely intervention, never escalate. This anticipatory logic is not about responding to an already exceptional event, but about ensuring that an emergent event never becomes exceptional in the first place. As Schulman et al. (2004) and Weick & Sutcliffe (2015) suggest in high-reliability systems such as the power grid, security is not the absence of events, but rather the constant effort to engage with the possibility of them occurring, as well as their management. The everyday, then, is the space in which the catastrophic is both incubated and deferred.

Foregrounding the everyday is not simply a matter of analytical preference but a methodological necessity. It follows a call within Critical Security Studies for grounded, empirical research that makes visible how security is practised (Mc Cluskey et al. 2022, Adey et al. 2015). Through ethnography, observation and interviews, this thesis engages directly with the sites and actors where security is enacted. Collier & Lakoff (2015: 19) argue that 'vital systems security' does not depend on "extraordinary executive powers" but on anticipatory practices that mitigate vulnerabilities through standardisation, simulation, and preparedness. For this thesis, these practices constitute the everyday labour of securing the electricity grid—not only for its continued operation, but also for the deferred possibility of its failure. The everyday is where security techniques quietly make possible the continuation of infrastructural life without fanfare, without spectacle, and ideally without notice.

Understanding how infrastructures are designated as critical is essential, as this process determines not only what must be secured but also frames the conditions under which everyday security practices emerge and become necessary (Aradau & van Munster 2011, Dillon & Lobo-Guerrero 2008). These designations shape which infrastructures are governed through anticipatory techniques, how responsibility is distributed among actors, and what levels of failure are deemed politically and socially (in-)tolerable. In Germany, what counts as critical infrastructure is defined by law (Bundesamt für Sicherheit in der Informationstechnik 2009). Critical infrastructure here "[…] comprises facilities, systems or parts thereof [… that] are essential for the functioning of society, because their failure or disruption would lead to considerable supply shortages or risks to public safety and security in Germany (Bundesamt für Sicherheit in der Informationstechnik 2009). Criticality in this definition is collective, a systemic attribute. In the Critical Infrastructure Act (Bundesamt für Sicherheit in der Informationstechnik 2016), the designation of infrastructural criticality is further demarcated through quantified thresholds. While the idea that infrastructural criticality arises from the collective importance of infrastructures for the populations' well-being, what is designated and counts as critical infrastructure differs by nation. Germany, for example, only designates ten infrastructural sectors as critical, while the US has 16 (US Cybersecurity and Infrastructure Security Agency (CISA) 2024, Bundesamt für Sicherheit in der Informationstechnik 2016).

In the German context, and indeed for most people in the West, the choice not to rely on infrastructure networks no longer exists. In theory, and within a Western context, withdrawing from public infrastructures is possible; yet, few still possess the necessary knowledge, skill sets, resources, and motivation to do so. You learn how to use infrastructures as part of your "membership" in the infrastructural system (Star 1999), and the choice to go off-grid (cf. Cross 2017) does not really exist anymore. In this context, reliance on infrastructure makes them critical as societies grow accustomed to their services and stop practising and possessing auxiliary means to cook, heat, or light their homes. Nevertheless, recognising the theoretical ability to replace these infrastructure services highlights the importance of paying attention to when and at what scale the criticality of infrastructures becomes a concern. If alternative, auxiliary means (cf. Rutherford & Marvin 2022) or stockpiles (cf. Folkers 2019a) exist to (partly) replace the infrastructure services locally, the moment the absence of infrastructural services becomes critical, it could be extended. For marginalised populations, however, the unevenness of infrastructure networks already renders their services, making them critically unavailable, unaffordable, intermittent or disrupted in the everyday (Graham & Marvin 2001, McFarlane & Rutherford 2008).

The recognition and declaration of infrastructures as critical for the continuation of life is a process that Collier & Lakoff (2015: 20) describe as a "relatively recent 'event in thought' (Foucault 2005: 9)" It is an event whose origin is attributed to the beginning and middle of the 20th century. Collier & Lakoff (2015, 2008, 2021) diagnose the potential for cascading infrastructure failure as a systemic problem requiring a particular kind of security. Thus, they advance the idea of 'vital system security'. In the early and mid-20th century, "military and civilian bureaucracies […] constituted system-vulnerability as an object of thought" (Collier & Lakoff 2008: 4, 2021).Infrastructural vulnerability gained relevance due to the economic turmoil of the great depression in the early 1930th and the emergence of 'total war' that extended to all aspects of life and industrialised warfare (cf. Clausewitz 1976).

Vital system security addresses concerns of systemic uncertainty. It addresses "events whose probability cannot be precisely calculated [the effects of strategic bombing or nuclear war], but whose consequences are potentially catastrophic" (Collier & Lakoff 2015: 22). As "a significant mutation in biopolitical modernity", it aims to protect the health and well-being of a population from the reflexive risks of infrastructural dependence. It does not protect through "statistical analysis of past events" but through "simulation and enactment of future events" (Collier & Lakoff 2015: 21). Simulation and enactment are tools developed and deployed by both civilian 'New Deal' and military planners in US governmental institutions and private corporations such as RAND, Herman Kahns Hudson Institute or CSIS (Collier & Lakoff 2021, Lakoff 2008, Geist 2019). For this thesis, however, infrastructure and power grid security are based neither on a statistical analysis nor just on simulation and enactment of future events. Rather, the empirical chapter show that their coming together through individual security techniques allows for a broader range of uncertainties and possible contingencies to be managed and secured against.

In terms of who provides vital system security for the power grid, this thesis understand security as co-produced between the state and the private sectorThe following pages highlight the growing historical relevance of private actors in power grid security, which justifies the focus of this thesis primarily on such actors. However, for Collier & Lakoff (2021, 2015, 2008) vital system security was and largely remains the responsibility of the nation-state**.** Yet, as the destructive capability of nuclear

weapons grew, the 'appetite' for state-led civil defence declined in light of its perceived 'uselessness' (Geist 2019). Nevertheless, "the problem of governing emergencies did not fade away", and so "techniques initially invented to address sovereign state security […] were increasingly used to address problems of domestic governance" (Collier & Lakoff 2015: 39). For the US-American context Collier & Lakoff (2008: 15) locate what would later be called critical infrastructure security, the generalisation and increasing privatisation of vulnerability analysis and response planning in the 1960s and 1970s. With the creation of the US 'Federal Emergency Management Agency' (1979), formerly exclusively military calculus became institutionalised in civilian all-hazard and contingency planning and (infrastructural) vulnerability assessments (Collier & Lakoff 2008, Wilcox & Garrity 1894). Furthermore, Folkers (2017a) highlights that these techniques further permeated the private sector and were foundational for business continuity management.

The breakthrough of 'critical infrastructure protection' and its coinage as a pronounced national security problem is locatable in the US Clinton administration (Clinton 1998, 1996). Yet, it was the events of 9/11 that propelled it into "the centre of domestic security doctrine" (Collier & Lakoff 2008: 28). In this moment of dismay, critical infrastructure protection succeeded in gaining the sustained political and bureaucratic allies it needed, and civil defence never had (cf. Geist 2019). The reliance on imagination, on the 'what ifs' and 'what could happen' characterises the post 9/11 security landscape (Anderson 2010b, Amoore 2014, Amoore & De Goede 2008, Massumi 2007, Rumsfeld 2002). As had the potential extensive destructiveness of nuclear weapons during the Cold War (Collier & Lakoff 2021, Geist 2019, Ghamari-Tabrizi 2005), the lack of data on potential threats, such as terrorism or critical infrastructure failure, requires different techniques to secure against them. In the context of power grid security, imaginative ways of securing are one way of countering uncertainty and receive more attention in the chapter on standards and standardisation.

From the German perspective, the concern for what today is called critical infrastructure protection emerged largely independently from US developments. It developed not primarily from a militarised debate on infrastructural vulnerability but from a discussion centred around the state's responsibilities for the well-being of its population. Pioneering this thought was the German constitutional lawyer Ernst Forsthoff (1938). He shared with Collier & Lakoff (2015) the concern for the increasing dependency on vital infrastructural services. For Forsthoff, Folkers (2017b) argues security was not understood as the absence of harm but positively the availability and access to vital infrastructural services. The state, or rather the state's bureaucratic apparatus, was, for Forsthoff (1938), responsible for providing these "existential provisions" (Daseinsvorsorge) (Folkers 2017b: 862). Similar ideas and frameworks of state-led provision existed in other nations simultaneously and have "contributed to the materialisation of the 'modern infrastructural ideal' (Graham & Marvin 2001)" writes Folkers (2017b: 867). With "splintering urbanism" (Graham & Marvin 2001), progressing neo-liberalisation and the alluring ideas of "the end of history" (Fukuyama 1989), the techniques of infrastructural provision and security changed. Infrastructures (including those deemed critical) became liberalised, and 'natural monopolies' were dismantled from around the 1980s onwards. The German government retracted from its direct involvement in infrastructural provisions. For the energy sector, today and after its liberalisation in the late 1990th, the mainly privately operated transmission system operators (TSO) shoulder much of the responsibility to guarantee the uninterrupted, or at least quickly recovered electricity flow (European Commission 2017a). Furthermore, the end of the Cold War in 1989 rendered one of the single most tangible rationales for state-led security provisions obsolete. These processes left behind an "institutionally fragmented environment" (Bruijne & Eeten

2007) in which infrastructural security increasingly became a “co-production” of public and private (Nolte & Westermeier 2020) as well as “extra-state” actors (Easterling 2016). This co-production, however, also extends into the supranational as the European Union is partly an infrastructural project (Opitz & Tellmann 2015, European Commission 2008) and is increasingly involved in critical infrastructure protection (European Commission 2006a).

In this splintered and fragmented security landscape, the concepts of 'vital system security' and 'Daseinsvorsorge' independently morphed into what today is widely regarded as ‘critical infrastructure protection/security’. For the German concept of ‘Daseinsvorsorge’ (existential provisions), Folkers (2017b: 868f.) observes its transition from an ideal that fosters “unity in living conditions” to one where the state, through critical infrastructure security, becomes a mere “warrantor of last resort”. This warranty is primarily provided indirectly through the delegation of its duty to “protect” to private entities rather than through “active provisioning” by the ‘state’ (Folkers 2017b: 869, Easterling 2016). The infrastructural provisions through which the state was to guarantee a ‘good life’ are replaced by a “minimum warranty” (Folkers 2017b), that is, to ensure the now private provision of critical infrastructural services. This minimum warranty is primarily located within the standards and standardisation discussed in Chapter 4. Furthermore, the state's focus on a minimum warranty requires to focus on averting exceptional and extreme forms of infrastructure failure in the everyday. Faced with an extreme, such as the blackout (discussed in the following section), the state and the private providers of critical infrastructures would (partially) fail their duty to protect. The eventuality of the extreme event would likely exceed the public and private security provisions (Petermann et al. 2011b, Foster et al. 2004).

Critical infrastructure security in a neo-liberal context refocuses the goal of securing and protecting (critical) infrastructure to “a minimal biopolitics of bare life and survival rather than an extensive biopolitics of good life” (Folkers 2017b: 869). More nuanced, however, this minimum warranty is sufficient in guaranteeing a ‘level of security’ proficiently safeguarding a ‘good life’ within the margin of the everyday, or normal incidents. The definition of this margin, of what is “safe enough” (Wellock 2021), of what is deemed the ‘minimum’ is increasingly dominated by (neo-) liberal economic rationales. The retrospectively short-sighted pay-out of the ‘peace dividend’ after the Cold War diminished ‘security’ budgets, infrastructure, and knowledge stands out as examples. As “privatisation led to a decline in the willingness and sense of responsibility of service providers to implement security measures”, writes Folkers (2017b: 868, 2017a), infrastructural liberalisation itself increasingly appeared as a potential threat to critical infrastructure security.

For this thesis, these two narratives of infrastructural security (Collier & Lakoff (2015), (Folkers 2017b) point towards three relevant aspects for further discussion on power grid security. First, they signal a tension between the security of the everyday and against extremes. To remain within the margins and avoid an event from escalating or cascading, it is required to manage uncertainty primarily in the everyday (Anderson & Gordon 2017, Anderson 2016, 2017). As the state receded from providing existential provisions (Folkers 2017b), the importance of securing the everyday, and engaging with potential extremes in the everyday, is increasing. The potentially catastrophic event, such as the blackout, must be stopped before it becomes extreme or catastrophic, as we are ill-prepared for it (Petermann et al. 2011b). Secondly, the two narratives of infrastructure security highlight how infrastructural security today is co-produced between the state and the private sector. As detailed in Chapter 3 when the research methodology is presented, engaging with transmission grid operators

and regional security coordinators recognises this, but focuses on the private actors. Yet, the state, or rather the supranational European Union, retains a prominent presence that will come out especially in the empirical chapter on standards and standardisation and through their industry-defining legislation. Thirdly, Collier & Lakoff (2015) highlighted a way of managing uncertainty to prevent extremes in the everyday through possibilistic, scenario-driven security techniques. This specifically informs how one security technique discussed in the empirical chapter will 'work on uncertainty', 'relate to a future' and 'secure by'.

1.2 Understanding Power Grid Security

The previous section broadly introduced infrastructure and how it became critical and an object of security. In turning towards the power grid as a specific form of infrastructure, this section presents the unique security challenges of the electricity grid. The power grid first requires constant security, as electricity generation must constantly and almost instantaneously be balanced with demand. Secondly, due to its vastness and our absolute dependence on its services, the stakes of power grid failure are higher than in other infrastructures. Both security challenges largely stem from the grid's complexity, that is, the number of grid components and their interrelationships. The complexity of this infrastructure denies its operators full knowledge and propagates systemic uncertainty.

In principle, the power grid consists of generators, transmission and distribution lines, as well as consumers. Depending on the amount of energy the components generate, transport, and consume, they are located at different network levels. Large conventional and nuclear power stations, as well as large hydroelectric dams, wind- and solar parks, produce in the low range of gigawatts, or in the high megawatt range (1 GW = 1000 MW = 1,000,000 kW). To minimise transmission losses, the electricity generated by around 2000 conventional and renewable (pooled) power stations (EnBW 2024) is transformed to ‘maximum voltage’. In Europe, this usually means 220, or 380 kilovolts (kV). When branching out to consumers, three further levels are passed through: ‘high voltage’ (110 kV), ‘medium voltage’ (10, 20, 30 kV), and ‘low voltage’ (400 V), until the electricity reaches a household. Langer consumers can be connected to the higher voltage levels. Besides the generating stations or fields, the substations are the essential nodes of the power grid. In them, electricity is not just stepped up and down, but power flows are measured, controlled and routed. In Germany, there are around 300 substations just for the transmission grid (EnBW 2024) and in my hometown of Gießen, around 930 for the high to low voltages.

Electricity, like gas, is difficult to detect and not always visible. Although, like gas in that electricity can be experienced through mediation by gauges that visualise, smell, or sound (cf. Forman 2017, 2018, 2020), electricity cannot be stored easily and in large quantities; it is volatile. The lack of storage (that is continuing despite a growing amount of grid-connected battery capacity) means that the demand or electricity consumption must instantaneously be matched and equalised with electricity generation. Distinguishing forecasts as security techniques from the ‘real-time’ management of the grid, the temporality of this balancing process will be further examined in Chapter Five. The indicator used for measuring the balance between demand and generation is the frequency of the alternating current (AC) of 50 Hertz (Hz) in Europe. Beyond a narrow bandwidth, either too much or too little, generation or demand would increase or decrease the current's frequency, indicating a potential problem. If an imbalance is not counterbalanced timely, it ultimately could lead to a blackout.

Orchestrating the power grid’s components and flows in each control zone (four in Germany as a historic anomaly, as seen on the right-hand side of Figure 3 on page 40) is the job of the transmission system operators (TSOs). The later empirical chapters will highlight three distinct techniques TSOs deploy to manage the grid. Each of these techniques will be shown to address the problem of systemic uncertainty stemming from the grid's complexity differently. The sheer number of components and their hard-to-calculate interdependencies inject uncertainty into the system. Furthermore, old truths are also changing. For example, the generation and demand patterns (historic data) that partially inform the grid operators' present and future decisions are changing due to the ongoing energy transitions. While generally larger patterns of consumption emerge and become known from the

accumulated flows (gridradar.net 2020, 2021, Powells et al. 2014), these can only partially serve to inform what is to be expected. The future demand largely remains uncertain, while the complexity of this infrastructure limits precise knowledge of the effects of present action.

For Charles Perrow's (Perrow 1984, 1994, Le Coze 2020) and in normal accident theory, the uncertainty within complex systems, like the power grid, is systemic. It stems from the number of components that interact in non-linear and sometimes unexpected ways, making local or total system failures hard to predict. Additionally, the tight coupling of the system as a whole, the time-sensitivity of processes and interdependences leave little room for error correction or human intervention. For the power grid and due to its complexity, small failures can remain hidden in the everyday, unexpectedly emerge, combine and lead to escalating and cascading system failure. Components can suddenly fail, or forecasts about demand and generation can be inaccurate, propagating originally local events to distant control zones, or even the entire network. The preface's example of the Emsland Case introduced an example of a cascading system failure.

With numerous potential vulnerabilities, the grid inherently poses a risk of catastrophic failure. Faced with multiple avenues of failure, the power grid's security will later be shown to be multiple, rather than singular as well. Ideally, it consists of an array of security techniques and technologies that complement each other to secure and, if necessary, restore the overall flow of electricity. Power grid security is a delicate balance between the need to ensure the everyday flow of electricity and grid operation, while also preparing for potential failures and extreme events, such as a blackout. Engaging now specifically with the blackout as an event of catastrophic infrastructural failure provides a negative picture to emphasise the unique stake of everyday power grid security.

All infrastructures deemed critical in Germany rely on the steady flow of electricity to function. A prolonged and widespread power outage or blackout would result in their cascading collapse (Pescaroli & Alexander 2015, 2016, Pescaroli et al. 2017). Where stockpiles of auxiliary means to pump blood, air, water, sewage, fuels, or information exist, they are insufficient to meet the public's demand over an extended period and a large affected area. In a report to the German Parliament, Petermann et al. (2011b: 32) highlight this when they wrote:

> "[…] [In the event of a blackout] even after a few days, it is no longer possible to guarantee area-wide supplies of vital/necessary goods and services to meet the population's requirements within the region affected by the blackout. Public safety and security is jeopardised; the state can no longer meet its duty of protection […] to protect the life and limb of its citizens."
>
> (Petermann et al. 2011b: 32)

To understand how the power grid is secured daily, it is essential to recognise the disruptions that can potentially threaten its operation. Here, the blackout takes a central role as the nemesis of grid security. It is the latent potential that the grid operators ultimately aim to secure against. Although the term 'blackout' is colloquially used to describe the loss of consciousness, amnesia, censorship, or the halt of communications, it appears here to describe the failure of the grid to provide electricity. This failure is distinct from general power outages in both spatial and temporal scales. As an extraordinary event, it exceeds expected "everyday emergencies" (Anderson 2017: 469). In Germany, for an outage to classify as a blackout, the outage is usually understood to extend over one or more transmission network areas (BBK 2019), affecting regions to continents rather than singular locations. In this geographically coined understanding, its duration is less deterministic for classification. Yet, its

duration determines its catastrophic potential (see Figure 1). When short-lived, even if widespread, like in the preface's Emsland case, it might just be a non-event for most (Nye 2010). Being long-lasting (days to weeks) and widespread, the blackout unfolds its potential for catastrophic disruption as an extreme event.

Related to the blackout and only named for clarity are brownouts, load-shedding and the 'black start'. Load shedding or brownouts are last-resort emergency measures used to safeguard a continued energy supply to a percentage of consumers if demand exceeds the available supply. They are distinct in the temporality of the events they cater to. Load shedding occurs if, due to a sudden disruption, an immediate imbalance of demand and generation exceeds the available reserve power, and connected frequency deviations demand acute intervention. Conversely, a brownout is a measure to manage chronic electricity shortages by curtailing power to parts of a population on a rolling basis. Examples of brownouts in Europe can be found during the Second World War, in strike-hit Britain of the seventies (Colvile 2006), or in East Germany during the catastrophic winter of 1978/79 (Mitteldeutscher Rundfunk 2015). While brownouts today are rare events in Europe, load shedding remains an occasional event, usually accompanying more significant transmission grid events, such as the system splits that occurred in January 2021 (ENTSO-E 2021b), or the Emsland Case, is engaged in the preface.

The 'black start' is an emergency measure that should allow for a quick recovery from a blacked-out power grid. When all lights go out and an entire control area is blacked out, each European TSO is legally required to be able to restart, to 'black start', power generation in their control zone (European Commission 2017a). For this purpose, specific 'black-start-capable' power stations, such as pumped storage or hydroelectric, are required to restart and re-energise the grid, independently from outside sources (European Commission 2017c, a). Small islands of consumers and other power stations would be re-energised by these power stations and successively grow and reconnect the individual islands to a functioning and interconnected power grid. To date, a total blackout over the entire interconnected European power grid has never occurred. The network broke apart in the preface's Emsland Case, and only a fraction of the European population was blacked out. Yet, a total blackout remains a possible scenario.

As a catastrophe and extreme, the blackout is positioned between disaster and apocalypse (cf. Neyrat 2016). As the above quote by Petermann et al. (2011b) highlights, it holds the potential to result in extraordinary loss of life and sustained disruption of populations and infrastructures (Foster et al. 2004, Petermann et al. 2011b). To state this catastrophic potential is not to catastrophise (Ophir 2010) or exaggerate but to recognise the interdependence of electric power and modern Western lives. For Aradau & van Munster (2011: 5), a catastrophe is "the intensification of disaster on a gradual continuum of destruction". As such, it "overwhelms the supposedly normal course of existence" while carrying "away the instituted order, habits and habitation, ways of life" (Neyrat 2016: 247). As a form of infrastructural breakdown, catastrophic blackouts, as well as 'ordinary' outages, are moments of (collective) "disempowerment" and "demodernisation" (Graham 2010) capable of "decompressing" electrified space (Nye 2010: 184). They disempower as they rob the affected of their ability to continue with their 'normal' modern "motorised, mobilised, mechanised routines of urban societies and economies" (Graham 2010: 59). Blackouts demodernise as electrified tools, and all (inter)dependent infrastructure deny their service. Seemingly archaic techniques re-dominate the daily routines. They decompress as electricity-enabled efficiencies compressing time and space (Altvater 1994, Marx 1993,

Harvey 1990) are reverted. Preparing food (if still available) takes longer on camping stoves or over an open fire, while travel (after the gas tanks of cars are empty) becomes primarily humanly powered. Yet, differing from the apocalypse, where the hope for salvation is provided mainly through religious beliefs, hope in the restoration of 'normality' remains.

The potential threat posed by a blackout is a product of our growing individual and collective dependence on networked infrastructure. Only after electricity penetrated and became critical to everyday life in the middle of the 20th century did its absence become a potential catastrophe. In the pioneering days of Western electrification, many different voltages, frequencies and currents existed, while faults and outages were common (Hughes 1983). Nevertheless, they were not regarded as abnormal or out of the ordinary, and blackouts, in today's understanding, did not exist (Nye 1999). The electricity customers (as with other infrastructures) were accustomed to the unreliability of electrical appliances and supply, thus continuing to have alternative means to cook, light and heat the house, move around, or communicate with others. It was only after more affordable and reliable "electricity wove networks together, [that] power failures became less and less tolerable because they shut down entire infrastructures" (Nye 2010: 27). With increasing standardisation, interconnectedness and coverage infrastructure networks (including the power grid) throughout the Second World War and the 1950s were thought to become critical 'life-support systems' (Gandy 2005). Meaning the well-being and survival of a population are increasingly dependent on critical and "vital" infrastructures such as the power grid (Collier & Lakoff 2008).

Through the infrastructural interconnectedness, interdependency, or "tight coupling" (Perrow 1984), a blackout today would significantly affect the functioning of infrastructures connected and relying on electricity. The longer a blackout lasts and the wider spread it is, the more damaging it is likely to be (Figure 1). Parallel to the occurring damage to lives and matter, the restoration and recovery time increases with the duration of the blackout. Furthermore, "[…] it is possible for the functional outages to become mutually reinforcing until at some point the degradation of infrastructure could have irreversible effects on the [a] country's ability to support its population" (Foster et al. 2004: 2). What allows for mutual support and efficiency gains in everyday infrastructural co-dependence, reflexively becomes a problematic potential of "escalating" or "cascading" failure (Little 2004). Due to this possibility, even minor everyday incidents, whether intentional or accidental, whether human error, technical failure, or a combination of both, hold the embryonic potential to end in catastrophe (Anderson 2017, Anderson & Gordon 2017). It is the containment, reduction or management of the potential for escalation or, as Zimmerman (2001) writes, the "decoupling, disengagement of faulty parts and the rerouting of services" that everts catastrophe, enabling quick recovery. While there is neither scope nor a need to outline infrastructural failure cascades in this introduction, a detailed study of what happens during a blackout can be found in Petermann et al. (2011b).

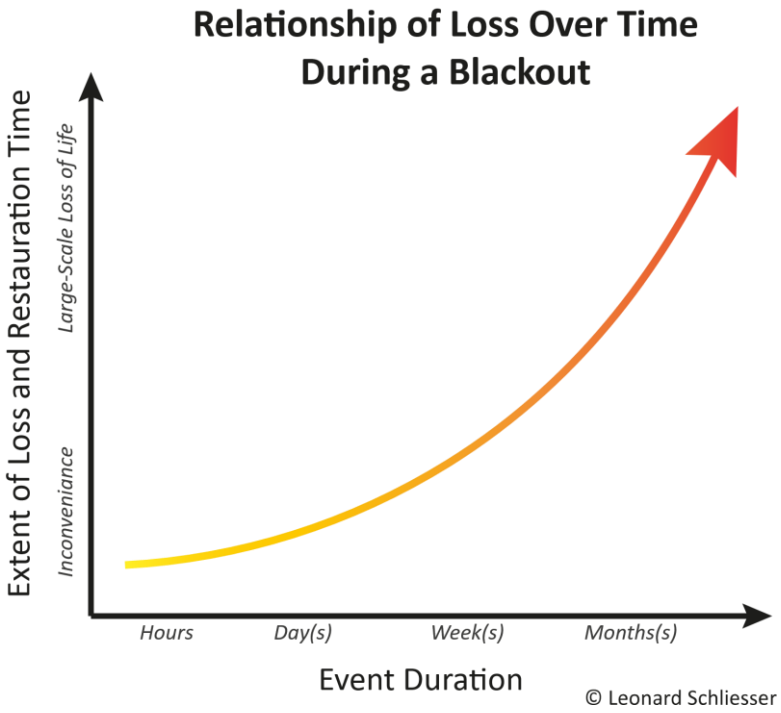


Figure 1 Relation of Blackout Losses and Recovery Time over its Duration

In their disastrous scale, catastrophes, such as potential blackouts, are maximum credible events. They are the catastrophic futures, which all security techniques employed by the grid actors try to ensure never happen. If a blackout occurs as a prolonged event, it will challenge the existing capacities and capabilities positioned to secure the well-being of populations (Quarantelli 2006, Petermann et al. 2011b, Foster et al. 2004). It would highlight the limitations of the security techniques positioned to secure against it and a contrast of a possible yet uncertain future (Neyrat 2016, Aradau & van Munster 2011). They are social, cultural and political events that disrupt routines and safeguards while uprooting the promise (whether public or private) of ensured service provision (Knox 2017, Nye 2010). As they are large-scale, low-probability, high-impact events, they rarely occur and even hardly ever unfold their full destructive potential, making securing against them ridden by difficulties (Murphy & Conner 2012, Boin & McConnell 2007).

The extreme of the blackout illustrates how the power grid operation and security are anything but straightforward. Instead, the power grid is complex. It does not only consist of many components but are also interrelated in multiple ways while constantly being rebuilt, upgraded, or retired. Electricity demand and generation (especially renewable generation) are volatile, and their balance is fragile. No single point of failure or button exists to shut down or restart the power grid. If the transmission grid fails, this mostly comes as a surprise and as a combination of factors, meaning a systemic failure (Nye 2010, UCTE 2006). The grid's potential vulnerabilities are plentiful and seam the path from electricity generation, over transmission, and distribution to the consumer. Like the gas network, the ensured operation of the electricity network depends on the security of both its nodes and the lines connecting them (Forman 2017, 2018). Threats to the continuous electricity supply can be external or internal. Threats to the grid can originate from its systemic and technical complexities (cf. Perrow 1984), from accidents, extreme weather or intentional, malicious acts. Yet, the reason for outages/blackouts might not always be clarifiable or is attributed to multiple factors (UCTE 2006, Nye 2010, OFGEM 2019).

To protect from external intrusion, power plants have their site security personnel; nuclear power plants are modern fortresses, substations are fenced-off, and transmission towers often have barbed wire to deter climbers. Surrounding the grid's physical assets, these barriers are intended to protect civilians from a high voltage as much as the grid's physical assets from (accidental) interference. In the traditional power grid, the larger an asset, the more critical it is and the better its security. Large power stations and transmission control rooms are better protected from outside interference than transmission and distribution substations and power lines. Historically, this has been and is being exploited by 'freedom fighters' (Raich 2021, Bennetto 1997), left- and right-wing extremists (Haupt 2024, Morehouse 2023, Serrano & Halper 2014) and military strategy (Graham 2005, Griffith 1994) as they attack and blow up transmission pylons or target substations.

Threats to the power grid from cyber-attacks are growing with the grid's progressing digitalisation and are thought to become a severe concern for 'smart' grids (Cisotto & Badia 2016, Ebrahimy & Pourmirza 2017). Yet, due to the separation, or air-gapping of the current grid's operational technologies (OT), such as their Supervisory Control and Data Acquisition (SCADA) systems, from their Internet Technologies (IT) used primarily in administration, this vulnerability, so far, remains a problem of second order. Furthermore, the most recent attacks on other critical infrastructures, such as the German-Russian and Finnish-Estonian sub-sea gas pipelines in 2022 and 2023, as well as the war in Ukraine, have highlighted that kinetic direct attacks on energy infrastructures are more (cost-) effective (Atug 2022).

To counteract the threats, the power grid on all levels has historically been built with many redundancies and overcapacity, ensuring operations even when network components go offline for maintenance or due to faults, failures, accidents, or attacks. For this purpose, the so-called 'N-1' principle guides network design and operation. European Commission regulation (EU)2017/1485 specifies in Article 3(2)(14) of the Network Code on System Operation that "the [grids] elements remaining in operation after […] a contingency are [must be] capable of accommodating the new operational situation without violating operational security limits" (European Commission 2017a). A contingency is the unexpected loss of a network element, such as a power line, a transformer, a generator or large consumption. Should redundancies and over-capacities not be able to accommodate contingencies, further measures, such as load-shedding or brownouts, are in place to prevent the collapse of the entire grid or to restart it after a blackout.

In conclusion, securing the electricity network is a continuous, everyday balancing act that manages the grid's inherent complexities thus uncertainties, as well as its latent potential for catastrophic failure. Even small or seemingly minor failures can lead to escalation and cascades that threaten the entire network. Working in the opposite direction, however, if small errors, failures, and anomalies can be detected in the everyday, escalation and cascading into catastrophe can be parried. To do so, the power grid possesses a suite of security and contingency techniques that aim to secure the everyday and prepare for the extreme, such as a system blackstart after a blackout. The empirical chapters of this thesis will shed light on the everyday techniques deployed in the German power grid to secure the everyday flow of electricity and against the possibility of catastrophic system failure.

1.3 Thesis Outline

In the **Introduction**, this thesis focuses on power grid security, situated in the broader context and discourse on (critical) infrastructures and their security. In **Chapter 2**, I review the literature and develop the conceptual framework for the thesis. It situates the project within Critical Security Studies (CSS) and anchors my contribution to a strand of CSS that focuses on everyday, technopolitical, and anticipatory security practices. The chapter explores how security is enacted not only through sovereign decisions or exceptional events, but also through mundane techniques that manage uncertain futures. In doing so, the chapter contributes to calls within CSS for more grounded and empirically informed accounts of how security is practised in infrastructural settings. To characterise the specific challenge of securing the electricity transmission grid, the chapter draws on a Foucauldian understanding of biopolitical security, which focuses on populations and the circulation of vital systems. This aligns with how the power grid functions to sustain life and productivity at scale. To advance and operationalise these categories, the chapter then turns to the literature on uncertainty. This body of work enables a distinction between probabilistic and possibilistic security techniques, each of which engages with uncertainty and the future in different ways. Taken together, these perspectives support a view of uncertainty as systemic, multiple, and ultimately inconceivable. Because no existing framework offers a clear overview of the range of uncertainties and their associated security techniques, the chapter introduces a typology adapted from Mason (1993, 2019, 2022). This typology illustrates the multiplicity of uncertainty and prepares the ground for the empirical analysis of how power grid security techniques— standards and standardisation, forecasting, and training—engage and manage uncertainty in practice.

In **Chapter 3,** I outline my research design and methodology, which are positioned to make visible the otherwise hidden infrastructure, as well as the different ways and multiplicity through which it is secured. This is achieved by deploying a qualitative interpretative research design relying primarily on ethnography and participatory observation. A review of relevant documents and semi-structured interviews complements these methods. Before detailing how I deployed these methods in detail, I reflect on the impact of the COVID-19 pandemic and my positionality as an active German expert civil defence volunteer.

Chapters 4 to 6 present my empirical findings, focusing on everyday power grid security techniques. They focus on standardisation, forecasting and training and highlight how the flow of electricity is secured against the uncertain potential of what might happen differently. The analytical categories deployed to distinguish them are '**work on uncertainty'**, **'relate to a future'** and '**secure b**y' developed in Chapter 2.

Specifically, in **Chapter 4**, I engage and position standards and standardisation as a security technique for the power grid. Standards and standardisation engage an unwritten future that has not emerged yet. They work on uncertainty by containing it and securing it through pre-emption. They rely on an imagined future ideal/threat to be avoided or achieved via informing present action through backcasting. The literature on standardisation is presented first and aids in classifying standardisation as both technical and procedural. This is followed by expanding on how standards and standardisation operate as security techniques of the everyday on two different scales, European electricity sector standardisation and German reserve power activation. The perspective on the everyday is followed by engaging the contribution to standards and standardisation for power grid security in exceptional situations.

In **Chapter 5,** the imaginary mode of standards and standardisation is contrasted with the calculatory mode of forecasting. The chapter opens by questioning the focus and positioning of forecasts as a security technique by contrasting it with the 'smart' and 'real-time' management of events. However, in engaging with my empirical observations, where I encountered near-instantaneous grid management, 'real-time' as a novel 'smart' and digital attribute is debunked. 'Real-time' is uncovered to rely on legacy electromechanical automation enabled through standardisation. Without its position as a security technique being challenged, forecasts are first conceptualised as such. Forecasts operate on a knowable, calculable future and aim to reduce the uncertainty of what might happen. In doing so, they offer a window of opportunity to prevent unwanted futures, potentially escalation or cascading of system failure. This is expanded through detailing three exemplary forecasts I observed and engaged with during my ethnography at TSCNET.

In the last empirical **Chapter 6**, the training of TSO operators and RSC, TSCNET operational managers (OMs) is discussed as the third technique securing the power grid. Training as a security technique is shown to be largely absent in the security literature, thus conceptualised as such first. While the future training engages is uncertain, its intent is not to contain or reduce but to manage uncertainty. It is further distinguished from standards and forecasts as training secures in a triad. First, I discuss how training enables the operators and OMs to use standards, standardisation and forecasts to pre-empt and prevent. Second, training secures as it fosters experience as a distinctive form of knowledge that the operators and OMs can fall back on when standards and forecasts fail to contain or reduce uncertainty. Third, training is positioned and demonstrated to foster precaution and vigilance, which sharpen the senses of the operators and OMs and remind them what might happen. Overall, by describing how training secures (in) the everyday and the exceptional differently, I extend and exemplify its functioning as a security technique.

In **Chapter 7,** I conclude the thesis by bringing together the analysis of the three security techniques discussed in the empirical chapters. It argues that standards and standardisation, forecasting, and training do not secure the electricity transmission grid in isolation but only do so effectively when combined and operating together. This layered and coordinated form of security is shown to be necessary to address the range of uncertainties and catastrophic potentials outlined in the introduction. This perspective offers a novel way of understanding infrastructure security—not as the effect of singular interventions, but as the outcome of multiple, everyday techniques working together to manage uncertainty. This chapter restates the thesis's contribution to Critical Security Studies by demonstrating how security is enacted through anticipatory and distributed practices within infrastructure systems. It also contributes to broader debates in infrastructure studies and socio-technical research by highlighting how security emerges from the interaction of technical routines, institutional coordination, and future-oriented work. The chapter concludes by reflecting on the study's limitations and outlining potential directions for future research. These include closer attention to the practical routines through which infrastructures are secured, and further investigation into how uncertainty is operationalised in other infrastructural or regulatory domains. The outlook is not prescriptive, but sketched, in line with the open-ended nature of the fieldwork and the systemic uncertainties at the heart of the thesis.

2. Literature Review

This chapter aims to provide an overview of the literature that, in addition to the introduction's discussion on critical infrastructure security, aids in examining the power grid as both an object in need of securing and an object that enables the securing of lives and life. This thesis does not easily fit into, but rather intersects with, the fields of infrastructural, energy, and electricity studies, as well as security studies and their respective literatures. Yet, in critically engaging with how infrastructural security is performed and sustained, it primarily draws on the field of Critical Security Studies (CSS). Specifically, it builds on a strand of CSS that focuses on the everyday practices, techno-politics, and anticipatory rationalities through which security is enacted (Amoore 2014, Anderson 2010a, Aradau & van Munster 2011, 2012, Amoore 2013). Rather than conceiving security as a response to defined threats, this literature attends to the dispersed, mundane and technical ways in which uncertain futures are governed.

While this thesis draws conceptually from Foucauldian biopolitics, its closest alignment is with contemporary CSS literature that has extended biopolitical thought into analyses of how security operates through mundane infrastructures, anticipatory practices, and technical systems. Scholars such as Dillon & Reid (2009), Amoore (2014), and Anderson (2017) have shown that contemporary security regimes increasingly govern not through sovereign decisions on visible threats but through the management of uncertainty, often via computational or organisational techniques. This thesis contributes to these debates by demonstrating how infrastructural actors, such as transmission system operators (TSOs) and Regional security coordinators (RSCs), employ specific security techniques to manage electricity as both a vital circulation and a potential site of systemic failure. It thereby brings critical infrastructure management into CSS, a domain that remains empirically underexplored.

In doing so, the security for this thesis will, in the later empirical chapters, be shown to be the coming together of security techniques—standards and standardisation, forecasting and training—that seem far removed from the subject, the grid, that they are to secure. Through a focus on security as biopolitical and preoccupied with engaging different uncertainties, this Critical Security Studies literature provides the framework that helps to unpack how the power gird is secured against uncertainty and that enables it to sustain and "let life live" (Foucault 1978).

This chapter will be divided along two strands of literature that provide and inform the analytical framework and categories through which standards and standardisation, forecasts and training are examined in the empirical chapters. The analytical categories, 'work on uncertainty', 'relate to a future' and 'secure by' originate first from a biopolitical perspective on how life and lives are secured (Foucault 1978, 2007, 2008). Furthermore, the Foucauldian biopolitical perspective is strengthened with literature on uncertainty (Adam & Groves 2007, Mason 1993, 2019, 2022). Combining these strands of literature provides the analytical underpinnings for deciphering how the contemporary German power grid is secured and uncertainties managed.

Foucauldian biopolitics offers a unique but general perspective and the analytical categories to broadly identify how the power grid is secured as a complex infrastructure in the everyday. Foucauldian biopolitics provides a toolset for identifying, locating, and visualising where and how the flow of electricity, as a form of circulation, is managed and controlled. Foucault's understanding of biopolitical security as the management of life and its basis of existence shapes the later empirical

engagement with uncertainty. In the empirical chapters, security will be demonstrated to reside in seemingly mundane, everyday practices, and through the ways standards and standardisation, forecasts, and training govern specific uncertainties.

The second section builds on and complements the previous engagement with biopolitics. It engages with recent work in Critical Security Studies that positions uncertainty as a central object of contemporary security governance (Adey et al. 2015, Aradau & van Munster 2011, Dillon & Reid 2009). This strand of CSS extends the biopolitical tradition by focusing on how uncertain futures are anticipated, governed, and rendered actionable through mundane and often technical practices. These insights provide conceptual grounding for this thesis, which examines how infrastructure security is performed through differentiated engagements with uncertainty.

While existing scholarship has offered separate accounts of how uncertainty is addressed through probabilistic or possibilistic techniques, there remains a limited empirical understanding of how such techniques coexist, interact, or are layered in contemporary infrastructures. This thesis addresses that gap by analysing how different security techniques operate not only with distinct epistemologies of uncertainty, but also in coordination, forming a composite architecture of anticipation. By bringing this conceptual insight into dialogue with grounded empirical research on the German electricity grid, this thesis contributes to CSS debates on the material practices of uncertainty governance.

Engaging with the literature on uncertainty enables us to see the multiplicity of uncertainties that security needs to address. In other words, since uncertainty and uncertain futures are multiple and potential threats, the security techniques deployed must be able to respond to this multiplicity. Only if the possible range of what is uncertain is addressed can the flow of electricity become secured. To operationalise this argument, this thesis draws on and adapts Mason's (1993, 2019, 2022) typology of uncertainty — not only as an epistemological framework but as a conceptual tool for CSS. Mason's framework supports a structured analysis of how different forms of (un)knowing inform different strategies of intervention.

2.1 Securing Life

The question of how individual and collective human lives should be secured is debated by a broad literature. Focusing on critical infrastructure security, the introduction highlighted a particular understanding of security that deviates from a 'traditional' understanding of security. For traditional security studies, (collective) life is rarely directly the reference object, as security is primarily understood as that of a nation-state, being ensured by military might, geopolitics, and a balance of power (Clausewitz 1976, Walz 1979, Herz 1950, Morgenthau 1950). Critical infrastructure security is sometimes framed alongside traditional security narratives (Alexandru et al. 2019). As an important attribute for national and union security, critical infrastructure takes centre stage in both European programs of critical infrastructure protection (European Commission 2006b) and US strategies for homeland security (Department of Homeland Security 2002, 2007). In contrast to these traditional notions of security, the introductions highlighted critical infrastructure security as relational and reflexively becoming a potential threat, not primarily to the state, but to collective life. It highlighted how infrastructures came to be seen as vulnerable, critical and vital to a population. While the introductory engagement with Collier and Lakoff (2015) located the origin of vital system security in traditional military thinking, they and Folkers (2017b) highlighted a progressive shift of infrastructural security to become a "co-production" (Nolte & Westermeier 2020) of public and private entities. The notion of critical infrastructure presented in the introduction and its literature share with critical security scholars a broadened understanding of security that is provided not just by the nation-state. Furthermore, critical infrastructure literature similarly often shares the focus on how power, governance and control are distributed and employed to secure complex, tightly coupled (Perrow 1984) networks of flows.

The literature on securing life is interdisciplinary and multifaceted. Beyond the literature on critical infrastructure security in the introduction, a wide variety of literature and approaches to securing life. Scholars critically studying security look, not least, at urban security (Lakoff & Klinenberg 2010, Coward 2009), surveillance (Zuboff 2019, Browne 2010), border security (Barry 2011, Salter & Zureik 2005), biosecurity (Lakoff 2017, Hinchliffe & Lavau 2013, Lakoff 2008, Cooper 2006), environmental security (Dalby 2022, 2002, Barnett 2001) and feminist and queer approaches to security (Hagen 2016, Browne 2015, Massey 1994). Geographers like Forman (2017) focus on overlooked security practices by focusing on specific entities and infrastructures, such as gas. Others, like Anderson (2010b) and Amoore (2013), engage with the different types of knowledge and connected temporalities that security techniques rely upon. With their perspectives, security scholars engage or question specific security concerns. However, a more comprehensive perspective is required to understand power grid security, which sits at the intersection of multiple fields (security, infrastructure, energy). While these studies address specific fields or objects of security, understanding electricity grid security necessitates a more comprehensive approach that encompasses security, infrastructure, and energy governance.

Across this diverse literature, Foucault's concepts of biopower and biopolitics have provided a shared foundation for understanding how life is governed and secured, particularly through mundane and technical means. Foucault's (1978, 2003, 2007, 2008) concept of biopower and his work on biopolitics enable a comprehensive approach to understanding security as more than state security, military power, or geopolitics. By examining how life is governed through public health, welfare, surveillance, and social regulation, biopolitical security reveals the governance of populations and circulations that extends beyond the traditional referent of the nation-state. For this thesis, a broadened understanding

of security helps identify, locate, visualise, and problematize how security is performed in the electricity transmission grid. This perspective is necessary to make visible what Star (1999) has described as "transparent" infrastructure, and to trace the often invisible or shadow work through which it is secured. It also helps to understand how the circulation of uncertainty becomes a problem for security practice. While Critical Security Studies includes other non-traditional perspectives—such as human security, feminist and queer security studies, and postcolonial (in)securities—these often focus on specific themes or referent objects. In contrast, this thesis adopts biopolitics as a more comprehensive framework that enables infrastructural practices to be analysed in relation to life, circulation, and uncertainty.

In sharing his perspective on the shift of political power through the past centuries, Foucault positions biopolitics as a distinct form of how power and control are being exerted in 'modern' times and increasingly since the Enlightenment (Foucault 2008). While biopolitics can be understood as the governmental techniques to manage and regulate a population and lives, biopower is defined by Foucault (2007: 1) more broadly as "the set of mechanisms through which the basic biological features of the human species became the object of a political strategy". In setting up his theory of biopower, Foucault details and then supplements earlier forms of sovereign and disciplinary power. This reconceptualisation of power — from sovereign control to the regulation of populations through circulatory management — laid the groundwork for critical engagements with security in later decades. In particular, it has been foundational for the development of Critical Security Studies (CSS), which builds on and extends biopolitical thought to explore how contemporary security is enacted and affects people's lives.

Sovereign power, he explains, is the monarchic absolute control over his subjects in a particular territory and allows the sovereign to subjugate the subjects to ritualised torture, creating its truth and punishment via spectacular public torture/execution (Foucault 1991). According to Foucault, this form of power faded towards the early 19th century and was replaced by 'discipline'. Discipline would still focus on the individual body but has to be produced and re/produced through the utilisation of "the instrument of permanent, exhaustive, omnipresent surveillance, capable of making all visible […]" (Foucault 1991: 214). Whereas the sovereign held absolute power, with the notion of discipline, Foucault identified a multiplication of how, where, when and by whom people would be subjugated to different forms of power (Foucault 2003: 27, 1991). Foucault exemplifies his idea of discipline by describing Jeremy Bentham's panoptic prison. Through the fear and uncertainty instilled in the inmates about being constantly watched, they would self-discipline and adapt their behaviour to a 'norm'. Moving into the late 19th into the 20th century, and through a non-linear process entwined with the rise of liberalism, Foucault (2008, 2007, 2003) describes how biopolitics began displacing, yet not wholly replacing sovereign and disciplinary power. What changed in comparison to disciplinary power was a shift in the focus from individual subjects that were to be disciplined to the governance of the 'population'. Biopolitics is distinct from the earlier forms of power as they "massify" (Foucault 2003: 243) the techniques and technologies deployed to exert power. Control and securitisation switch from being directed from the state to particular individuals and is now "to be exercised over a whole population" (Foucault 2007: 11). Whereas disciplinary power exerted biopower over a specific space and to correct 'bodies', biopolitics explores how power is exerted over the aggregate of bodies as a population with the aim "to improve the condition of the population, to increase its wealth its longevity and its health" (Foucault 2007: 105).

While Foucault's concept of biopolitics and governmentality does not presume a nationally delimited population, his analysis emphasises how populations are managed as collective entities tied to specific territories through regulatory and statistical techniques (Foucault 2007). Subsequent scholarship has extended this view by emphasising how biopolitical governance often operates through anticipatory, circulatory, and infrastructural arrangements that exceed state boundaries (Dillon & Lobo-Guerrero 2008). National legal frameworks shape infrastructures such as electricity transmission grids, yet they are embedded in broader regional and supranational regimes. In the European context, security is enacted not only through state agencies but also through transnational regulatory bodies, harmonised standards, and cross-border operational coordination. As Keller (Easterling 2016) observes, infrastructure can function as a form of "extrastatecraft", exerting power through spatial protocols and technical systems that lie beyond the formal mechanisms of state control. The referent objects of biopolitical security, a population, thus emerge across multiple and overlapping spatial registers. Because the governance of infrastructure, circulation, and uncertainty unfolds across overlapping territorial and operational regimes, it is necessary to adopt a spatially flexible understanding of biopolitics. It requires an experience that is attentive to how security is practised across national, supranational, and infrastructural scales.

Alongside these spatial considerations, biopower and biopolitics have also undergone significant conceptual development. While this thesis draws its analytical categories from a general Foucauldian perspective, it is important to clarify how these categories relate to and differ from adjacent concepts. A range of theoretical mutations—most notably necropolitics, bare life, and vital systems security—have emerged to critique or expand the initial framing of biopolitical power. They offer a compelling perspective on the relationship between infrastructure, life, and power that resonates with the concerns of this thesis. However, while they could serve as alternative frameworks, this project deliberately adopts a more general biopolitical lens. Engaging them here allows for a more precise articulation of the conceptual choices that structure the thesis.

While biopolitics holds a positive connotation towards sustaining and improving life (Foucault 1978, 2007, 2008), critics of biopolitics, such as Giorgio Agamben (1998) and Achille Mbembe (2003) contest this. Through a focus on "bare life" (Agamben 1998) and "necropower" and "necropolitics" as "the power and capacity to dictate who may live and who must die" (Mbembe 2003: 11), they write against the focus on sustaining and improving life. For Puar (2017: 35), necropolitics begins "at the limits and through the excess of […]" biopolitics, while it is biopolitics that "[…] masks the multiplicity of its relationships to death and killing to enable the proliferation of [… necropolitics]." From a necropolitical perspective, for example, the potential for extreme infrastructure failure, such as a blackout, might become pronounced and a subject for enquiry. A population critically dependent on the uninterrupted flow of electricity would be unable to sustain its life without dedicated preparations for its absence. In the debate on existential provisions touched upon in the introduction, Folkers (2017b: 864) describes this necropolitical potential of critical infrastructure when he writes:

> "The government's increased technological care [through infrastructural provisions] for life is the growing necropolitical potential of the techno-biopolitical state. *Dasein* [existence] becomes bare life left to die whenever it becomes unhitched from its infrastructural ties and finds itself abandoned in 'zones of infrastructural disconnection' (Marquardt 2017). Under techno-biopolitical conditions, to 'make life'

> means to connect life to the grids […], while to 'let die' (Foucault 2003: 241) means pulling the plug." (Folkers 2017b: 864)

As this thesis is concerned with everyday power grid security, a necropolitical perspective as an extreme form of biopolitics does not aid in uncovering how the uncertain potential of emerging events is secured. While a necropolitical perspective highlights the death-dealing potential of biopolitical regimes, this thesis is primarily concerned with the more subtle, technocratic, and anticipatory forms of governance that operate through critical infrastructure in the everyday; a concern that aligns more closely with recent work in CSS on opaque security practices (Adey & Anderson 2012, Adey et al. 2015, Amoore 2009, 2013, Aradau 2010). Yet, the blackout as a catastrophic extreme is always latently present. Its potential to disrupt and cause deaths is even higher in countries like Germany, as the excellent quality of the everyday electricity supply (Bundesnetzagentur 2023) becomes a reflexive threat that hinders preparedness measures.

Collier and Lakoff's (2015) "vital system security" introduced in the previous chapter, advances a second noteworthy mutation of biopolitics for this thesis as it addresses the reflexive risk of infrastructural dependence. They highlight the importance of complex infrastructures, designated as critical and vital for sustaining and promoting the prosperity of life. For them, "the very instruments of biopolitical government [vital infrastructures such as electricity, water systems and hospitals], which aimed to foster the health and wellbeing of the population, came to be seen as potential sources of vulnerability" (Collier & Lakoff 2015: 21). While they highlighted the everydayness of this dependence, they primarily focus on the threat of extreme "events whose probability cannot be precisely calculated" (Collier & Lakoff 2015: 22). Similarly, to the necropolitical being an extreme form of biopolitics, vital system security is primarily conceptualised against and along the lines of possibilistic threats. This constrains the ability of this thesis to analyse how uncertainty in different forms is secured against.

Another extension of biopolitics, "energopower" argues for the importance of the modalities of "harnessing electricity and fuel and vice-versa" for enabling and sustaining biopower (Boyer 2014: 309, Chandrashekeran 2022). As Szeman (2014: 456) concludes, Boyer criticises the non-recognition of energy in Foucault's development of biopolitics, as energy is "connected to the state and fate of populations." Energy is the literal fuel of circulation that keeps a population and the state alive (cf. Petermann et al. 2011b). For Boyer (2014: 327), "power" is "the ability to do something, enablement, forces that allow other forces to happen." Thus, "it would be impossible to say where the power of energy ends and that of life begins" (Boyer 2014: 327).

Previous energy discourses of energy focused on energy security and self-sufficiency (Attenberg 2009, Winzer 2011), while the energy infrastructure, such as the transmission grid, has been neglected in these discussions. Here, 'energopower' can serve as a conceptual tool to more holistically examine how energy infrastructures govern life biopolitically (Boyer 2014, Szeman 2014). Viewing the energy infrastructure through energopower might help uncover the ideologies and political imaginaries tied to this infrastructure, while also highlighting how this infrastructure itself shapes people's imaginaries and lives around it. While the concept of energopower helpfully emphasises the entanglement of energy and governance, this thesis takes a more grounded, empirical approach by focusing on how electricity infrastructure is secured in practice, through specific security techniques that aim to govern uncertainty. It furthermore does not aspire to provide a holistic analysis of power grid security across

all scales from generation, the markets, through distribution and prosumption, but rather focuses on the transmission grid.

Necropolitics (Mbembe 2003), vital systems security (Collier & Lakoff 2015), and energopower (Boyer 2014) offer critical conceptual insights into the relationship between life, (energy-) infrastructure, and governance. Yet, for this thesis, they lack the analytical accuracy required to investigate the specific practices, techniques, and rationalities through which infrastructural security is enacted in the everyday. While powerful in critique, these frameworks offer limited traction for tracing the operational logics and organisational forms that shape how actors manage uncertainty in real-time grid operations. Instead, this thesis adopts a general biopolitical lens, informed by Foucault's work on circulation, population, and uncertainty, and sharpened through recent developments in Critical Security Studies that examine the mundane and anticipatory character of contemporary security practices.

Building on this perspective, recent work in Critical Security Studies has explored how security is enacted not through sovereign decisions or military interventions, but through everyday practices embedded in systems, infrastructures, and risk models (Amoore 2014, Anderson & Adey 2012, Anderson & Gordon 2017, Aradau & Van Munster 2007, 2011). This scholarship foregrounds the role of anticipation, simulation, and mundane interventions in governing uncertain futures. In this framing, infrastructures do not merely require protection; they become active instruments through which security is performed. The empirical chapters that follow analyse how these dynamics unfold in the German electricity grid through the practices of standardisation, forecasting, and training.

Drawing together insights from biopolitical theory and recent developments in Critical Security Studies on anticipatory and infrastructural security practices, this thesis derives the analytical categories of 'work on uncertainty', 'securing by', and 'related future'. These are employed in the empirical chapters to trace how actors, such as TSOs and RSCs, manage the potential for infrastructural failure in the everyday.

Regarding the analytical category of 'work on uncertainty', Foucault's notion of circulation is essential, as it highlights how different flows, such as those of people, disease, or electricity, can become an object of biopolitical securitisation. The focus on circulation arises as securing a population requires focusing "on a range of factors and elements that seem far removed from the population itself […]" (Foucault 2007: 72). Electricity is such an element that, as detailed in the introduction, became critical for the sustainment of life and lives. On the other hand, behind the concern for controlling different circulations, such as electricity, lies their uncertain potential to threaten life and lives if not properly managed, if faulting or being blacked out. The "risky and inconvenient" circulations, Foucault (2007: 19) writes, "will never be completely suppressed". Thus, the challenge of biopolitical security for Foucault (2007: 11) becomes the management of circulating "uncertainty". This uncertainty stems from "an indefinite series of mobile elements" (Foucault 2007: 20), thus is inconceivable and inextricably becoming an attribute of life. In the case of the electricity infrastructure, this uncertainty stems from its complexity, the number of its parts, as well as the multiplicity of its potential interrelations. Understanding uncertainty as the underlying subject of securitisation forces us to engage with security in relative terms. It positions uncertainty and security as a "wicked problem" (Rittel & Webber 1973) that cannot be resolved but only managed. For the empirical engagement with power grid security, this allows and demands the identification of how uncertainty is being managed and secured against. Foucault's perspective on managing circulation and uncertainty promotes paying

attention and provides a tool to identify how different circulations differ, including their inherent uncertainty.

Regarding 'securing by', biopolitical security is giving up a totalitarian claim of control. The singling out of circulation uncertainty as a medium through which life is "fostered" or "disallowed" (Foucault 1978: 138) complicates the meaning of security. Biopolitical security for Foucault (2007) extends beyond disciplinary and sovereign control, beyond the dichotomies of right or wrong, life or death, strict limits and disciplinary perfection. It is replacing these forms of control with one that manages and balances too much or too little. Securing thus becomes the art of managing uncertainty and negative potentials despite the reflexive risk of doing too much or too little. Furthermore, it is to act even if not aware of the exact location of where these balances and thresholds lie. For the analysis of power grid security, this generally does two things. First, it focuses on the need to understand the management of uncertainty for how electric flows are secured. Second, and looking beyond the resemblance of control, it advances the need to investigate how and where the circulation of uncertainty is managed and what tools are deployed to control and secure, at least partially.

Regarding 'related future', Foucault's idea of biopolitical security emphasises the future rather than the present as the reference temporality for securing. The future is inherently "uncertain" and in need of securitisation, as it is grappling with an "indefinite series of mobile elements" (Foucault 2007: 20). Yet, in considering "what might happen" (Foucault 2007: 20), the future also imprints the present. To view security as biopolitical, this thesis also highlights the need to engage with the future's role in securing, partially controlling, and managing the circulation of electricity and uncertainty.

For this thesis, life is secured biopolitically through the proxy of ensuring the circulation of electricity, that is, trying to control and manage it. It generally provides the analytical categories to frame the engagement with the three security techniques engaged in the following empirical chapters. However, it focuses on circulating uncertainty, on security as only partially achievable, and the (potential) future as the temporality through which security acts. To supplement this general approach and operationalise how uncertainty can be engaged, the following section engages with literature that addresses uncertainty in more detail.

2.2 Uncertainty as an Object of Intervention

Engaging with the literature on uncertainty enables the reinforcement and advancement of how uncertainty management matters for power grid security. While Foucauldian biopolitics roughly highlights the importance of uncertainty and the future for security and securing categories, Foucault does not elaborate on the specifics of how uncertainty is addressed, secured, or how the future is engaged. Thus, the literature review on uncertainty advances, deepens, and reinforces the importance of these categories for securing the biopolitical aspects of the electrical infrastructure. In so doing, this section contributes to Critical Security Studies (CSS) by extending existing debates on anticipatory governance. While much CSS work foregrounds uncertainty as a discursive or anticipatory logic, this thesis demonstrates how uncertainties are engaged and intervened upon.

The literature on uncertainty is interdisciplinary and multifaceted. Generally, however, there is broad agreement that uncertainty is not knowing what has, is, or might happen. From these temporalities and for the following analysis of different security techniques, the temporality of the future and its relationship to various security techniques are of interest. "Future matters" (Adam & Groves 2007) for

the ways security techniques are deployed, manage the future's uncertain potential and aim to exert some control over it.

In the geographic and sociological literature on security over the past decades, techniques for securing and managing uncertainty have increasingly focused on the future and its relationship to the present. In writing on anticipatory security, Anderson (2010a: 782) notes that "uncertainty is both a threat and a promise: both that which must be secured against and that which must be enabled." The future thus holds both generative and destructive potential. As a positive potential, it underpins liberal rationalities (Foucault 2008) and is embedded in imaginaries of 'creative destruction' (Acemoglu & Robinson 2012, Kissinger 1977). Yet in the context of security, the future is often framed primarily in terms of negative potential — as a horizon of risk, crisis, or catastrophe (Bonß 2013). For Ulrich Beck (1992), writing on reflexive modernisation, second-order risks such as climate change, nuclear annihilation, or financial collapse exemplify how the future becomes saturated with the possibility of systemic failure. In outlining the "imperative of responsibility", Jonas (1984) similarly foregrounds the stakes of governing an unknowable future. "The magnitude of those stakes [of second modernity], taken together with the insufficiency of our predictive knowledge, leads to the pragmatic rule to give the prophecy of doom priority over the prophecy of bliss" (Jonas 1984: X). In the work of Beck and Jonas, uncertainty is not located in the present, but in the future: it is the potential for irreversible and unknowable harm that must be anticipated and addressed in the present. These perspectives provide a crucial foundation for understanding anticipatory governance; yet they remain primarily focused on political theory and ethics. This thesis builds on their insights by examining how such future-oriented rationales are enacted in the everyday security practices of critical infrastructure operators.

Uncertain futures are plural and multiple along a bandwidth from hopeful to catastrophic. Along this axis, they come to matter not merely as "imagined, but they are also made" (Adam & Groves 2007: xiii). Security techniques differ in their engagement with uncertainty depending on their relationship to different futures (Adam & Groves 2007). Security techniques referencing the future might either now-, fore-, or backcast and approach the future either as open to being created (present future and through forecasting) or as a tool to inform present action (future present and through backcasting) (Kitchin 2019, Adam & Groves 2007). Both forms later inform the empirical chapters on standards, standardisation, and forecasting individually. In addition to the later discussion on forecasting, nowcasting is discussed as a contrast and potential concurrent to forecasting. For Kitchin (2019: 783), nowcasting is the "annihilation of space and time to the point where governance [and security] is enacted in a 'perpetual present' (de Lange 2018b)". Similarly, and diagramming the computational city Luque-Ayala & Marvin (2020: 130) describe 'nowcasting' as operating "through the microhorizon of the future".

Scholars such as Aradau & Van Munster (2007, 2011, 2012), Adey et al. (2015) and Adam & Groves (2007) argue that security practices increasingly operate in a mode of anticipation, where governance targets not concrete threats but the possibility of disruption. These approaches treat uncertainty not merely as a lack of knowledge, but as a productive force that justifies and organises new forms of intervention. For Dillon & Reid (2009), such interventions are deeply biopolitical: they aim to protect life by acting on the unknown, and often do so through simulation, modelling, or preparedness planning. This thesis extends these arguments by showing how uncertainty is operationalised in power grid security through specific practices — standardisation, forecasting, and training — each of which engages a distinct form of uncertainty and relates to the future in particular ways. Rather than

introducing new security techniques, this thesis contributes to Critical Security Studies by showing how different forms of uncertainty are recognised, distinguished, and acted upon in combination within critical infrastructure operations.

These different ways of engaging with an uncertain future pick up, advance, and sensitise to the importance of the future as both uncertain and relating differently to forms of security; thus, the analytical category of 'related future'. Especially in its relation to identifying and describing security techniques in the following chapters, and their uncertainty relation, the future matters. The multiplicity of potential futures and their relation to security techniques indicates the need to engage power grid security as guaranteed by a similar multiplicity. Independent from its origin, the uncertain future (as a potential danger) "do[es] not depend on subject and situation" (Bonß 2013). The uncertain future only becomes acutely problematic when brought to the fore (Campbell 1998a). This 'becoming problematic' then requires a conscious act of constructing it as a threat to, for this thesis, the flow of electricity. Each security technique then recognises and constructs the threat differently from uncertainty and an uncertain future (cf.Adam & Groves 2007).

Regarding the analytical category of 'work on security', the literature on uncertainty highlights the construction of the future as a threat and its use in security rationales along two rough fronts. On the one hand, strands of literature discuss security as probabilistic. They, for example, discuss 'risk' and analyse and describe the present and future in a positivistic light and as (partly) controllable (Amoore & De Goede 2008, Bonß 2013, Ewald 1991, 1993, Lobo-Guerrero 2012, 2013). On the other hand, possibilistic security narratives discuss what might happen as remaining largely uncertain but with the possibility to be imagined, felt, enacted or exercised (Anderson 2010a, b, Collier 2008, Adey & Anderson 2012, Anderson & Adey 2011, Amoore 2013).

Since the "taming of chance" (Hacking 1990) in the 19th century, mathematicians, statisticians and social scientists were able to calculate probabilities and risk, thus providing a seemingly objective measurement for the level of (in-)security (Bernstein 1998, Porter 1986). As the "commodification of exposure to contingencies [, i.e. uncertainty]", the "biopolitization of security installed risk as one of its single most important devices", writes Dillon (2008: 320, 310). Through this seemingly objective measure of 'risk', control can be gained and exerted over individuals and a population. Lobo-Guerrero's (2012, 2013) work in the insurance industry is exemplary here. Through "an insurance logic, rendering uncertainty as risk became a way of colonising the future […]", he writes (2012: 5f.), that is, "bringing relative certainty to the world" and in borrowing from (Luhmann 2014) "creating a security of experience". Through a "trust in numbers", as Porter (2020) calls it, the regularity of scientific laws, empiricism, and positivism persuasively unfolds a belief in the controllability via predictions over what has, is or might happen.

Generally, probabilistic security techniques aim to control some aspects of everyday life and primarily operate in the everyday and on seemingly 'mundane' everyday metrics. Writing on the algorithmically driven securitisation and surveillance post 9/11, Amoore (2009), for example, highlights this when she examines the practices of border control controlling the everyday flows of travellers. Yet, innovating and containing the exposure to uncertainty/insecurity, Lobo-Guerrero (2012) discusses and explains how 'parametrical insurance' allows even for the commodification of risks that scholars like Beck (1992) deemed catastrophic, in-calculable, and thus uninsurable. For Beck (1992) these risks reflexively arose as a result of "second modernity". Industrial societies underwent a second phase of modernisation to become networked and interdependent, thus rendering the risk of climate change,

zoonotic diseases, and nuclear power/weapons potentially catastrophic. Refuting the idea of incalculability and citing the US Department of Homeland Security (2010), Luise Amoore (2014: 425) similarly highlights a shift towards "conditional" and "subjective" probabilities of risk calculus. Additionally, Jasanoff (2010: 21) identifies the upcoming computer power, big data, and 'smarter' ways of doing statistics to have reconstituted a belief in the "possibility of accurate prediction and control, even for seemingly incalculable, catastrophic risks". Systemic uncertainty about the future can be circumvented through these partial calculations or brute force statistics.

This literature on probabilistic security techniques provides one lens for understanding and analysing power grid security techniques. It generally highlights the contemporary relevance of probabilistic security techniques. However, this literature has generally not been used to describe/investigate the security of a critical infrastructure, such as the power grid. Yet, it offers to see the grid as partly controllable and controlled through different predictions, primarily for the everyday. While writing of extremes, Amoore (2014), and Lobo-Guerrero (2012) highlight that probabilistic security techniques do not need to secure in a totalising fashion but that their security provision can (intentionally) be partial and incomplete. For the later analysis of how the power grid is secured, this raises awareness of the potential limits and multiplicity of probabilistic techniques deployed to secure the power grid. Focusing solely on probabilistic security techniques would unnecessarily limit my perspective on power grid security. Thus, a second strand of literature focused on possibilistic security is needed to complement the analysis. When together, they provide a comprehensive understanding on how uncertain futures are secured (Adey & Anderson 2012, Adey et al. 2015, Amoore 2013, Anderson 2010a, Collier 2008).

Possibilistic security techniques have received increased scholarly attention in the aftermath of 9/11, the global war on terror and the preemptive US invasion of Iraq (Amoore 2013, Aradau & Van Munster 2007, 2011, Anderson 2010a). In reflecting on Dillons and Lobo-Guerreros (2008: 10) ontological claim that "life [can now be] understood as a continuous process of complex adaptive emergence", as "meta-stable" (Massumi 2009) and "turbulent" (Amin 2013), Adey et al. (2015: 7) argues that this "radical contingency of environments [their inherent uncertainty, …] necessitates new ways of governing events and lives" through possibilities. Such new ways of security uncertainty often start with a 'pre'. Amongst them are pre-emption (Anderson 2010a, Amoore 2014, Cooper 2008), precaution (Anderson 2010a, de Goede & Randalls 2009) and preparedness (Anderson 2010a, Collier 2008, Anderson & Adey 2012). Additionally, the literature on resilience similarly engages a world of circulating uncertainties and in need of constant securitisation (Chandler 2014a, b, Cutter 2016, Grove 2013, 2018, O'Grady & Shaw 2023). Yet, these forms of possibilistic, anticipatory governance are not entirely new. In examining the Cold War civil defence and nuclear preparedness from 1945 onwards, Collier & Lakoff (2015, 2021) as well as Geist (2019), for example, highlight the continuity of anticipatory, possibilistic logics for securing against the extreme threats of (nuclear) war.

What distinguishes security techniques with the prefix 'pre-' or resilience from probabilistic forms of security is that their uncertain future is incalculable and, at times, inconceivable. Probabilistic control of this kind of future is impossible, while the threat of uncertainty often lies in the extremes and the exceptional. In the literature, such extremes are catastrophe (Aradau & van Munster 2011, Ophir 2007), emergencies (Anderson 2016, Anderson & Adey 2012, Anderson et al. 2020) or crisis (Roitman 2014, Aradau & Blanke 2010). For Aradau & Van Munster (2007: 44), extremes serve as "worst-case scenarios" that inform present action through backcasting. To unfold their potential in the present,

futures to be avoided or desired are “performed” (Anderson 2010a), they are “enacted” (Adey & Anderson 2012, Anderson & Adey 2011, Anderson 2010b, Collier 2008), “simulated” or “modelled” (Collier & Lakoff 2021, Amoore 2011, 2013) and “played through” and wargamed in the present (Schechter et al. 2021, Der Derian 2009). The imagined futures are rarely singular but often multiple (Heinzen 2004). The “security calculations” of possibilistic security, writes Amoore (2014: 427), is about “the arrangement of possible combinations” of these multiple future imaginaries. Control of the uncertain future is impossible, yet what might happen can be narrowed down through the layering of ‘what ifs’.

Possibilistic security techniques contrast with probabilistic ones and, for this thesis, provide a second way of thinking and identifying how the power grid might be secured without the aim or ability to control what is or might emerge. Beyond this different lens, possibilistic security highlights how multiple ideas, visions and imaginaries about the future shape present action.

The distinction between probabilistic and possibilistic approaches to uncertainty has broader implications for the critical study of security, as it shifts attention from security as a response to predefined risks toward an understanding of security as a mode of engaging with indeterminate and structurally unknowable futures. By foregrounding the technical and epistemic labour through which such futures are rendered actionable, this thesis contributes to CSS debates on how security is constituted not only through discourse or exception, but through everyday practices of infrastructural governance (Amoore 2014, Anderson 2010b, Aradau & van Munster 2011). Although the above-engaged literature on different forms of securing indirectly provides a perspective on different forms of uncertainty (knowable, unknowable, positive-negative potential), it does not offer tools to conceptualise and understand the multiplicity of how different security techniques work on uncertainty in detail. As this thesis aims to comprehensively engage with German power grid security and not just through a specific security technique, diagramming the bandwidth of uncertainty becomes necessary.

To ensure the continued provision of critical infrastructure services, such as electrical power, is to work with and through uncertainties. Regarding the ‘work on uncertainty’, uncertainty in the related literature is systemic. Concerning infrastructural networks, uncertainty is systemic as the complexity, the richness of their components and their relationships negate the possibility of ‘full’ (human) control, as well as the reversibility of actions (Kavalski 2009). It poses the issue of unintended reflexive risk (Esposito 2011, Beck 1992, Der Derian 1992) and the possibility of “de-bounding” (Beck 1992) of cause and effects (Keohane & Nye 2000, Kellert 1993, Lorenz 1972) though not least, cascading events (Pescaroli & Alexander 2015) or escalation (Little 2004). Uncertainty, however, does not solely originate in the complexities of critical networked infrastructures but in (21st century) life itself. Dillon and Reid (2009: 85) make the ontological claim that life itself is “continuously becoming dangerous to itself, and other life forms” and “is continuous complex adaptation and emergence” (2009: 85). Uncertainty, as a systemic attribute that cannot be dissolved, highlights the need to secure against it continuously.

As systemic and multiple uncertainty relates differently to knowledge and forms of knowing. The need for intervention in one of the multiplicities of uncertainty varies depending on its perceived intensity, location, and timing. The magnitude of uncertainty tends to exponentially increase over time, while the now and ‘near’ future are/seem more certain (Luque-Ayala & Marvin 2020). To speak of certainty here recognises that in specific space-times, ignorance towards (residual) uncertainty becomes

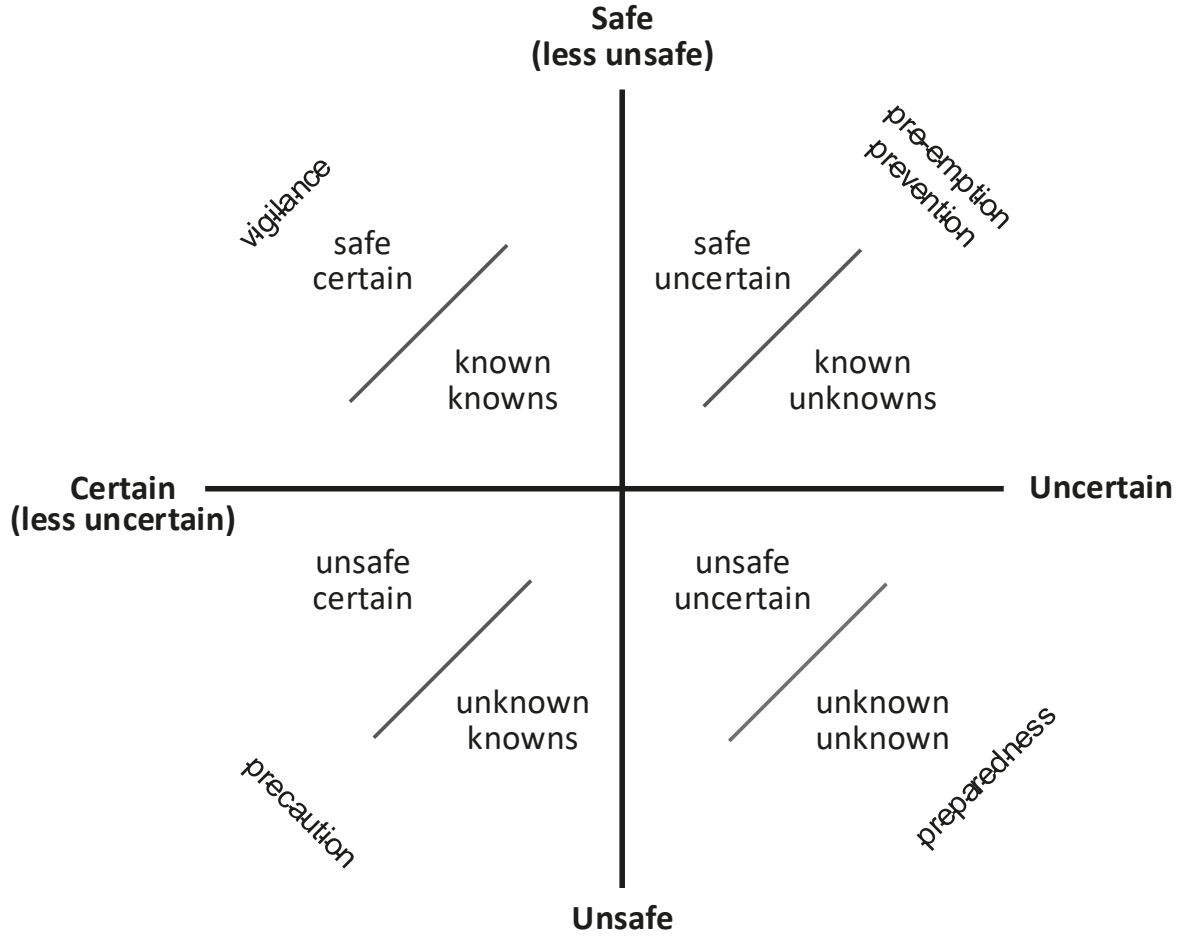
permissible. Although security techniques aim to mitigate uncertainty, they can never fully eliminate it. However, residual uncertainty in these spacetimes, after almost all catastrophic and threatening potential has been secured, loses its significance. When it does so, uncertainty might not just be "survivable" (Heinzen 2004) but potentially "safe" (Mason 2022, 2019, 1993).

Posing the question of "safe uncertainty", Mason (1993, 2019, 2022) offers not just to investigate potential security techniques through their approach to making an uncertain future known, but to do so not in absolute terms, but in relative ones. Aradau & van Munster (2011: 34) point out that "unpacking unknowns [, uncertainty, …] allows us to understand the modes of knowledge and regimes of truth" and security techniques behind them. Yet, Mason (2022, 2019, 1993) highlights the importance of not getting fixated on the absolute ability of one individual security technique to solve unknowns, but on whether the remaining uncertainty is seen as problematic and in need of further securitisation or permissible and allowed to be ignored. Furthermore, pointing out that individual security techniques only possess a relative ability to make known and secure, focuses attention on how they are layered and deployed in combination. In other words, the multiplicity of uncertainty necessitates a corresponding multiplicity of security techniques to ensure security.

Posing the question of "safe uncertainty", Mason (1993, 2019, 2022) does not approach uncertainty as a simple binary between knowing and not knowing, but develops a typology that differentiates qualitatively distinct forms of (not) knowing. His concern is not with resolving uncertainty, but with identifying the different epistemological conditions that structure how it may be recognised, named, and approached. While Mason does not directly engage with security or governance, his typology provides a valuable conceptual tool for distinguishing how different forms of uncertainty imply different constraints and possibilities for action. This aligns with Aradau and van Munster's (2011: 34) abovementioned argument and the security techniques they make possible. While this insight has informed much of the literature on anticipatory security, there remains a tendency within Critical Security Studies to treat uncertainty in general terms — often as an ontological or epistemic condition — rather than as a differentiated field of intervention. By adapting Mason's typology to the context of infrastructure security, this thesis contributes a more fine-grained analytical framework for understanding how uncertainty is managed in practice. It demonstrates how standards and standardisation, forecasting, and training each address different forms of uncertainty and operate in combination to secure the grid in everyday operations. In doing so, the thesis shifts the analytical focus away from abstract logics of anticipation toward the situated techniques through which infrastructures are made secure; not by eliminating uncertainty, but by working on it partially, differentially, and in layered ways.

Making a specific uncertainty a subject of securing requires this uncertainty to be named and demarcated (Stern 2006). Figure 2 does this by advancing a matrix originating from Mason (2022, 2019, 1993). In an idealised form, it sketches out the possible multiplicities of uncertainty as a combination of 'safe' and forms of knowing. Safe here denotes a technical term that describes the relative ability 'to rely on' what is unknown or becomes known (Bonß 2013). In relation to security, 'safe' characterises the tolerability of (un-)certainty that the correlating security techniques aim to secure. Depending on the combination of (un)safe and (un)certain specific security techniques can be attributed to them. For this thesis, Figure 2 highlights how, for the individual quadrantes, a particular uncertainty becomes a problem that correlates with security techniques. Observing the entire figure highlights that it is insufficient to secure one quadrant if the goal is to secure the entire system, in this

case, the power grid. The diversity of potential uncertainties necessitates the convergence of multiple security techniques to secure against the full spectrum of uncertainty. This typology of uncertainty will later structure the empirical analysis. It will help to identify and engage how the German transmission grid is secured by standards and standardisation, forecasting, and training that engage uncertainties differently.



© Leonard Schliesser,
advanced from Mason 2022, 2019, 1993

Figure 2 A Diagram of Uncertainty

'Safe uncertainty' is a space-time that allows for the (past, present, and) future to become known through specific security techniques, such as prevention and pre-emption. They lessen the uncertainty for specific timeframes and spaces through calculation and imagination. In following Massumi (2007: 2) prevention here is the "ability to assess threats empirically and identify their cause", thus taking action to avoid their realisation. Pre-emption, on the other hand, is a security technique that operates through imagined, enacted and performed future present (Adam & Groves 2007, Massumi 2007, Anderson 2010a). Through their effects, the "nature of [a potential] threat" (Massumi 2007: 4) becomes and can become known, thus specified and operationalised. Pre-emption is the ability to creatively make a particular future known. The affectual creation or calculation of a particular future is selective. Through imagining or calculating one future, the ability to 'know' another is lost. Thus, 'safe uncertainty' only exists within the confinement of ignorance towards other possibilities and residual uncertainty. However, some certainty can be gained within the area of these 'known

unknowns'. Prevention and pre-emption create a space of relative comfort with the residual uncertainty, as what is known and unknown can be demarcated with relative certainty. Thus, this quadrant offers 'safe uncertainty'.

'Uncertain unsafe' is a space-time of "surprise and novelty" (Aradau & van Munster 2011: 44) that cannot become known beforehand, in the now, and retrospectively. This kind of uncertain potential cannot be alleviated through anticipatory techniques such as pre-emption or prevention, as narrowing down what might happen remains impossible. Therefore, the space of uncertain and unsafe is one of preparedness. The attention shifts from the pre-event temporalities "to the time of the event" (Aradau & van Munster 2011: 45) to the ability to manage what might emerge. As a rationality of living with uncertainty, thus ultimately the potential for catastrophe, only general preparedness offers some sense of security and hope to weather uncertainty (Aradau & van Munster 2011, Lakoff 2007, Anderson 2010a). "Preparedness does not seek to prevent [or pre-empt], rather it assumes the[a] event[s] will happen" (Lakoff 2007: 253). Preparedness assumes many (worst-case) possibilities without specifying a particular threat. It does not limit what might happen through calculating or imagining a particular future. In this space, "we must learn to plan for what is possible", writes Brown et al. (2006: 531), and to do so, "worst-case analysis is critical". What might be possible is imagined and enacted but does not identify a path for pre-emption. In practice, 'what ifs' are layered and combined into 'all-hazard' approaches (All-Gefahren-Ansatz) and worst-case planning. These multiple possible futures act as a crutch to identify vulnerabilities and their subsequent mitigation (Aradau & van Munster 2011, Anderson 2010a, Collier 2008, Lakoff 2007).

'Unsafe certain' is a position where the solution to a perceived problem might seem straightforward but does not guarantee success. In relation to family therapy Mason (2019: 346) describes this state as one where "the person […] tends to lean towards feeling convinced of the certainty of their points of view". The solution to a problem might seem obvious, while seemingly only the path to it remains uncertain. Unsafe certainty is then the ignorance towards the possibility of other. What we know is either vailed from recognition, or even if awareness about a possible solution exists, it might not be trusted or trustworthy. Uncertainty about the applicability of what can be and is known remains. Unsafe certain is a space-time where ignorance towards the possibility of other requires precaution (Dunning 2011). Precaution is to "focus on the production of 'early warnings', on detecting and isolating symptoms", write Aradau & van Munster (2011: 43). Precaution operates on an emerging rather than an embryotic potential threat, while a threshold of irreversibly is not yet crossed. Still, the potential of inaction might be catastrophic (Anderson 2010a). What measures are to be taken against a perceived threat, writes Anderson (2010a: 789), then is a question of "proportionality" between "what the threat could become and the costs of (in)action in the present.

'Safe certain' is a space seemingly characterised by the absence of uncertainty. It is a space where knowledge about components and procedures is almost total and little room for error or chance remains. In such systems, like nuclear power plants, the in- and outputs are stabilised and known with relative precision, allowing for control (Schulman et al. 2004, Rerin 2006). Although what has, is, and might happen seems known at the moment, the duration of this state is unknown. Some residual uncertainties remain. The level of residual uncertainty, however, is too diffuse to warrant precautionary action. Instead, constant vigilance, or as Weick & Sutcliffe (2007, 2015) would call it, "mindfulness", is deployed to spot patterns or arrhythmias that might become precursors of potential events of emerging unwanted circulations.

The literature on uncertainty and correlated probabilistic and possibilistic security techniques engage with different forms of uncertainty, yet none provides a comprehensive overview and classification of what is uncertain. Having these uncertainties illustrated in Figure 2 helps recognise that the individual security techniques can only engage a particular uncertainty and require their combination to offer a comprehensive form of security. To ensure the continued provision of critical infrastructure services, such as electrical power, is to work with and through these different uncertainties. Only if all quadrants of uncertainty are addressed by corresponding security techniques can the power grid be secure. Thus, these individual quadrants of uncertainty will resurface and guide the inquiry into power grid security as the empirical chapters explore how the power grid is secured.

2.3 Conclusion

This chapter establishes the conceptual and analytical framework for examining the security of the contemporary German power grid. Out of the many possible approaches to security, a general Foucauldian perspective on biopolitical security was selected. Unlike more individualist or event-driven conceptions, this framework enables security to be analysed at the scale of populations and vital circulations, including electricity, which are essential for sustaining life but often remain removed from direct securitisation discourses. From this biopolitical perspective, the importance of uncertainty and the future emerges not as an ancillary consideration but as central to the problem of governing circulatory systems, such as the power grid.

Coupled with the literature on uncertainty, this biopolitical approach provides the analytical categories deployed throughout the thesis: 'work on uncertainty', 'relate to a future', and 'secure by'. Like electricity, uncertainty is a circulation; diffuse, relational, and potentially problematic if not carefully managed. Following Dillon & Lobo-Guerrero (2008), uncertainty is systemic and embedded not only in infrastructure but in life itself. However, while the Critical Security Studies literature has primarily engaged with uncertainty at the level of discourse or ontological condition, this thesis advances a more differentiated account. Building on Mason's (1993, 2019, 2022) typology, the chapter has conceptualised uncertainty as multiple and qualitatively distinct. This distinction enables a more granular analysis of how different security techniques relate to and intervene upon different forms of not knowing, of uncertainty.

In doing so, the chapter identifies two broad modes of securing the future: probabilistic and possibilistic. Probabilistic techniques seek to calculate and model uncertainty through quantification and prediction. Possibilistic techniques, by contrast, engage with futures that are not objectively knowable but imagined, contingent, and potentially catastrophic. The use of Mason's framework allows these different epistemic orientations to be mapped against specific forms of uncertainty, offering a structured lens through which to analyse how infrastructures are secured in practice.

Rather than viewing technical practices as separate from the political, this thesis adopts a technopolitical perspective, understanding infrastructure operations as deeply entangled with questions of governance, responsibility, and potential threats. The aim is not to depoliticise these techniques, but to show how the political is enacted in technical form. In doing so, the thesis contributes to ongoing efforts within Critical Security Studies to understand how security is materially performed, not only imagined, but enacted through routine practices of management, coordination, and intervention.

The electrical infrastructure is complex. It sustains life by enabling the generation, transmission, and distribution of electricity. Its operation is marked by systemic uncertainty and constant vulnerability. As the introduction has shown, the stakes are high. A single security technique cannot secure the power grid alone; instead, different security techniques must be combined to address the varied and interacting uncertainties that threaten the flow of electricity. To identify how these techniques operate in everyday grid security and how they work on uncertainty and relate to imagined futures requires a methodology capable of tracing practices that are often hidden from public view.

The next chapter outlines the research methodology used to approach this task. It details how an ethnographic and document-based inquiry made it possible to locate, observe, and analyse the practices through which power grid security is enacted in everyday life.

3. Research Design and Methodology

3.1 Introduction

In examining the security of the German power grid, this thesis combines research on electricity infrastructure and security, drawing on fieldwork conducted over nine months in 2021. It addresses the problem of researching power grid security, the transparency (cf. Star 1999) of both the electricity infrastructure and its security in the everyday. The wires might not be seen, for the pylons and the instability of the electrical supply is missed for its steadiness. Furthermore, as a sociotechnical infrastructure, the power grid is complex, and thus, so is its security. It is rich in components, actors, and their interrelationships. Understanding power grid security — enabling and ensuring the flow of electricity — requires a specific methodology that localises, makes visible, and problematizes what is otherwise hidden and taken for granted. This research design and methodology should not oversimplify but acknowledge and reflect the multiplicity and relationality of the power grids' complexities.

In my research design and methodology, I further justify and outline my choice for an ethnographic approach, as well as the perspective on everyday power grid security. I will reflect on my positionality and ethics before outlining my methods, particularly my three-month ethnography at the regional security coordinator (RSC) position, TSCNET. The Methods section will primarily focus on how I conducted my ethnographic work in the energy sector. The ethnography at TSCNET was the most important source for my empirics; thus, it will receive the most attention. In parallel with this ethnography, but in a less sustained manner, I also conducted participatory observations during a 'future innovation challenge' and a control room visit at the German transmission system operator (TSO), TransnetBW.

Rather than trying to remain a passive observer, I choose to seek proximity to transmission grid actors through engagement and involvement. The rationale was to gain deep insights and understanding of power grid security while getting close enough to observe, experience and learn from those who operate the grid and manage its uncertainties. Thus, this thesis reflects my role as an active "observant participant" (Moeran 2013). Furthermore, this ethnographic research was supplemented and supported by a review of relevant documents, audio-visual materials, and semi-structured interviews. This combination of methods allowed me to supplement and validate my empirical findings from my three-month ethnography (September – November 2021) with the 'Regional security coordinator' (RSC) TSCNET. In addition, this research design and my interest in power grid security were and are imprinted by my positionality as an active German expert civil defence volunteer.

Conducting this research during the COVID-19 pandemic and in a critical infrastructure posed significant challenges for gaining access to the transmission grid actors in two ways. During the waves of COVID-19, access to especially TSOs was severely restricted and impossible for 'outsiders'. Thus, until September 2021, some semi-structured interviews were conducted remotely, more literature, industry documents and legislation were reviewed, and online industry events were attended. Furthermore, even without a pandemic, critical infrastructures are securitised spaces. This means the transmission grid actors tightly control access to their facilities and personnel. However, conducting this research in my home country while being an expert civil defence volunteer of the German Federal Agency for Technical Relief (THW) helped to mitigate some concerns related to my nationality and intentions. Under these circumstances, engaging with actors on the transmission scale, nevertheless, required flexibility and improvisation.

3.2 Research Design and Methodology

To answer the question of how the contemporary German power grid is secured, this qualitative and interpretive research design draws on ethnographic approaches found in the study of science and technology (STS) (Bijker et al. 1993, Latour 1987, Rochlin et al. 1987). This thesis combined ethnography and participatory observations, supported by a review of documents, audio-visual materials, and semi-structured interviews (Table 1). My methodological choice enables a relational approach to analysing power grid security as constructed in the specific spacetimes of my fieldwork in Germany. Specifically of interest were the contemporary realities 'on the ground' and "what people actually do" (LeCompte & Schensul 2010: 2) to secure the flow of electricity in the everyday. This included observing and inquiring about the techniques transmission grid actors used to manage and secure against uncertainties in their everyday operations. Engaging with the actors who secure the power grid in the everyday should allow me to answer how uncertainty is managed and what techniques are deployed to secure against it.

Table 1 Methodological Overview

Method	Duration	Aim
Ethnography	3 Months	To understand how and through what techniques uncertainty is managed and secured against.
Participatory Observation	Throughout 3 Months	
Review of relevant documents and audio-visual materials	9 Months	Supporting the ethnography and participatory observation. To initially gain an overview and select the actors to engage with.
Semi-structured interviews	Initially	

The focus on the everyday rather than on exceptional events or catastrophic extremes, such as the blackout, was deliberate. Yet, while interested in everyday power grid security, asking about the extremes helped to highlight the security practices in place to manage uncertainty from becoming a threat to grid security. The answers about the potential for a blackout helped pinpoint what transmission actors considered both a threat to and a guarantor of power grid security in the everyday. It is in the seemingly mundane actions and easily overlooked details of the everyday that a potentially catastrophic future becomes, escalates, cascades, is averted, and prepared for (cf. Anderson & Gordon 2017). Due to the complexities of this infrastructure, excessive or insufficient intervention can reflexively become a security concern. In the everyday, this balance is maintained, or rather, the act of balancing is performed. As highlighted in the introduction, a stable equilibrium does not exist. In the everyday, security-supporting or eroding behaviours and patterns form and cement. Furthermore, it is in the everyday that capabilities and capacities are formed that are required to halt or reverse (potential) extreme events (Weick & Sutcliffe 2015).

For the geographical scope of this thesis, I focused on the German transmission grid and its actors (see Figure 3). This choice was guided by the role of the transmission grid as the scale at which electric flows are governed, monitored, and secured across regional, national, and international levels. Germany's transmission grid occupies a key position within the 'Synchronised Grid of Continental

Europe'—a tightly integrated high-voltage network spanning multiple national jurisdictions. As such, what appears to be a national infrastructure is embedded in a transnational system where interdependence and cross-border coordination are the norm, rather than the exception.

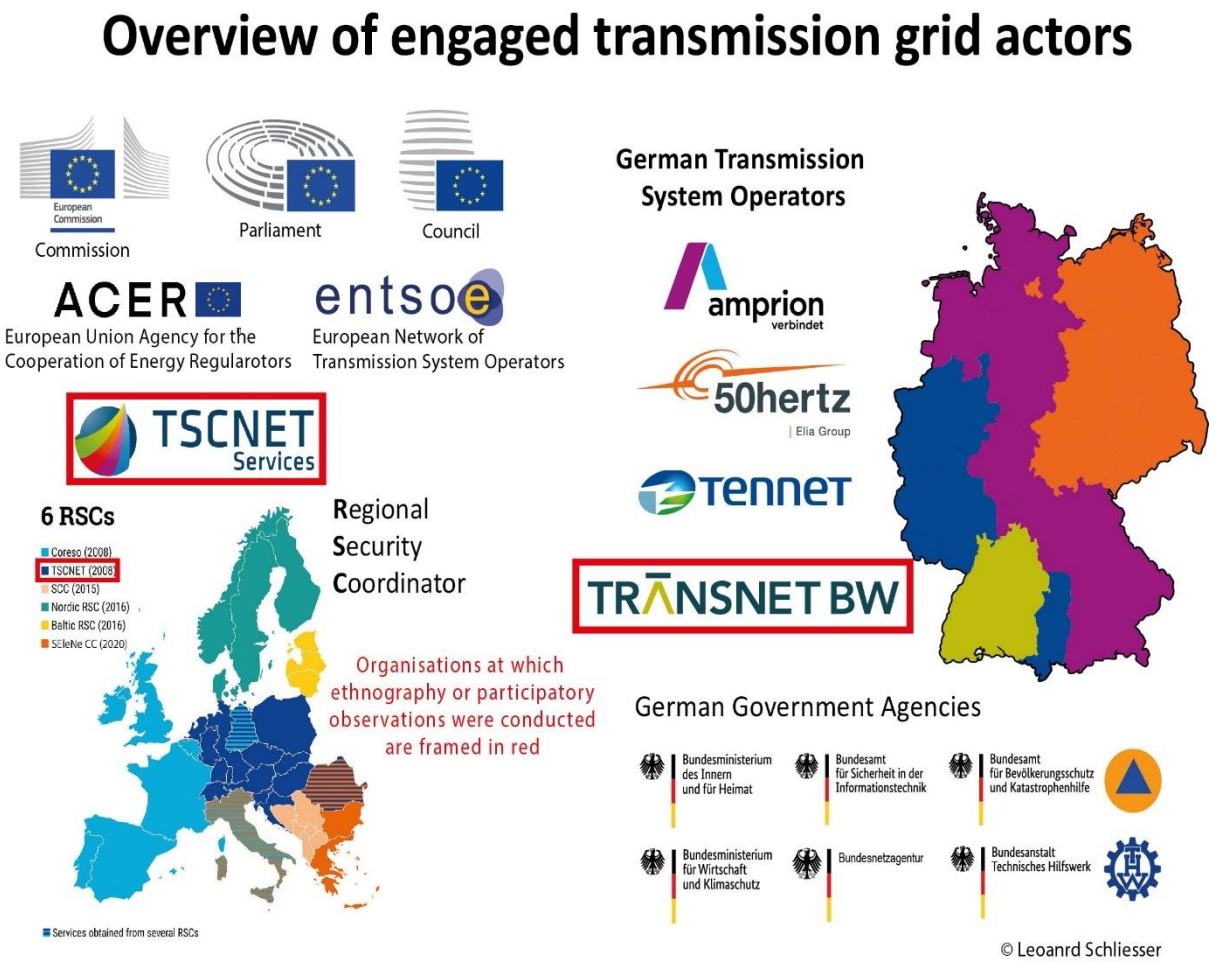


Figure 3 Overview of Engaged Transmission Grid Actors

This interconnectedness is not only physical but also institutional and procedural. The four German ransmission system operators (TSOs) are legally responsible for securing electricity flows within their respective control zones (Deutscher Bundestag 2005). However, they do so in coordination with European regulatory frameworks (European Commission 2017a) and in constant interaction with neighbouring TSOs. The role of Regional security coordinators (RSCs) such as TSCNET, based in Munich, exemplifies this. TSCNET supports 15 TSOs across Europe, coordinating operational forecasting and contingency planning to ensure stability across national boundaries. Although based in Germany, it operates over most of central Europe. Its presence reflects how national infrastructures are increasingly embedded within European regimes of infrastructure security.

Focusing on the transmission scale, rather than the distribution level, was a deliberate methodological decision. The transmission system is where the potential threat of cascading and escalating failures—such as a blackout—is most likely to materialise. These failures are not simply national events but

transboundary phenomena, shaped by the topology of interconnection and the rhythms of synchronised operation. Through this lens, grid security is not only about managing internal system dynamics but also about mitigating the potential for cross-border disruptions. It is at the transmission scale that uncertainty becomes a systemic feature, and where security must be enacted in anticipation of events whose origins may lie outside national territory.

This multiscalar character of the infrastructure also shapes the functioning of the techniques examined in this thesis. Standards and standardisation, forecasting, and training are not purely national practices. They are designed to function across spatial boundaries, enabling coordination between actors with different institutional mandates, technical cultures, and regulatory obligations. Standardisation, for example, aligns operational expectations across Europe through binding technical codes and common procedures. Forecasting involves integrating data and models across transmission zones to anticipate cross-border flows and potential overloads. Training ensures that operators across jurisdictions respond coherently to shared challenges. Each of these techniques enables electricity to circulate through a transnational infrastructure while making that circulation governable at multiple scales.

The methodological focus on Germany thus provides an empirical anchor, but the arguments developed here are not confined to a nationally bounded space. Instead, the thesis shows how security is performed across spatial scales and how the practices that secure electricity flows are themselves constituted through multiscalar coordination. The 'German' transmission grid becomes visible not as a closed national system, but as an infrastructural node within a wider European regime of interdependence, uncertainty and security. What appeared as national security practice was always already entangled with European regimes of coordination, making the fieldwork both locally grounded and continentally relevant. This spatial entanglement also reconfigures the referent of security. While biopolitical accounts often take the national population as their object, the practices observed here—particularly forecasting and standardisation—extend biopolitical rationalities across borders. The power grid, as a transnational infrastructure, becomes a site where life is secured through anticipatory labour across scales.

Through personal engagement and over time, it became possible to gain fine-grained insights into the everyday practices of securing the transmission grid, to see and understand them. This was made possible through engaging with transmission grid actors as an "observant participant" (Moeran 2013). As an observant participant, the goal is to observe while participating in the daily activities of the research subjects, thereby becoming an active part rather than a passive, observing researcher. In engaging with the TSO and TSCNET, I not only wanted to learn through the proxy of my research subjects but also through my own experience. This intimate engagement with how the power grid is secured against uncertainty in the everyday promised an enhanced quality of empirical data while offering to validate and advance my understanding and findings during my fieldwork (DeWalt & DeWalt 2011). An engaged and participatory research design enabled me to enter and become familiar with an environment mainly alien to me. By investing time to build trust, this research design enabled me to engage with actors who value their security and are cautious of 'outsiders'.

The substantial time spent with the RSC, TSCNET, and a TSO allowed me to gain a technical understanding and become accustomed to the language and terms used by my power engineering colleagues. Thus, with growing insights, conversations and engagement about power grid security

were (almost) on equal footing. This allowed me to participate and observe their everyday operations and how they manage uncertainty.

For me, the proximity gained to my engineering colleagues at TSCNET, and the TSO manifested particularly in two types of conversations: First, in those about past grid-related incidents, such as the Emsland Case or the Munich power outage of May 2021. Before conducting my ethnography and participatory observations, I reviewed the official event reports and discussed these incidents during interviews. Secondly, it showed in conversations about the limitations of security techniques and the TSO's or TSCNET's ability to continue, uphold or recover their operation. Partly due to my background (discussed in the next section) and my willingness to engage with their perspective, I did not feel like a complete outsider in both conversations and was received with frankness and openness.

The access I ultimately gained confronted me with a dilemma of what to observe. Rather than constraining myself and predefining the observational categories, the focus of my observations, through my ethnography at TSCNET and participatory observations at the TSO, TransnetBW, was left wide open. This included an openness about the processes to be observed and about when and where to observe. This allowed me to attune to the different ways, spaces, and times in which uncertainty was managed and the grid secured. I continuously journaled throughout my fieldwork to record my observations, thoughts, and feelings. These detailed descriptions of my ethnographic fieldwork preserved my experience and became the foundation for answering how the power grid is secured. A review of relevant documents, audio-visual materials and semi-structured interviews supplemented them.

Through engaging, particularly with the regional security coordinator (RSC), TSCNET and over my three-month ethnography there, I could experience, ask about, and ultimately gain an understanding of the relevance of different techniques fostering power grid security. Their details and nuances mattered. The moment of becoming critical as an infrastructure, as well as the moment of actions, technologies, and procedures contributing to or eroding grid security, depends on specific spatiotemporal contexts. Thus, uncovering and understanding power grid security requires paying attention to the relationality of when and how specific techniques secure.

Paying attention to the technical details was particularly important. On the one hand, understanding the technical details deepened my knowledge of how the grid functions and operates. While the interviews and the review of documents and audio-visual materials established a foundation, deepening this knowledge during my ongoing ethnography served as a basis for becoming more involved and appearing less as an outsider. On the other hand, acquiring technical knowledge laid the foundation for understanding the language and perspectives used by my engineering colleagues to describe the techniques they deploy to manage uncertainties and secure the flow of electricity. Understanding the technicalities of grid operation (if not entirely, though) allowed me to identify, make visible and prioritise which actors and processes contributed to grid security, when, and how. Through this learning process, for example, I discovered the role of the regional security coordinators (RSCs), like TSCNET and their focus on coordinating the TSOs actions through forecasts. In joining shifts and seeing and learning about their processes, I was able to identify and the importance of standardisation in action.

3.3 Positionality and Ethical Considerations

Reflecting on my positionality, my choice for the research design, methodology and methods is strongly imprinted by my background as an active expert volunteer of the German Federal Agency for Technical Relief (THW) and active reservist with an interest in security studies (part of my elective bachelor curriculum). Perhaps it is precisely because of this background that I am drawn to the problem of how security is done in practice and in relation to the tension between everyday security and that for exceptional events and extremes. Rather than trying to create an artificial distance between myself and the research subject, I choose to incorporate my positionality and experience in the design of this research project.

Engaging with the actors around the transmission system, my long-term membership in and collaboration with the THW made a practical difference in multiple ways. First, it gave me an appreciation and sense of the transparent and often overlooked details that support or compromise security in specific spacetimes. Secondly, my civil defence background meant that I was already familiar with some of the terms and concepts circulating in the transmission grid-related spaces. Thirdly, at times, it seemed that I was treated as an insider due to my background, or at least gaining access was easier. Occasionally, during my fieldwork, I was invited by interview or conversation partners at TSOs or TSCNET to contribute to discussions on various security and continuity topics. At TSCNET, I was also invited to support their professionalisation of emergency and crisis management processes.

Nevertheless, my affiliation with federal civil defence and being a security researcher, inquiring about ostensibly sensible topics in a corporate context, also appeared to have closed some doors. Although I cannot separate this effect from the COVID-19 fallout, I believe it at least partly contributed to a decrease in the number of initial interviews and an increase in the number of unanswered access requests I received when I first started my fieldwork. Where engagement was sustained rather than spotty and time sufficient to explain my project and intentions, polite scepticism at the beginning of encounters usually turned into benevolence.

My personality strongly influenced my choice of research design, methodology and methods. Regarding ethical considerations, my positionality required me, for example, to consider how my predisposition might influence my data selection and analysis. Initially, only publicly available documents and audio-visual materials were used to gain an understanding of the transmission grid and its actors. Later, I had, especially at TSCNET, access to internal documents. While these informed my focus and analysis, the precise content was not shared or cited due to the need to uphold confidentiality. The potential for subconscious selection and interpretation of reviewed and audio-visual materials was consciously counterbalanced by validating my focus, analysis, and interpretation of studied materials during the interviews and ethnographic engagements that were conducted.

Before the fieldwork began, the research design and methodology underwent and were approved by a university-mandated departmental ethical review process. This confirmed the focus, importance and approach taken towards informed consent and transparency. These were especially important for navigating the ethnography and participatory observations, as well as the semi-structured interviews. To be transparent and work only where consent was given laid the basis for a trustful relationship and minimised potential harm.

During my fieldwork, I was always transparent about my role as a researcher and my intentions towards the individuals and institutions I worked with. On the one hand, this was intended to foster trust and mitigate the potential for harm, as my conversations and observations informed my research. Complete anonymity could not be guaranteed and was not requested by my counterparts or their institutions. It could not generally be fully ensured, as the unique position of some individuals in an institution would make them identifiable to colleagues or industry insiders. However, anonymity was provided by referring to general positions wherever possible.

Informed consent was obtained for interviews and throughout the ethnography at TSCNET, as well as during participatory observations at TransnetBW. In practice, this meant obtaining both general institutional consents to conduct my ethnography and participatory observations, as well as the consent of the individual operational managers at TSCNET and the TSO personnel at TransnetBW whom I would encounter during my fieldwork. The institutional consent and the consent for the interviews were received in writing. For personal encounters during shifts at TSCNET or the TransNext Challenge, consent was requested and received verbally only. This was the most practical solution, as it avoided unnecessarily creating a boundary between my colleagues at these institutions and me.

Finally, a key part of my ethical considerations was a strong emphasis on collaboration, or at least reciprocity and benefit for the organisations that allowed me to conduct my ethnography (TSCNET) and participatory observations (TransnetBW). At TSCNET, this meant that I contributed to some of their ongoing projects and shared my knowledge about emergency and crisis management and organisation, as well as for a GIS project. At TransnetBW, participating in their TransNext challenge meant providing and sharing my expert opinion and labour to identify one of the potential problems the TSO would face until and beyond 2050 and to prototype a solution. Implementing some reciprocity into my fieldwork allowed me to build more trust by acknowledging and showing respect for my counterparts, thus conversing on a more equal footing.

3.4 Methods

3.4.1 Ethnography and Participatory Observation

Participating and taking part is the methodological backbone of this thesis. It was operationalised primarily by conducting a three-month-long ethnography with the RSC, TSCNET, in Munich. Shorter instances of participatory observation were conducted at the German TSO, Transnet BW, and its operational headquarters in Wendlingen. Focusing on my activities at TSCNET, this section will provide insights into my research on the ground and daily routines. It will highlight some key challenges encountered when conducting ethnographic work in the energy sector and during a global pandemic.

Table 2 Instances of Ethnographic Fieldwork

Instances of ethnographic fieldwork	Duration	Location
1. Ethnography at TSCNET	Sep – Nov. 2021	Munich
2. Participatory observation at the 'TransNEXT Future Innovation Challenge' of TransnetBW	Sep – Nov. 2021	Wendlingen
3. TransnetBW Control room observations	6 hours in Oct. 2021	Wendlingen

Ethnography at TSCNET

As a regional security coordinator (RSC), TSCNET is not directly involved in managing electric flows in the German transmission network. Rather, it is an entity that is mandated by the European 3rd energy package (European Parliament & Council of the European Union 2009d) and the "Clean Energy for all Europeans" package (European Commission 2016a) to coordinate and advise the individual TSOs by providing various forecasts and services. As an important organisation for grid security, it was not known to me before my fieldwork. However, by engaging with the mentioned legislation and its role as a 'security coordinator', I realised its relevance for power grid security and uncertainty management via forecasts. At a time when other access requests for conducting ethnographies at TSOs were unsuccessful , TSCNET invited me for three months, from September to November 2021. Despite studying the available documents and audio-visual materials available online, when I arrived, I was still uncertain about how exactly they were involved in securing the flow of electricity.

I began my time at TSCNET in Munich alongside a novice operational manager (OM), and was similarly treated as a novice OM. Based in their operational department, the plan was for me to follow along the path of the initial three-month training required for novice operational managers to gain their OM clearance. This included completing an introductory online self-training, receiving individual introductory presentations on their structure, services, tools, and shadowing experienced operators on their various shifts throughout day and night. Furthermore, the initial training involved completing a written examination involving 120 questions from an examination catalogue. While I was not required to take their final qualification examination, their 'Matura' or answer from this catalogue proved valuable as guides and tools to validate my understanding of their processes. Overall, the initial training process established an OM's understanding of TSCNETS' internal processes, services, and language, while power system knowledge was presupposed. Where my power system knowledge was limited, my senior colleagues generously elaborated and did so without hesitation or resentment.

As part of TSCNETs onboarding, I was provided with a corporate laptop that offered access to their online databases, an information security awareness briefing and an introduction to their HR procedure. Their database proved particularly insightful for me as I had access to a plethora of internal documents. Amongst these were their combined internal operational manuals and documentation for their services. I consulted them (as did the OMs) regularly to learn and understand procedures and required sequences of actions. Furthermore, they also contained event logs, thus allowing me to study and learn about past shifts and events, such as the system splits and the local Munich power outage of 2021. Reports such as these provided insights into how they dealt with incidents, which services they prioritised and how their training informed their responses. This knowledge influenced the choice of the exemplary forecasts and the perspective on training that will be presented in the following empirical chapters.

Within the first week of joining TSCNET, I had completed the self-study-only training. In parallel, I already started shadowing their OMs on shift. Besides this, as opportunities arose, I was also given full access and autonomy to participate in various further activities. These included, but were not limited to:

- Cybersecurity awareness seminars
- Online training seminars taught by TSCNET staff on their services and tools for TSO personnel
- Online seminars by the European Network of Transmission System Operators for Electricity (ENTSO-E) on future developments of tools and their methodologies
- Internal seminars on specific forecasting models, services and strategic development
- Meetings of the service quality department, going over data- analysis and quality reports
- Bilateral meetings with senior staff to discuss various aspects of their work, such as TSCNET's participation in European-level regulatory consultations or risk preparedness

Besides these activities and due to my civil defence and geography background, I was invited to contribute to small projects. For example, I contributed to a project about the geo-referenced display of power grid data in their service quality department. Furthermore, upon invitation, I consulted with senior managers about and aided in their emergency and crisis management professionalisation. Having experienced a recent local power outage and the uncertainty of the COVID-19 pandemic, TSCNET intended to improve its business continuity and crisis management. As TSCNET is not designated a critical infrastructure by German law, they performed this professionalisation voluntarily. This included studying existing standards and procedures, further updating and standardising their procedures, and raising awareness for internal emergency preparedness. Being present and involved in these occasional activities allowed me to gain a more rounded insight into TSCNET and its role in power grid security. Furthermore, it enabled me 'to give something back' while becoming a part of their day-to-day operations.

On a typical day, however, I would usually shadow the operational managers on the afternoon shift between 14:00 and 22:00. Nevertheless, I would usually aim to arrive early in the morning, between 08:30 and 09:00. I would then read up on subjects, terms, or procedures encountered and what I had journaled the day before, complete fieldnotes, or conduct the abovementioned activities. Spending these extended periods of time in the office allowed me to maximise my exposure to their culture, rhythms, and routines. Furthermore, it maximised my chances of engaging in informal talks and discussion in the corridors or over breakfast-coffee-, lunchtime-, and afternoon breaks while being able to get to know and speak to most of their staff on a regular basis.

When possible, my physical presence allowed me to engage in relatively informal conversations easily. They propelled forward my understanding of TSCNET's work and contribution to power grid security and created opportunities to engage with people from other parts of the company. In one instance, I had a longer conversation with the head of service quality about my experience at the TransNext challenge (next section). This was valuable as the conversation engaged with the difference between the TSO and RSC perspectives (Fieldnote 170921). Another such moment was with their main 'IT guy/data infrastructure architect' and his elaboration on the various standards they were obliged to adhere to and the work it takes to prepare their regulatory audits (Fieldnotes 051021).

The afternoon shift in TSCNET's three-shift system was advertised to me as the most interesting, as it contained some of TSCNET's most essential services and forecasts. It was also the most accessible as, due to COVID-19 regulations, the OMs mostly conducted the morning and night shifts remotely. While physical presence was allowed in principle, it was still limited due to COVID-19 regulations, and I had to pre-book my physical attendance in the office. On a handful of days when I could not come into the office, I still had VPN access to their internal databanks and would accompany the OMs on their shifts via video calls and screen-shares. This was also the case for the night and morning shifts, of which I accompanied a few. The forecasts encountered and observed during these shifts form the later empirical section on forecasts as security techniques. In particular, the Day Ahead Congestion Forecast (DACF) was part of most of my daily routines and the forecast to which I had the most exposure.

During these shifts, depending on the operator's character and the 'businesses' of that day, I would observe the OMs and their processes while inquiring about how, what, and why they were doing. These observations taught me how individual forecasting processes worked, as well as their metrics, elements, and measurements. I got to experience the success and failure of the forecasts, bugs and debugging and learned about and saw different patterns. As my ethnography fell into autumn, for example, bad weather and storms with high winds were a regular topic, leading to increased numbers of forecasted overloads. Seeing such patterns play out through the forecasts helped me understand when and how the individual forecasts became particularly important for power grid security.

If the shifts were relaxed to 'boring', the conversations would also meander beyond the forecast or procedure at hand. In such moments and occasionally when directly asked, the OMs, for example, shared their previous experiences from working with their national TSOs, working during transmission grid events, such as the two 'system splits' of early 2021 or the local 2021 Munich power outage that also affected TSCNET's ability to provide its services. These anecdotes of various degrees of system failure aided me in reconstructing where, what, and when security techniques had failed or prevailed. Furthermore, and particularly in the beginning, the OMs were curious about my reasons for accompanying them and my research project and understanding of power grid security. This curiosity was usually genuine, and throughout my time, I generally received their benevolence and was welcomed.

Throughout my time at TSCNET, I would record my observations and experiences in notebooks. Originally, I was concerned that the act of journaling and taking notes during my attendance of the coordination room shifts would be perceived as alien, potentially signalling me out as a researcher and others. These worries were unfounded. As I followed the path of an operational manager in training, note-taking was part of their routine. Furthermore, some OMs were even curious about my journal and the notes that I would take. On more than one occasion, this led to conversations about my notes, my perspectives and the understandings encoded in them. In one instance and while on

shift with the head of system operations, this led to a conversation and discussion between us and the other OMs present in their coordination room about the benefits and risks of their process automation.

The depths and detail of experiences, learnings, and understanding built in this three-month-long ethnography at TSCNET fundamentally shaped the outline of how I view power grid security. The focus of my empirical engagement with standards, forecasts, and training as techniques for power grid security can be directly attributed to it. Nevertheless, spottier moments of participatory observations supported my ethnographic research at TSCNET.

Participatory Observation at TransnetBWs 'TransNEXT Future Innovation Challenge'

Despite the ethnography secured at TSCNET, I continued trying to gain broader access to a German TSO as I lacked first-hand insights into them. As a result of these efforts and after successful application, I was invited to the 'TransNEXT challenge'. Parallel to my internship at TSCNET, this event was organised by the German Transmission System Operator (TSO) TransnetBW and ran from September to the end of November 2021. As a platform for knowledge exchange and innovation, it tasked the transdisciplinary participants, from industry and research, with identifying a transmission grid (security) problem that this TSO would face up until and beyond 2050 and envisioning a solution.

Six teams of three to five people competed and had to pitch their final ideas to TransnetBWs executive board members. The winner's problem and solution would be taken forward for further in-house development. Each team comprised TransnetBW employees and an interdisciplinary mix of (early) career researchers from fields such as (power) engineering, physics, urban planning, politics and geography. It had four one-day in-person events (on Fridays or Saturdays) and three week-long 'field phases' in between. During the field phases, we digitally collaborated as a group to identify our problem and prototype a solution. In my team of four, we focused on the issue of sector coupling of electricity, heat, and transport and the TSO's balancing demands.

At the in-person events, senior personnel presented on key technical, operational, and strategic subjects, while time was also available for personal conversations and exchanges. I used these moments to introduce and discuss my research project, experiences, and understandings developed through my ethnography at TSCNET. As the field phases ran parallel with my internship at TSCNET, I worked for this during free periods and on the weekends. I was either excused from work at TSCNET for the in-person events, or they took place over the weekends.

The insights gained helped me expand my understanding of transmission grid operation and its security in at least three ways. Firstly, the event allowed me to engage with a TSO directly, which I had lacked during my fieldwork. It was an opportunity to see and understand how a TSO operates in the everyday and where its specific (security) challenges lie. Participating in this event enabled me to visualise, from a TSOs perspective, the locations and moments the power grid is secured while providing further clarity on the roles and relationships of the transmission grid actors. Secondly, and specifically regarding the materiality of the grid and its technical functioning, the time spent at the TransnetBW location in Wendlingen was insightful. The event space in their old control room had multiple technical exhibits (transmission insulators, switchgear, and dioramas of substations). Taking together with the introductory presentations about the functioning of the power grid, these exhibits, tours, and explanations from senior TransnetBW technical staff provided me with unique insights about the functioning and security mechanisms of the grid. This knowledge would typically only be

received by power engineering students, exemplarily influencing the discussion of real-time security mechanisms in the forecasting chapter. Thirdly, my participation in the TransNEXT challenge allowed me to advance and validate my ideas of power grid security. The informal conversations with TransnetBW's personnel served as a tool to reflect on what I had learned and offered a fresh perspective on my experiences from TSCNET and vice-versa.

TransnetBW Control Room Observations

Born out of my participation in the TransNext challenge, I got the opportunity to conduct a control room observation. This complemented and contrasted my experiences gained at TSCNET. During a six-hour-long shift at Transnet BW's main control room, I observed, listened, and inquired about how the balancing operator I accompanied secured electricity flow. The operator had ample time to explain his side of the main control screen and what and why he had eleven further monitors circled him. He explained the relationships between grid frequency and different patterns of demand and generation (especially renewable wind and solar infeed) and how the market does (is supposed to) do most of the balancing work. In this conversation, we also talked about past grid incidents. For example, the system splits on the 8th of January, 2021 (ENTSO-E 2021c) and the 4th of November, 2006 Emsland incident, recited in the preface of this thesis. For the latter, he recounted his experience as an operator on shift. Although anecdotal, his shared experiences provided valuable insight into how TSOs deal with grid incidents. Progressing from this conversation, I gained insights on power grid standardisation, automatisation, and training requirements, as well as how they have changed over the years; likewise, the general (physical) security regime and, specifically, the infrastructural security implications of COVID-19 measures and preparation needed.

As the only visit to a TSO control room, this opportunity was particularly important to me. It offered a first-hand insight into a relatively secure place where grid operations become visual and multiple workstreams converge. This visit allowed me to observe and engage with on-the-ground grid operation from a TSOs perspective. In this place, it was possible to directly observe the governance of electrical flow “through and by technology” (Otter 2007: 580), as well as the discrete preparations for possible disruptions. It provided me with a unique opportunity to learn, see, hear about and experience an aspect of grid operation, namely balancing that I only knew about through documents and in theory. Furthermore, as with the conversations during the TransNext challenge, this was a possibility to grow and validate my understanding of the meaning of power grid security from a particular perspective.

3.4.2 Review of Relevant Documents and Audio-Visual Material

Reviewing documents supported the ethnographic and participatory methodology. This sustained effort engaged multiple documents and audio-visual formats (see Table 2). During the COVID-19 lockdowns, they were the only way to progress my research as I did not manage to recruit online interviewees then. Furthermore, at the beginning of my fieldwork, reviewing documents helped develop my foundational knowledge of the power grid, its actors, and its operations. This aided me in identifying and precisely targeting the places for my ethnographic research and provided the foundational knowledge to engage as a participatory observant.

Among the reviewed documents, where the web pages of the main actors shown in Figure 3 (Chapter 3.2), especially of the European Union Agency for the Cooperation of Energy Regulators (ACER), the European Network of Transmission System Operators for Electricity (ENTSO-E), the German Federal Network Agency (BNetzA) and those of the four German TSOs (Amprion, 50Hery, TennetDE and TransnetBW). A multiplicity of introductory and advanced material was available on these organisational websites.

Throughout my fieldwork, the study and review of documents provided further context and deepened my understanding of encountered processes and legislation. An example during my time at TSCNET is ENTSO-E's grid map (ENTSO-E 2023). During my shifts at TSCNET's coordination room, I regularly consulted it to locate the power stations and transmission lines that were forecasted to overload. I did not do this to directly answer this thesis's question of power grid security but to deepen my understanding of the forecasts deployed at TSCNET and their outputs and spatial relations. During my ethnography, internal and not publicly available documents at TSCNET, such as their operational handbook and shift-handover protocols, were the primary documents studied and part of my initial 'training'. They laid the foundation for me to understand TSCNET's specific services and procedures, while providing an opportunity to learn from (past) shifts I could not attend. The reviewed handover protocols included descriptions of past grid security incidents like the European power system splits of 2021 (ENTSO-E 2021c) and the preface's Emsland Case (UCTE 2006). These reports provided rare insights into situations beyond the everyday, including possible event cascades, and how grid operators managed the escalating uncertainty.

Throughout writing the thesis, some newer or updated documents became available and were included, such as the German TSO Amphion's (2023) description and image of substations (part the standardisation and forecasting Chapters 5 and 6). Furthermore, those documents I engaged with during my ethnography and cross-referenced in my fieldnotes remained reference points, were revisited and supported articulating and substantiating my ideas on power grid security. The *operational guidelines on electricity transmission system operation* of the European Commission (2017a) would be one example that plays an important role, especially in the empirical chapter on standardisation.

In addition to the written documents, I reviewed audio-visual materials from the transmission grid actors portrayed in Figure 3 (Chapter 3.2). Besides industry-hosted webinars, most of these materials are available on the organisation's websites or YouTube. ENTSO-E, for example, produced five short video clips introducing the services of the regional security coordinators (RSCs)(ENTSO-E 2019). This led me to discover the role of RSCs and TSCNET. Furthermore, with the pandemic progressing, attending webinars hosted by these organisations or watching their recordings on YouTube became

possible. Among these was, for example, a consultative group meeting providing in-depth discussions about the CORE FB MC forecast introduced later in the forecasting chapter (ENTSO-E 2021a).

Table 3 Quantitative Overview of Engaged Documents

Type	Approximate Quantity	Rational
EU/national Legislation	~ 27	To understand the legislative foundation of what the TSOs and TSCNET were doing. To read them as high-level forms of standardisation
Government Documents	~ 41	To gain an understanding of how various government bodies view the transmission grid and its security
Industry documents (incl. internal)	~ 67	Primarily TSOs, ENTOS-E documents that provide insights into specific processes (for example, outage planning) and an overview into what they are doing more generally.
Webinars (live and recorded)	~ 18	To broaden my perspective on the transmission grid, to get a better understanding of interrelations and interdependencies
Process Methodologies	6	To gain in-depth knowledge and understanding about specific processes, such as the forecast detailed in Chapter 6
Incident reports	5	To understand how and why the power grid can fail and what these analyses say about grid security.
Position papers	3	To understand how various organisations see the transmission grid and its security.
Plans and Maps	5	To understand the power grid's speciality and how it has been and is developing, including where its weaknesses lie/will lie.

3.4.3 Semi-Structured Interviews

Semi-structured interviews were the third method deployed to understand how the power grid is secured. A total of 5 key stakeholder interviews were conducted with personnel from transmission (TSOs) and distribution system operators (DSOs) and one energy trader (see table 3). Initially, these were intended to spearhead the engagement with transmission system actors and are well-suited for narrative yet structured engagements with senior personnel (Sayer and Morgan 1985 cited in Longhurst 2016). Senior personnel here meant 'rank' in the approached organisations, specifically the TSOs, and time worked in the power industry. The interviews were intended to provide an introductory insight into the field and to build up knowledge, contacts and relationships that could help me gain access to my ethnographic work. Despite sending out over 30 interview and contact requests during the initial months of my fieldwork (spring of 2021) to individuals and institutions related to the transmission system, only five interviews were conducted (table 3). For me, this low turnout had less to do with an inadequate approach to the potential interviewees or inappropriate questions but with the unfortunate timing of a COVID-19 wave in early/mid-2021. To partially compensate for this limitation, the scope of organisations and personnel was enlarged to include DSOs and an energy trader.

Table 4 List of Interviews Conducted

Interview	Interviewee	Duration
1	TSO, Head of System Restoration	130 minutes
2	TSO, Head of System Security	120 minutes
3	Power Supply Company, Energy Trader, Market Risk	130 minutes
4	DSO, Head of Operation	145 minutes
5	DSO, Senior Operator and Crisis Management	145 minutes

Each interview was around two hours long, conducted in German and, upon request of all interviewees, not recorded. Instead, notes (German) were taken, and an interview summary (German) was written directly afterwards to minimise the loss of information. The interviewees were a TSO 'Head of System Security', a TSO 'Head of System Restoration, an Energy Trader, a long-term operator of a 1st tire Distribution System Operator (DSO) and the head of a 2nd tire DSO network control centre. These interviews provided relevant orientation and direction for further inquiry and context.

The interviews with the head of system security and system restoration contributed directly to my understanding of how the transmission grid is secured. As I had only read about system restoration in incident reports, this interview was an opportunity to hear firsthand about the requirements, training for, and limitations of the 'black start' of the power grid. Amongst them, the 'reliability of expectation' (Erwartungssicherheit), which will play an essential role in the standardisation chapter, was highlighted in this interview, and the difference between a market- and load-following grid operations was explained. The interview with the head of system security touched upon the importance of standardisation for grid operation and restoration (Chapter 5). Furthermore, forecasts, including those of TSCNET, were part of this conversation and contributed to the later forecasting Chapter 6.

From the interviews not directly related to the transmission scale, the interview with the energy trader contributed to my understanding of the interrelationship between energy markets and grid operations (TSOs) and centred around the importance and turbulence (of that time) on energy generation, demand and price forecasts. The two interviews with different DSOs helped me understand the centrality of TSOs and their concentrated responsibility while also touching on training issues for everyday and exceptional grid operation.

3.5 Conclusion

This research design and methodology addressed two main challenges to determine how the contemporary German power grid is secured. Firstly, it had to make visible and locate the spacetimes in which the power grid is secured in the everyday. Secondly, it had to navigate the multiplicity of actors and their interrelationships. The transmission system was chosen as the scale at which power grid security could be best observed. The transmission system operators (TSOs) are legally responsible for upholding the flow of electricity at this scale. Furthermore, due to the transmission grid's importance and interconnectedness, the potential for escalating or cascading events leading to a blackout is also primarily located here.

An ethnographic research design was deployed to make visible, locate and narrow down how the grid is secured. This was primarily achieved through a three-month ethnography at the regional security coordinator TSCNET, a core actor in the transmission grid and its security. In addition, spottier participatory observations at a German TSO provided an additional perspective. A review of relevant documents, audio-visual materials, and semi-structured interviews supported their findings.

Through this multifaceted engagement, everyday power grid security became visible and observable, understandable, and experienced through the transmission grid's systemic lens. Specifically, through sustained ethnographic engagement and as an “observant participant” (Moeran 2013) I was able to see and experience how the flow of electricity is secured in the everyday. Extensive field notes were taken during my ethnography and participatory observations, and they form the basis for the upcoming empirical chapters.

Standards and standardisation emerged as a security technique (Chapter 4) not distinctively through a particular ethnographic engagement or method but as a cumulative combination of them. At the beginning of my fieldwork, I reviewed legislation, standards, industry norms and process methodologies. During my initial training at TSCNET, I learned about the processes and the standardised sequence of actions from their internal handbook and connected them to European legislation. Reflecting on my experience, fieldnotes, and interview summaries, I realised that standards and standardisation had always been transparently in the background, securing the grid.

The organisational ethnography conducted over three months at the RSC, TSCNET, resulted in the centrality of forecasts and forecasting emerging as a specific power grid security technique (Chapter 5). Providing forecasts to the TSOs is the core and everyday service TSCNET provides. The forecasts presented in Chapter six are some of those directly observed when joining the forecasting shifts and shadowing TSCNET operational managers (OMs). Furthermore, in both interviews with the TSO head of system security and during my control room visit, forecasts were identified as essential for power grid security.

Training, as the final empirical chapter (Chapter 6), like standards and standardisation, emerged as a security technique, not through a single encounter, but through its sustained presence during my fieldwork, particularly in my ethnography and participatory observations. Nevertheless, the initial training I underwent at TSCNET had a disproportionate impact on how training emerged as a security technique. It allowed me to see and experience its value throughout my following ethnography.

In conclusion, the research design and methodological choice enabled the identification, analysis, and positioning of standards and standardisation, as well as forecasting and training, to be identified as three everyday security techniques for the contemporary German power grid. Primarily through the

three-month-long ethnography at TSCNET, it became possible to allocate sufficient time to locate and make visible where security occurred while ordering and understanding the multiplicity of transmission grid actors and their interrelationships. By remaining flexible and undertaking fieldwork for an extended period, I was also able to weather the fallout from the COVID-19 pandemic, which further increased the challenges of conducting security research in secure environments and critical infrastructures.

4. Standards and Standardisation as a Security Technique

4.1 Introduction

In this chapter, I position standards and standardisation as crucial security techniques in the power grid. While there has been ample discussion on other techniques for securing life and (critical) infrastructures, such as surveillance and policing (Salter & Zureik 2005, Gekker & Hind 2019), insurance (Lobo-Guerrero 2012, 2013), or resilience (O'Grady & Shaw 2023, Wakefield 2020, Welsh 2014, Grove 2018) standards and standardisation were rarely part of this debate. Yet, standards and standardisation processes kept surfacing during my fieldwork. When they emerged in conversations with the TSOs and TSCNET, their importance for various aspects of power grid security was usually highlighted. Thus, this chapter engages standards and standardisation as a security technique that secures the power grid and the lives connected and dependent on it. The chapter argues that standards and standardisation 'secure by' pre-emption in the everyday and prepare for the exceptional. Both forms of securing 'relate to a future' that has not yet emerged and 'work on uncertainty' by containing what might and is emerging as a possibilistic form of security.

In advancing this argument, the chapter contributes to a growing strand of Critical Security Studies that conceptualises security as an anticipatory practice rather than as an exceptional or sovereign intervention (Amoore 2014, Anderson 2010b, Aradau & van Munster 2011). This literature foregrounds how uncertain futures are governed through calculative techniques, epistemic devices, and organisational routines. While techniques such as surveillance and forecasting have received considerable attention, particularly in relation to risk, algorithmic governance, and pre-emption (Amoore 2009, Anderson 2010a, Gekker & Hind 2019, Salter & Zureik 2005), the role of standards and standardisation remains comparatively underexplored. Yet, as this chapter demonstrates, standards and standardisation are not merely administrative artefacts or technical tools. They program futures, thus containing uncertainty, and enabling security by making (infrastructural) behaviours predictable. This becomes evident in the Emsland Case, where the failure to coordinate and a dissimilar situational understanding led to a blackout in Western Europe. It exemplifies how the failure of a mundane security technique—standards and standardisation—can materialise insecurity at a continental scale and contribute to infrastructure failure.

In bringing attention to this underexamined domain, the chapter adopts a technopolitical perspective that treats standards and standardisation as artefacts in which governance, expertise, and political rationalities coalesce (Folkers 2017b, a, Lampland & Star 2009, Star 1999). Standards and standardisation are not neutral; they structure what is knowable, actionable, and governable within the transmission grid. They stabilise expectations, delimit tolerable failure, and coordinate responses across highly complex systems. As such, they participate in the biopolitical organisation of life through infrastructure (Bowker et al. 2019, Collier & Lakoff 2015). This chapter thus contributes to the thesis's broader argument that security is not only imagined or discursively constructed, but materially enacted through technical acts and classifications, routinised conduct, and embedded protocols. These practices render possible the partial governance of uncertainty in the everyday. By demonstrating how standards facilitate pre-emption and preparedness through the encoding of imagined futures, the chapter extends CSS debates on anticipation and biopolitical governance to infrastructures by highlighting how security is enacted through layered, historically situated, and often invisible techniques.

Standards and standardisation are pre-positioned to secure the everyday primarily, yet are also doing so for exceptional situations when intended as such. By specifying and thoroughly describing their subjects, they create a reliability of expectation, shape expectations and contain uncertainty. Because they are developed and come into effect before something happens – they are pre-positioned - they can contain uncertainty. They contain uncertainty to the point where it is safe, but only for as long as what is emerging stays within the parameters of the standard. Standards and standardisation for this thesis are loosely defined as outcomes and processes of 'making similar' and include both technical and procedural standards, norms, legislations, rules, codes and procedures. Standards and standardisation are the underlying infrastructure that enables and allows for the secure operation of the grid (Hughes 1983). Standards for this thesis describe the 'end products' of standardisation processes. Their act of making similar secures by enabling effective coordination between the multiplicity of transmission system actors. As coordination tools, standards are the language used by power engineers, operators (TSOs) and operational managers (TSCNET) I engaged with to describe, get to know, build, and order transmission grid operation coherently and interchangeably.

Relating to standards and standardisation pre-emption, for this thesis, is 'disconnected' from the political debates around the post 9/11 security dynamics and the global 'War on Terror' (de Goede et al. 2014, Anderson 2010a, de Goede & Randalls 2009, Massumi 2007). The literature discussing pre-emption describes the technique as offering security in an environment of uncertainty but with a "potential future threat" (Massumi 2007: 4). For this thesis pre-emption becomes a technical tool that describes how standards and standardisation secure. Pre-emption, writes Anderson (2010a: 790), "acts over threats that have not yet emerged" but over those that can be imagined, enacted or performed (de Goede et al. 2014, Anderson & Adey 2011). Standards are perceived as static, yet harness a similar creativity of experts (Easterling 2016, Lampland & Star 2009), that Anderson (2010a) identifies as a generative characteristic of pre-emption. Citing Martin (2007) Anderson (2010a: 790) states that pre-emption has the "generative power to make and reshape life", and I suggest that standards and standardisation share this power. They are sediments of specific ideas and visions about (un-) desirable futures (Lampland & Star 2009, Brunsson & Jacobsson 2002b). Through backcasting, these sedimented visions of a potential future coordinate and shape present action to forestall potential harm from materialising (Adam & Groves 2007, Holmberg & Robert 2000).

Standards and standardisation secure in the everyday through pre-emption but aim to prepare for exceptional situations. Preparedness "assumes that events will happen" (Lakoff 2007: 253) and "intends to intervene in a (catastrophic) future" (Lakoff 2007: 248). Through standards and standardisation, preparedness aims to provide capacities and capabilities to either halt the worsening of a situation or enable (swift) recovery from it. While the future engaged through preparedness cannot be known, it can, through the same generative creativity as pre-emption, be imagined, enacted, or performed (Aradau & van Munster 2011, Anderson & Adey 2011, Collier 2008).

By standardising both technical and procedural aspects of grid operation, uncertainty about what is and might happen is contained, and a window for possible future control is opened. As specific visions about a future take precedence, they exclude other possibilities and contain them beyond what has been imagined. As long as what is emerging stays within the parameters, within the guaranteed range of the standard or what is standardised, standards and standardisation can make known what is or might emerge in this range. For the bandwidth and subject, they address, standards and standardisation contain uncertainty.

Depending on what I later call their scope and reach, technical and procedural standards and standardisation provide their own framework through which what is or might emerge becomes known or described. What can be known becomes limited through standards and standardisation itself. I distinguish between technical and procedural as their scope and reach vary. Technical standards, specifications, and norms about the materiality of infrastructure and the grid appear more backgrounded and are more deterministic regarding the described subjects. Procedural standards instead focus on processes, standard operating procedures, and regulated activities. As such, they can be more flexible and less deterministic.

Standards and standardisations were present in multiple ways during my ethnography at TSCNET and participatory observations at the TSO, TransnetBW. While I will draw on these to illustrate my arguments in the following section, for this introduction, the 'Emsland Case' described in the preface serves as one example. As an event of un-coordination (cf. UCTE 2006), it highlights what is at stake when standards and standardisation fail to secure a potential future and coordinate, threatening the flow of electricity. On November 6th, 2006, a power line needed to be taken offline and what should have been a routine operation nearly ended in catastrophe. A lack of standardisation and adherence to existing standards led to a different understanding of powerline ratings, thus obscuring what was happening. Furthermore, unsynchronised action between two TSOs caused the continental European synchronous area to split (UCTE 2006). Fifteen million households were left in the dark for up to two hours. Although this incident did not receive sustained media attention, it was a "watershed moment" (Fieldnotes 090921) for the power industry. It influenced the 3rd European energy package being drafted at this time. It expedited a renewed focus of the industry and its legislators on fostering coordination through standardisation (European Parliament & Council of the European Union 2009c, a). It highlighted the crucial role of standards and standardisation in pre-empting such incidents and their contribution to power grid security.

This chapter starts by engaging with the available literature on standards and standardisation as both a security technique and one of coordination. This literature-driven section illustrates the difference between technical and procedural standardisation through the help of empirical examples. While always working through containing uncertainty and pre-empting potentially dangerous futures, standards and standardisation are multiple, of varying scope and reach. The second section then turns to standardisation in and for the everyday, illustrating how it secures and coordinates the grid on both the European and national scales. A network of European bodies and legislation is the foundation of the synchronous grid of continental Europe. At the national scale, balancing demand and generation through the activation of reserve power will illustrate the vital importance of standards and standardisation for the everyday security of electrical flow. The third section engages with how standards and standardisation for and in the exceptional aim to preempt or prepare for escalation and cascading events. This will be illustrated by drawing on examples from both my observations at the TransnetBWs control room and ethnography at TSCNET. In conclusion, I summarise how standards and standardisation are a security technique of the power grid that 'work on uncertainty' by containing what is and might happen. As a form of possibilistic security, they 'relate to a future' that has not yet emerged but can be imagined and is 'secured by' pre-emption and preparedness.

4.2 Standardisation as a Security Technique and Coordination Device

Standardisations and standards secure both in the everyday and in exceptional situations pre-emptively and prepare through backcasting. As they contain uncertainty about what is and might happen, they secure the power grid. Present action is informed and coordinated by an imagined and idealised future. Through standards and standardisation, the technical and material properties and the procedural conduct are coordinated and secured against the future potential of un-coordination, disorder, or misunderstandings. Unsecured these could lead to an escalation or cascading events that threaten the security of electric supply. While standards and standardisation do not appear prominently in the existing literature on securing life or critical infrastructure, this section addresses some literature on them. Speculating, one could say that the lack in recognition as a security technique is because of their severe backgrounding, as they are taken for granted or perceived as mundane and boring (cf. Lampland & Star 2009, Star 1999).

Since the early days of electrification, standards and standardisation have played a defining role in the creation and evolution of the power grid (Mohla 2017, Hughes 1983, Taylor 1941). They enable the grid to function while simultaneously providing logic for its governance and describing how things are to be done. In following Star (1999) the grid can be understood as the embodiment of standards that co-constitute it as electrical infrastructure. Today, the European synchronous Area spans 24 countries, from Portugal to recently added Ukraine, supplying over 400 million customers with reliable electricity around the clock (ENTSO-E 2022b). Synchronisation to and upholding or restoring the network's beat of 50 Herz, would be impossible without the work of standards.

In making similar material components as well as operational processes, specifying and demarcating their 'territory' and relationship to one another, standardisation functions "protocological" (Galloway & Thacker 2004, Galloway 2004). For Galloway & Thacker (2004: 8) protocols encompass the "rules and standards that govern relationships in networks" and, as such, aim to exert "totalising control" for the subject they try to describe. Protocols are systems "for maintaining organisation and control in networks" (Galloway & Thacker 2004: 9). While Galloway & Thacker (2004) understand protocols primarily in the context of computer and biological networks, I relate their idea to the electrical infrastructure as well. Standards and standardisation are both outcomes and processes that secure the networked power infrastructure in an environment of uncertainty and emergence. They combat uncertainty by focusing and trying to exert control over a specific subject and through well-defined parameters. Depending on the varying degree of totality with which they describe and standardise, they shape and control the reliability of expectation.

The reliability of expectation created by standards and standardisation functions in a duality. In the face of uncertainty, it provides information about what is or might happen and possible responses. Firstly, the information encoded within the standard does not need to be acquired anew each time and provides a framework to understand what might or is emerging (Brunsson & Jacobsson 2002a). This reliability of expectation is, in part, implicitly developed through "habituation" (Edwards 2019). It is learnt as part of "membership" in the electric infrastructure (Star 1999). Secondly, standardisation offers to standardise the conduct with and in the face of uncertainty. It partially alleviates the burden of ad-hoc decision-making in the face of uncertainty and under time constraints, thus offering control over an uncertain situation. Already established forms of knowing and response can be applied (Edwards 2019, Brunsson & Jacobsson 2002b). Intended behaviours are encoded in standards, and unwanted specified to be excluded. The created reliability of expectation then secures potential

emergence and response as it significantly reduces the time needed to translate, explain, evaluate, and decide on an issue at hand. Through standards and standardisation, the response time can be compressed to the point where it almost disappears, and automatised control becomes possible.

Standards and standardisation secure stockpile-like as they "hoard time" and "store power" (Folkers 2019a: 1). They require an up-front investment to pre-positions a common "knowledge infrastructure" (Edwards et al. 2012) and rely on future imaginaries, through which the reliability of expectation is formed. In so doing, and if implemented correctly, the time required to act uniformly, to coordinate, and to become aware of what is happening has already been invested through a standardisation process. Action can be taken in response to an emerging event without undue delay.

Standards and standardisation pre-empt a future need to make ad-hoc decisions. Through standards and standardisation, an imagined future is shared, and what is to be achieved or avoided is "backcasted" (Kitchin 2019: 782, Adam & Groves 2007, Holmberg & Robert 2000). What is emerging becomes known through these selective futures, creating and shaping expectations and actions in the present. However, standards and standardisation work only for as long as what is emerging stays within the specified scope of what is standardised, within the range of what has been imagined. The scope of a standard is its specificity (what it describes), while its reach describes the area and extent of its usage. As compromises (Brunsson & Jacobsson 2002b), standards provide a negotiated (minimal) level of security (cf. Folkers 2017b). Warranty-like standards and standardisation lose most of their power to secure and coordinate when applied outside of what they were developed for.

Standards are limited in their scope. Their scope primarily depends on their creator's intent and motivation. Encoded in their scope is not just a specific vision of a future, but connected to it a specific understanding of and level of security that is deemed desirable/undesirable or "safe enough" (Wellock 2021). The level of security that is imagined as safe enough depends on the subjective assignment of criticality to infrastructure for its ability to sustain lives or its potential risk for and consequences of catastrophic failure. The higher the 'risk' write LaPorte & Consolini (1991) as well as Schulman et al. (2004), the more regulated and standardised critical infrastructures and their installations become and should become. For nuclear power stations (cf. Rerin 2006), or the main transmission control room, the level of standardisation and the desired level of security are higher than for transmission towers deemed 'less critical' (European Commission 2017a, European Parliament & Council of the European Union 2016). Standards and standardisation processes, like infrastructure, are "always valuation regimes that constitute orders of worth" (Bowker et al. 2019: 4). Standards carry with them their creators' imaginaries, worldviews, and perspectives. They are relational and bound to the place and time of their creation.

In citing Millerand & Bowker (2007), Lampland & Star (2009: 7) state that "standards are always relative to the infrastructure within/upon/sometimes against which they are implemented". For the German context, this means that the experience of this infrastructure and its standards is bound to the history of Western electrification (Hughes 1983). While "standardisation in electrical engineering is almost as old as the science itself" (Taylor 1941: 747), standards today reflect the historical and political changes through the past century. Being entwined with and becoming an infrastructure themselves, standards and standardisation are never neutral but always "politics pursued by other means" (Latour 1988: 22). While subtle and inapparent, some values are encoded into the standards, while others are excluded. Particular solutions are negotiated, decided by experts and enforced, ignoring other pathways while reflecting little on their underlying values (Pargman & Palme 2009:

186). This thesis focuses on the technicalities of power grid security, yet recognising the political dimension is important. It is important, not least, as the level of security inscribed in and described by standards and through standardisation has changed over time. As touched upon in the overall introduction (Chapter 1), the state, as the former owner of most public works, such as the power grid, transitioned from being directly responsible for "existential provisions" to a "guarantor of last resort" (Folkers 2017b, 2018). In this context, standards and standardisation today are implemented to ensure a very specific, sometimes minimal level of security (cf. Folkers 2017b, a).

Despite differences in the motivation to standardise (legal necessity, industry initiative etc.), standardisation becomes primarily through the subject judgement of experts (Easterling 2016, Lampland & Star 2009, Brunsson & Jacobsson 2002b). "Standardization is closely linked to expertise", writes Jacobsson (2002: 40) and "motivated by the view that there are some persons who know best", the expert. In closed-door events and usually, only upon invitation, groups of experts decide technocratically for others, based on what they perceive as 'right', 'the best solution' or a compromise (Brunsson & Jacobsson 2002b). As a modern phenomenon (Giddens 1990) potentially in decline (Reed & Reed 2023) the expert and expert knowledge are given authority to decide for others. For Easterling (2016), these experts today reside outside the state and national regulators and are organised in powerful conglomerates such as the International Standardisation Organisation (ISO). Such standardisation bodies centralise power while distributing control through the dissemination of their standards (Galloway & Thacker 2004, Galloway 2004).

Standards and standardisation assume the ability to completely describe material properties and behaviours for areas where the motivation to control and where the demand for security is high (cf. Rerin 2006). Nevertheless, any too much or too little standardisation can also reflexively become a problem (Hanseth et al. 2006). If the subject being standardised is described in excruciating, excluding detail or not described thoroughly enough to become 'useful', standards and standardisation loses its power to secure (Brunsson & Jacobsson 2002a). In both cases, too much or too little standardisation can lead to a diffusion of responsibility (West 2000, Bierhoff & Rohmann 2017), as well as to disorder (Hanseth 2001, Hanseth et al. 2006). For West (2000), the diffusion of responsibility is a "problem of many hands" or a "bystander problem". The individual's urge to act and to decide is severely dampened when in the proximity of others and flanked by stringent technical and procedural standards. The responsibility to act can comfortably be shifted to an 'anonymous' other or the standard. If labour is divided by standards and standardisation, so is responsibility. This can hinder the containment of emergent situations as 'I am not responsible for this, and someone else will deal with it'. In referral to others, the standards or standardised order duties and individual responsibility can comfortably be refused.

Yet, any standards are "always already incomplete and inadequate" (Lampland & Star 2009: 14). Like infrastructures, they are negotiated and require time to be established and changed, thus can easily be overtaken by new events (cf. Abram 2014, Star 1999). Infrastructure-like standards, whether techno-material or procedural, are legacy systems, layered or nested onto each other (Lampland & Star 2009, Galloway & Thacker 2004, Star 1999). They stack over time, relate to each other and are only being further specified, reworked, or abandoned modularly (Star 1999). While standards are often presented as static to argue against their benefits (Brunsson & Jacobsson 2002a), Millerand & Bowker (2007: 165) contest this "narrative" and point out that "standards are in constant flux". Furthermore, the power of standards to make known, thus securing a particular future, depends on

them being accepted, useful and used. Standards, whether technical or procedural, are a language that, unless spoken, becomes irrelevant (Millerand & Bowker 2007: 158).

To further illustrate where and how standards and standardisation function as security techniques in the electricity grid, the next two subsections will discuss technical and procedural standards separately. This separation accounts for the different relationships of technical and procedural standards to the electrical infrastructure and their ways of containing uncertainty, making known, and thus securing futures. While technical standards are far more backgrounded, develop slower, and are more totalising, procedural standards are more habitual, especially on the company scale. Furthermore, this separation allows the sharing of empirical material that underlines how standards secure by making known, containing uncertainty, and coordinating actions.

4.2.1 Technical Standardisation

As a sub-category of general standardisation, technical specifications, norms, and standards aim to secure by providing a standardised vision, thus ensuring certainty about the technical properties of, in this case, the power infrastructure. In providing a standardised vision, they pre-empt not knowing where the limits and operational ranges of technical components and systems lie. Their reach can be global, while their scope is generally relatively limited and focused on individual technical specifications of characteristics and features. Taking the transmission tower as one example, standards govern its foundation, steel, or structural engineering and describe the transmission tower together.

Infrastructure-like (cf. Star 1999) the users of technical standards and standardisation have only limited influence on their creation or usage; if any (Pargman & Palme 2009). As an individual, you may choose to use a screw (flat, or Philips's head, Torx etc.) or a certain system of power plugs and sockets, but the user barely gets to influence their characteristics and design. It is the technical experts in (inter)national standardisation committees, such as the Organisation for Standardisation (ISO), the 'Deutsches Institut für Normung' (DIN), or the EU Agency for the Cooperation of Energy Regulators (ACER) that set disband or modify them. The opinions and views of these experts decide the level of security encoded in them. Borrowing from Palme (2006) and Lessig (2006) and their engagement with computer code (technical) standards due to their persistence can function law-like and provide systems of enforcement. They are barely ever disbanded altogether, but tend to be replaced by newer ones incrementally (Star 1999). Throughout its use, the standardised head of screws, for example, changed many times (from flat head to Robertson, to Philip's, to Hex, to Torx etc.) and was improved to allow for higher torque and tighter fastening (cf. Rybczynski 2000).

Through standardisation of components and systems, 'complete' technical knowability is striven for, maximising predictability and rendering surprises, i.e. uncertainty quasi-non-existent. If the object standardised remains within the standard's bandwidth, its properties are known as described by the standard. Nevertheless, it is not just the standardisation of specific properties but also their maximally tolerated deviation or point of failure that contains uncertainty within a defined range. The specification of the maximally tolerated deviation and point of failure accounts for imperfections of the product due to its manufacturing or material properties and defines what is 'good enough'. Trust in the individual part is built. Three examples will illustrate this further:

Transmission towers and iconic buildings of the 20th century, such as the Eifel-Tower or the Golden Gate Bridge, were held together by rivets. The point of failure of rivets remained relatively uncertain and relied on a multiplicity of factors. The possibility of rivet joint failure mandated frequent inspections and thorough maintenance. Therefore, and with improved metallurgy, manufacturing and standardisation in the 1960s and 70s, bolts and nuts started to replace rivets as their properties, including their sheer strength, could be determined with higher precision (DeBruler 2018, Wilbur 1905). This example of standardisation is useful not just to highlight how uncertainty is contained and constructions secured against structural failure but also how strongly technical standards are backgrounded, becoming transparent (Star 1999). When engineers or mechanics, today, request an 'M12' screw, they are likely to get it as their colleague instantly knows what is required, including matching tools, ensuring fit and guaranteed holding strength. The engineer or mechanic building or maintaining a transmission line does not (need to) consider the standards that make these possible. Existing in the background, the technical standards are not regularly contested. They are only contested and become problematic when their scope is deemed insufficient for the occurring event or when they are used outside their ecosystem. Although similar, metric and imperial screws differ slightly. A metric M12 screw will cause a headache for a US-American engineer or mechanic who only possesses imperial wrenches or vice versa. The coordinational benefit of standardisation is partly lost.

An anecdotal example of what can happen in the power grid when the scope of a standard is breached was provided by the head of system security of a TSO in one of my interviews (Interview 2). In 2005, an extreme winter storm in North-Western Germany caused snow and ice to form and grow on transmission lines. The subsequent weight of this ice build-up exceeded the regional-specific structural-design requirements 40-fold (Klinger et al. 2011). Additionally, unforeseen, unstandardised degradation and embrittlement of some diagonals had occurred and had not been addressed. Subsequently, 82 transmission towers collapsed, leaving 250.000 people in the region of 'Münsterland' in the dark for up to a week (Schröder & Klaue 2015). As only this region was blacked out, help and relief were mobilised from the rest of Germany and could alleviate the situation within days.

This example of the 'Münsterland' power outages highlights the limited scope of standards as their guarantee to contain uncertainty becomes void when exceeded. A standard from 1956 governed the strength of the 65-year-old transmission towers, made from 'Thomas-steel', that collapsed under the excessive snow load. While other standardised steels with higher strength were used for security reasons since the 1960s and 1970s, the legacy standard remained the foundation for much of the legacy infrastructure. This 'Thomas-steel', governed by the outdated standard, did not withstand and account for the ice-load-induced torsion forces appearing on that day (Bundesanstalt für Materialforung und -prüfung 2006).

An everyday example of technical standardisation are the electrical plugs and sockets that are the termination of the grid. With progressing electrification in the first part of the 20th century and the increase of especially electrical household appliances, the question of how to securely connect them to the grid became increasingly important (Oud 2009, Hughes 1983). "The absence of adequately protected appliances and poorly designed plugs and sockets were a constant source of danger" (Hahn 2017: 1). Then, in 1929, the German engineer Wilhelm Klement of the Siemens-Schuckertwerke AG applied for and received the patent for what today is called the 'Schuko-Stecker' (Schutzkontaktstecker, earth contact socket). Almost unchanged, it has prevailed until today and is

commonly referred to as Type F plug/socket and is used in large parts of Europe and in over 70 countries worldwide. The standardisation of these plugs and sockets has drastically reduced the number of injuries and deaths by electrocution or electrical fires (Hahn 2017). As the Schuko-Stecker is rated for 250 Volts of alternating current (AC) at 16 Ampers, it contains uncertainty as it eliminates the need to question whether it is secure enough to be used up to this threshold. Even if it can accommodate a larger power flow, theoretically, the guarantee of secure usage expires beyond it. Above the Schukos rating, part failure becomes likely. In everyday usage and operated within their design specification, these plugs and their standards are omnipresent yet barely ever noticed. They come to mind only if they break or if, while on holiday, you suddenly realise that your destination has different outlets. This incompatibility does not erode the trust in the plug/socket itself but only in its convenience of usage. Adapters, connectors, or auxiliary power sources then allow for the continued, if more inconvenient, usage of the appliances connected through the Schuko plug.

Technical standards secure by making know the material properties of the objects they are written for. Specifying and guaranteeing in detail their properties for a specific bandwidth and their point of/type of failure they build trust in the individual components and in accumulation in the overall system. By making similar, they contain uncertainty as they allow for the predictability of the component's properties. In functioning like an infrastructure and offering an eco-system, they allow for the coordination of praxis without the need to second guess, increasing working efficiency. Technical standardisation increases trust in the individual parts and frees up resources that would otherwise be required to understand an emerging problem, coordinate, and engineer a common solution.

4.2.2 Procedural Standardisation

Whereas technical standards control material characteristics, features, and their deviation, procedural standards are concerned with operational processes, ordering the relationships and conduct of and between the non-human and human grid components. Depending on their context, the terminology differs, yet they follow a similar logic of securing by maximising the predictability of processes. Best practices, standard operating procedures, handbooks, manuals, guidelines, and routines resemble procedural standards or following Galloway & Thacker (2004) are ‘protocols’. They regulate the flow of information as “the key component in the organisational logic of protocological control” (Galloway & Thacker 2004: 20). In the words of Adam & Groves (2007: 8) “habits, customs and traditions as well as laws, rules and moral codes provide a degree of foreknowledge and anticipation. They make the behaviour of others predictable and facilitate a certain measure of security.”

Through standardised processes, the transmission systems operators and the operational managers from the regional security coordinator gain an awareness of what is going on and what should go on. By describing processes and specifying who/what should exchange what kind of information, when, and with whom, operations become standardised, allowing for the reliability of expectations to form. In standardising what needs to be done in a clear and defined language, uncertainty is contained beyond the standardised subject.

On the EU level, the ‘System Operation Guidelines’ (SO GL) for the transmission system govern and secure much of the conduct between the actors of the transmission system (European Commission 2017a). Through standardisation, they both distribute operational responsibilities and define key

terminology. The SO GL is “a detailed rulebook governing how transmission system operators and other relevant stakeholders should act and cooperate to ensure system security” (European Parliament & Council of the European Union 2019b: 2). It distributes the operational responsibilities and writes into code the relationships between different European transmission grid actors. It mandates TSOs to, for example, establish a system defence and restoration plan or to only suspend the market as a last resort while requiring the TSOs to coordinate with the Regional Security Coordinators (RSCs) (European Commission 2017a). In standardising the conduct of the transmission grid actors, uncertainty in these standardised processes is contained, and interactions become predictable, making the grid more secure.

Furthermore, procedural standards and standardisations contain uncertainty by defining key terms. A “normal state” of the power grid is, for example, described in the SO GL as a “situation in which the system is within operational security limits in the N-situation and after the occurrence of any contingency from the contingency list, taking into account the effect of the available remedial actions” (European Commission 2017a: 5). All other terms within the definition of ‘normal state’ (operational security, N-situation, contingency, remedial actions) are also specified, leaving little room for misunderstandings. The operational security limits mentioned in this definition are technical standards that, for example, specify clear limits for the normal operation of a specific power line. Technical standards interact with and supplement procedural standards. Building a web of mutual supporting definitions reduces the possibilities of potentially dangerous misunderstandings. Should this mutual supporting web fail or individual standards, whether procedural or technical, ignored or breached situations like the 2006 Emsland Case mentioned in the preface are possible (UCTE 2006). For the standards to be able to secure a specific future, they need to be accepted and used in the everyday.

Procedural standards operate on various scales (multinational/EU, national, company), so their level of detail and ability to contain uncertainty to secure vary. This is intentional, as the procedural standards governing the conduct on the transmission grid are more political than their technical counterparts. High-level procedural regulations, like the SO GL above, build on the consensus established through the EU legislative process (European Commission 2015). As the next section on everyday standardisation will highlight this process takes time. Furthermore, due to the process of their origin and perspective, they are less stringent. As high-level protocols, they are legally binding but leave room for their subordinated scales (national and organisational) to operationalise them. Procedural standardisation on the multinational/EU scale is negotiated and comes into force as top-down regulation. The operationalisations on the lover scale, however, are more akin to “social analogues of individual habits and skills” (Edwards 2019: 359). Procedural standardisation in the transmission system is also created from the bottom up. Two brief examples illustrate this.

At TSCNET, the rulebook that described their services and individual forecasts is the first example and was an ‘in-house’ creation. As a living document, the rulebook is updated by the operational managers (OMs) and used to train, learn, or during operations regularly. It operationalises higher-level regulations by filling in the uncertainties left by them and applying the vision of these higher-level documents to the local processes as it thoroughly describes them. Through this, it contains potential uncertainty. It pre-empts the potential future need to determine what to do, when and how. It does so through thorough descriptions of processes and examples of what might or has gone wrong, offering possible contingencies. Furthermore, it specifies further points of contact should additional

help be required. When creating and updating this rulebook, its creators backcast from the ideal set out by the higher-level regulations and their own ideas of what 'ideally' should be explained in it.

A second and similarly habitual way of how conduct is standardised at the local level of the operator is illustrated by the practice of protocoling or logbook writing. Keeping a log of what happened is a legal and insurance responsibility for TSOs and RSCs. Ideally, and based on my time at TSCNET, they serve three further functions. First, they are a tool used to log and track actions taken, not to forget a step in an ongoing process. Secondly, they also serve the handover process at the end of a shift and convey to the new shift what has happened. Thirdly, logs retrospectively allow for the analysis of incidents and processes. A 'standard' logbook usually contains features like event number, date and time, event description, and a comment section. However, how it is filled out depends on the local culture and even the individual operator or OM, yet the ideal function of the logbook just mentioned guides them. At TSCNET, novice OMs would occasionally ask for advice on what to include and exclude from the handover, while experienced OMs would develop their own 'styles'. Upon occasional self-critical review of the logbook entries by the operations team and against what they ideally should accomplish, the OMs would adjust their practice if needed. Making similar recordings of what happened, the encounter with the past that informs their future and present actions is standardised and becomes more reliable. By recording their actions in a particular and similar way, the operators and OMs forestall the potential future need to figure out what happened, where something went wrong, or even who was on duty.

These collaboratively established operationalisations by the electricity industry then further synchronise their conduct in more detail to the point where they can offer decision-tree-like clarity on what is going on and what to do. SOPs, best practices, routines, and the code used to exchange information generate a framework that frequently is more stringent than the original legislation (Lessig 2006, Palme 2006). It is often historically grown processes that persist (cf. Star 1999) and are imprinting coordination processes. Bottom-up procedural standards are created in the privacy of the workplace, the control room, or office kitchens and through a multiplicity of industry exchanges where a shared vision and understanding of a future ideal of processes, structures, and duties is formed. As situated futures, these forms of procedural standardisation secure in the same way as their top-down or technical counterparts. Uncertainty is contained by creating a reliability of expectation, and the potential for escalation or cascading of events is pre-empted. The initial intention to secure, control and routinise the conduct in the transmission grid of the procedural standards created from the bottom-up might, over time, however, become "black--boxed" and might not be recognisable as such anymore (Edwards 2019: 359).

4.3 Standardisation in and for the Everyday

The previous section explored standardisation as a coordination device that secures pre-emptively through backcasting. Through standards, what is or might emerge becomes known through pre-positioned categories of expectations and possible responses are coordinated through them. Uncertainty is contained within the margin, the bandwidth, the scope of the standards that are to secure in the everyday. By elaborating on the European-level standardisation process for the electricity sector and the German national coordination for reserve power activation, this section illustrates how standards secure the everyday flow of electricity. Standards in these examples secure by building reliability of expectation that contains uncertainties by either shaping how uncertainty

becomes known or even providing the categories through which what might emerge becomes framed. In both examples, security becomes relatively abstract, mundane and in part far removed from the direct governance of electricity flows while taking time to be negotiated and for the security potential of the standard to unfold.

4.3.1 European Standardisation and Coordination

Today, most legislation relevant to the German transmission grid originates from European energy legislation. Standards on operating and securing the grid in the everyday and exceptional take shape and become through European processes and institutions. Besides the European legislature, the 'EU Agency for the Cooperation of Energy Regulators' (ACER) and the 'European Network of Transmission system operators' (ENTSO-E) play an outstanding role. While the EU does provide some technical requirements, for example, for the connection of power stations to the grid (European Commission 2016b) their legislation primarily standardises procedures. Through their legislation, the conduct between TSOs and RSCs is moved onto a similar footing and is coordinated through standards. The internal processes of TSOs and RSCs are provided with sets of requirements that standardise the encounter with the power grid and its operation. These requirements then contain a vision of how the conduct within and between the transmission grid actors should be performed. Depending on the rigour of these standards, they provide an epistemology through which the encounter with the grid is shaped. In both ways, European standardisation is making certain. It builds reliability of expectation that secures the conduct on the transmission grid and helps to coordinate the different European transmission system actors.

The 'European Union Energy Packages' (Third in 2009, Fourth in 2019, Fifth in 2024), as bundles of legislation, mostly initiated the development process of new standards for the energy and electricity sector. Through them, the idea of a future yet to come is formulated and becomes the legal basis for action in the present and the pre-emption of unwanted futures. The idea of a future represented in the 4th energy package was originally outlined in the European Commission (2016a) Communication (860) titled "Clean Energy for All Europeans". It put forward "energy efficiency", "global leadership in renewable energy", and "providing a fair deal for customers"(European Commission 2016a: 3) as core ideals that present and future action should achieve over time. In 2019, after a legislative process, the European Parliament & Council of the European Union (2019c, 2019d, 2019b, 2019a) adopted (with amendments) these ideas and operationalised them for the electricity sector. Operationalising the European Commission's strategic vision backcasted and further contained uncertainty about what future should be achieved and secured.

Besides the political EU bodies, like the parliament, council, or commission, two EU entities stand out in developing new and enforcing existing standards in the securitisation of grid operation. First, the 'EU Agency for the Cooperation of Energy Regulators' (ACER), founded in 2009 as mandated by Regulation EC No 713/2009 of the third energy package and the European Parliament & Council of the European Union (2009b). Its primary task, as envisioned by the legislature, is to "ensure coordination" between National Regulatory Authorities (NRAs), "recommend, assist and advise" them and "monitor regional cooperation" (European Parliament & Council of the European Union 2009b: 2). In anticipation of an increased "need for coordination" due to more volatile power flows and growing numbers of actors in the grid, ACER's role and powers were solidified and advanced following the fourth energy package in 2019 (European Parliament & Council of the European Union 2019c). ACER

addresses a threat to grid security that stems from un-coordination, which can be a potential source for escalation or cascading towards a blackout (i.e., the Emsland Case). ACER coordinates the transmission grid actors by legislating the standardisation of conduct in the transmission grid. By making the conduct between the grid actors reliable and reliably similar, it secures against potential un-coordination and misunderstandings.

Based on a requirement in the System Operational Guidelines (SO GL), introduced in the previous section, for "regional outage coordination" (European Commission 2017a: 56) ACER, after a consultation process with the TSO, RSCs and ENTSO-E, for example, delivered a "Methodology for assessing the relevance of assets for outage coordination" (ACER 2019). This methodology becomes relevant for the example of the 'Outage Planning Coordination (OPC)' forecast in the next chapter. For this chapter it is relevant as a document that provides a standardised epistemology on how certain grid elements (transformers, generators etc.) become known as a 'relevant asset'. Standardising what elements become relevant when and where ACER contains uncertainty about what should be viewed as a 'relevant asset'. It secures against a potential future where it would be unclear what asset should be included or excluded in the different processes, such as the outage planning coordination.

The second organisation that helps to ensure the security of grid operation through standardisation is the European Network of Transmission System Operators (ENTSO-E). It does so, like ACER, not directly by being involved in grid operation but by creating, maintaining, and upgrading the standards necessary to operate the grid securely, effectively, and efficiently. Succeeding the Union for the Co-ordination of Transmission of Electricity (UCTE), ENTSO-E was, like ACER, established through the EUs third energy package (European Parliament & Council of the European Union 2009d). As a network of European transmission system operators, ENTSO-E coordinates industrial expertise and opinions and builds consensus regarding new or updated standards or legislation. In this regard, ENTSO-E almost functions like a multinational standardisation body that can draw from the expertise of the individual European TSOs when it, together with ACER, operationalises the European regulations and directives. During my time at TSCNET select senior personnel would regularly participate in ENTOS-E working groups or directly contribute to proposals for the methodologies for different processes. After the adaptation of the fourth energy package, ENTSO-E is now responsible for electricity regulation and preparedness, for the former Regional security coordinators (RSCs), now Regional Coordination Centres (RCCs), for the pan-European resource adequacy (electricity generation) assessment and new network codes (European Commission 2019). In collaboratively developing new network codes with the TSOs and ACER, ENTSO-E is negotiating futures to avoid or achieve, which become the basis for further backcasting and operationalisation at subordinate scales.

In developing and standardising methodologies for calculations and models, ENTSO-E provides epistemologies, a standardised language/lens through which various futures become known. Uncertainty about how to measure/assess potential futures becomes known, and vice-versa, the future to be avoided or achieved becomes known through the selected standardised measurement. The need to guess, to be uncertain, is pre-empted. For the mid-term resource adequacy assessment, as an example, this would be the definition of its key indicators (ENTSO-E 2021d). The mid-term adequacy assessment is supposed to evaluate for up to 10 years ahead if there will be enough electricity generation capacity to meet the demand. Its key indicators are the 'loss of load expectation' (LOLE) measured in "hours during which resources are insufficient to meet demand" and the 'expected energy not served' (EENS) measured in gigawatt hours (GWh) (ENTSO-E 2021e: 7). As a measure for

the duration and intensity of power outages, or even blackouts, these indicators provide a tool for assessing what potential future imagined and modelled is more desirable. In doing so, ENTSO-E does not simply pre-empt through standardising but provides the foundation for pre-emptive, preventive, and preparatory action as it lays the foundation for defining a desirable, undesirable future.

The development of not just standards but their epistemological basis and the securitisation of everyday grid operation through standardisation takes time (cf. Abram 2014). The SO GL again are exemplary. Initiated by the EU's third energy package, ACER, in 2011, started the negotiation process via a public consultation for a draft 'Framework Guidelines on Electricity System Operation' (ACER n.d.) with ENTSO-E and its national TSOs. While the initial consultation phase was only three months, it was only after years of workshops with stakeholders, formal, written exchange of opinions, expressions of views and recommendations that the draft versions of the network codes were submitted by ENTSO-E in 2013 and after revisions in 2015 (ACER n.d.). In their final form, the 'standard operations guideline' (SO GL) became part of legislation and were adopted by the European Commission (2017c, 2017a) eight years after being mandated. Today, these regulations are the backbone of power system operation and security and are updated periodically. They regulate and coordinate the conduct of TSOs and RSCs while demarcating their responsibility.

The standards developed and negotiated between ACER and ENTSO-E today pre-empt through controlling how an uncertain future becomes known by providing epistemologies and methodologies for operational processes, such as the abovementioned mid-term adequacy assessment. Providing the methodology for processes, such as reserve power activation, standards and standardisation also control how an uncertain future can become known. During my ethnography at TSCNET, the basis of all their forecasting, on which the next chapter is based on, was built upon a legacy data exchange format (DEF). It now serves as an additional example of how standards secure in the everyday and on a European scale. Uncertain about what might happen is contained by providing a standardised data format that establishes how the grid can become known. The Union for the Coordination of Transmission of Electricity's data exchange format (UCTE-DEF) provides the language for the grid forecasts, which are discussed in the following chapter. In standardising what can and cannot be a potentially dangerous future, the potential for miscommunication or misunderstandings is pre-empted within the scope of what is standardised.

The TSOs and RSCs require a standardised language, a DEF, for operational information/data exchange and to be able to conduct combined calculations, models, and forecasts. Without a standardised language, they would be unable to communicate and understand each other. The Union for the Coordination of Transmission of Electricity's data exchange format (UCTE-DEF) was developed by ENTSO-E's predecessor and sought to standardise and ensure that data exchange between TSOs was possible (UCTE n.d.). It does so by simplifying and describing the grid elements through seven blocks or categories (nodes, lines, exchange of powers, Two windings' transformers (T), Two windings transformers regulation (RR), Two windings transformers special description (TT) and Exchange powers (E)). The values of these categories rely on the US ASCII standard and its range of characters. Information is exchanged via an unformatted .txt file (PowSyBL 2022). While reductionist, the UCTE-DEF has been the backbone of all operational data exchanges between the transmission actors. Though deterministically defining the range of values possible in these categories, the UCTE-DEF provides the language through which the grid can become known in this form of operational data exchange. A node in the grid is, for example, specified only to be able to possess ten different voltage

levels (UCTE 2006: 4, n.d.). Within this bandwidth, uncertainty about the possibility of values is contained, and reliability of what values are possible and can be expected exists.

Standardisation for the transmission grid and on the European scale is managed cooperatively through ACER, the regulator's coordination body, ENTSO-E, the network for transmission system operators, and the different European legislative bodies and processes. European-level standards and standardisation processes primarily secure through formalising procedures that contain uncertainty, make known, and create a reliability of expectation. They do so by providing regulations, directives, methodologies, or standards that order and make similar, depending on the depth with which they standardise and describe. By providing a common language and reference framework, uncertainty is contained beyond what is defined and potentially dangerous futures of uncoordination, misunderstandings, and disorder pre-empted.

4.3.2 Standardised Reserve Power Activation

The previous section provided examples and explanations of how European-level standardisation for the everyday helped secure the flow of electricity by standardising the conduct on the European transmission grid actors. This section now focuses on how standardisation becomes important for one aspect of the security of everyday electricity flow nationally in Germany: reserve power activation. As the balance between electricity demand and generation is never perfect, reserve power is activated to balance and bring the frequency (as an indicator of this balance) back to within its optimum around 50 Herz. For their respective control zones, TSOs are ultimately responsible for this balancing (Deutscher Bundestag 2005, European Commission 2017b). While this process relies on technical standards, it is primarily procedural (European Commission 2017b).

Visiting the main transmission control room, the 'Hauptschaltleitung' (HSL), at the TSO, TransnetBW, I observed reserve power activation as a mundane and almost invisible process of everyday securitisation. It is almost invisible during normal operations, as the activation of reserve power is highly standardised, partially automated and a process primarily operated through markets and their platforms. The TSOs are only allowed to intervene if the market (partially) fails to balance the grid (European Commission 2017b). As one of at least four engineers in the control room, only the system balancing controller I joined for his shift in the control room monitors the actual and forecasted (im-) balances and reserve power activation. Pointing to one of the 11 PC monitors in front of us, he explained what looked like a stock market 'bid and ask' kind of screen where the market acquisitions of reserves flickered by.

This moment and this one PC monitor are the tip of the iceberg of a process that is vital for the security of electric supply and is highly standardised. In detailing and explaining how standardisation secures the life dependent on this balancing, it will be discussed as an area of European top-down legislation and bottom-up German innovation that became mainstream EU practice.

The balance of demand and generation in the power grid is never perfect. Thus, various frequency containment and restoration reserves are needed to keep the frequency close to the optimum of 50 Herz. Should this balancing act fail and frequency deviation from 50 Herz exceed a threshold of +/- 0.2 Herz, brownouts and low/high-frequency disconnects will follow (ENTSO-E 2022a). If the imbalanced frequency escalates or cascades further to +1,5/-2,5 Herz, all remaining generators would disconnect from the grid automatically (the work of technical standardisation) to not become damaged or

destroyed, a total blackout (Deutsches Institut für Normung 2011). Before these exceptional situations emerge, however, standardisation helps to pre-empt the possibility of being unable to balance the grid. Through standardisation, various frequency reserves are enabled. 'Frequency Containment Reserves' (Primary Reserves, FRCs) are the first line of defence against frequency deviations. Their job is to contain and halt any further frequency deviation. They are decentralised and distributed, automatically responding reserves over which the TSO only have limited control. The 'Frequency Restoration Reserves' (Secondary Reserves, aFRR) are the second line of defence and aim to automatically restore and bring back the frequency to within its optimum. Tertiary Reserves (Minutenreserven) are called manual Frequency Restoration Reserves (mFRR), and they compensate for larger imbalances and require manual activation by the TSO. During normal operation, the TSOs automatically or manually activate these reserves. The TSOs purchase the reserve capacity in specific reserve power markets.

The activation of reserve power is severely standardised to pre-empt the threat of contracted reserves not being available to perform their task (automatically) and within seconds to minutes (European Commission 2017c, b, a). Potential reserve power providers must be pre-qualified according to European Commission Regulation 2016/631 and follow technical standards (European Commission 2016b). The potential need to question the contracted reserves' ability to fulfil their standardised and specified requirements obligation is alleviated. From the requirements outlined in this regulation, the potential provider can backcast what actions to take to prepare for reserve market participation.

European Commission Regulations (EU)2017/2195 provides most of the regulatory framework for balancing and describing the methodology of balancing and reserve power activation (2017b). The system operations guidelines described in European Commission regulation 2017/1485 (2017a) further, quantify the amount of FCR that must be available at any time to be dispatchable over continental Europe as 3000 megawatts (MW) in both directions. Too much and too little generation, too much or too little demand are both potential problems. Through this specification, the security of electricity supply is defined as the ability to absorb the simultaneous loss of two generators (usually up to 1,5 gigawatt (GW) per power station bloc) or demand of up to 3GW. The probability of such an event is calculated to be below once in 20 years (European Commission 2017a: 91). Beyond this range, the grid's potential to collapse into a blackout increases significantly.

Despite their task to stabilise a fluctuating frequency, the activation of reserves can reflexively become problematic if too much or too little is activated or their simultaneous activation is opposed. Such a situation could reinforce frequency oscillations while spiralling to the exhaustion of available balancing reserves, potentially leading to a blackout. Furthermore, due to their limited availability and unique characteristics, activating these reserves is costly. Thus, (neo-) liberal ideals of efficiency cemented in European legislation warrant TSOs to deploy them cautiously and only if necessary (Consentec 2022, European Commission 2017b).

While in most European countries, only one TSO is legally responsible for ensuring the flow of electricity, there are four German TSOs (Amprion, Tennet DE, 50Herz and TransnetBW). As a historical Germany-specific anomaly, this elevated the need for close coordination regarding reserve power activation. In accordance with the German Energiewirtschaftsgesetz (EnWG, energy law) (Deutscher Bundestag 2005), each TSO is responsible for ensuring the load-frequency control (LFC), the balancing of demand and generation in his respective areas. Because the TSOs are individually responsible for balancing their control area but are physically interconnected to their neighbours, exceeding, or

opposed activation of balancing energy can occur and be a potential problem. To avoid this and to reduce the cost of balancing, the German TSOs are cooperating in a joint 'Netzregelverbund' (grid control area). Having formally started their coordination in 2008, their standardisation of methodologies and supporting infrastructure, such as data exchanges, evolved over four modules and has since been adopted on a European scale (Übertragungsnetzbetreiber 2022, ENTSO-E 2024c, b).

In these four modules, each of the German TSOs addresses a specific uncertainty and future that is to be pre-empted. They first created standardised methodologies and a (data) infrastructure that allowed them to pre-empt the threats from opposed activation by 'netting' their joint reserve activation first (Übertragungsnetzbetreiber 2022). In the second module, they similarly worked to jointly dimension their required reserves by establishing a fictitious unified control area. This aimed at pre-empting the possibility of individual over- or under-dimensioning of reserves and subsequently higher individual costs or the potential for insufficient frequency response reserves. The German TSOs developed a joint procurement market in the third module to profit from increased reserve power market competition. The fourth and last module aims to cost-optimise the usage of reserves (Übertragungsnetzbetreiber 2022). A joint-procurement and cost-optimised activation of reserves is important for the TSOs as high costs for reserve procurement and activation, in the extreme, threaten their financial solvency. From 2011 until 2018, the netting of imbalances alone saved the German TSOs around 150 million Euros (International Grid Controle Cooperation 2019).

As the success of this coordination within Germany materialised, other European TSOs started to adopt this German model. To implement this model EU-wide, the International Grid Control Cooperation (IGCC) was formed in 2011, and the imbalance netting (who needs how many reserves to be activated) was realised through a standardised platform (International Grid Controle Cooperation 2019). With the start of the 'Platform for the International Coordination of Automated Frequency Restoration and Stable System Operation' (PICASSO), almost all European TSOs now participate in the joint acquisition of balancing power on a mainland European scale (ENTSO-E 2022b).

The standardisation of various aspects of the process of acquiring and activating reserve power increased reliability, availability, and cost-optimised use of reserves to balance demand and generation (ENTSO-E 2024c, b, International Grid Controle Cooperation 2019). While the mandate to coordinate the balancing originated from European codes, the German TSOs operationalised these through their own development, which is now being implemented European-wide. The securitisation of the flow of electricity through reserve power activation happens in and for the everyday. It relies on technical and procedural standards positioned to pre-empt the possibility of insufficient and reserve power activation from becoming a reflexive security concern. Through standardisation, the uncertainty about sufficient reserves and their availability is contained. The bandwidth of what is considered a normal incidence, a sudden loss of +/-3000 megawatts, is demarcated by the SO GL on a European scale (European Commission 2017a). Beyond this threshold, the guarantee of ensured service provision becomes void. While a 'rare' event, it is possible, and specific standards designed for exceptional events exist to secure against its possibility.

4.4 Standardisation in and for the Exceptional

The previous section showed how standards and standardisation are essential to safeguard everyday grid operation. Especially for reserve power activation, one of the most important processes in the

grid, standardisation is crucial to guarantee the possibility of automation and timely response. While in the everyday, the flow of electricity is already constantly at risk of breaking down and blacking out, this risk increases in exceptional situations as uncertainty about what might or has happened propagates. Staying with the example of reserve power, an exceptional situation would be if the 3000MW of frequency containment reserves would be maxed out or exceeded, and the frequency would deviate from its optimum at 50 Herz for more than +/- 0.2 Herz. Yet, even in these situations, standards and standardisation secure.

Most standards operate to govern the infrastructures of the everyday and contain uncertainty by pre-empting an imagined potential situation from escalating or cascading. Within their designed scope, everyday standards secure a range of 'normal incidents'. Facing exceptional events, however, that exceed this bandwidth, their security guarantee becomes void. Standards that are particularly designed for and based on imagined extremes supplement them. Layered with everyday standards, they secure the grid against a wider range of potential uncertainties or threats. As the operational bandwidth of eventuality of standards for the exceptional lie above that of everyday standards, they start and continue to work in situations that exceed the everyday standards' coping capacities. Furthermore, some standards are designed as hybrids operating in a wider range of both everyday and exceptional contingencies.

Standards that are to secure against a potential that might exceed the everyday secure with the same creativity of pre-emption as in the everyday. Imagined future extremes that are to be avoided inform present actions through backcasting (Adam & Groves 2007). Technical and procedural standards are pre-positioned before an event takes shape. Yet, whereas standards and standardisation in the everyday only pre-empt to intervene on a future that has not yet materialised and with the intention to foreclose it, this does not always work for the exceptional. Additionally, in the exceptional standards and standardisation, through preparedness, also promise to contain escalation or cascading events, to manage them or, in the worst case, ideally, to recover from them. While the focus of preparedness is the emerging or ongoing event, actions of preparedness take shape before an event emerges and through imagined futures as well. While both rely on the same creativity to secure pre-emption and preparedness are two different qualities. First, standards aim to pre-empt and halt the emergence of a potential threat. Uncertainty about what might happen and the potential threat itself can still be somewhat contained. Secondly, through preparedness, standards focus on enabling continuity and on the management of emerging extremes, including the recovery from them. Uncertainty and the emerging event are now uncontained. For the latter, rigidity is not the goal but fostering flexibility and adaptability that enables continuity. While conceptually separated, pre-emption and preparedness for the exceptional coexist, intersect, supplement, and occasionally oppose each other in practice.

For the exceptional, two distinct 'protection schemes' are mandated by the European system operation guidelines (European Commission 2017a) and operated by the TSOs to pre-empt the possibility of not being able to respond to exceptional situations. Visiting TransnetBW during both the control room observations and my participation in the TransNext challenge I learned about them. These protection schemes dissect 'exceptional' into two categories of 'in-' and 'out-off' range contingencies. They standardise the encounter with the exceptional and their response to them. The so-called 'special protection scheme' functions by pre-empting "a limited number of critical contingencies" that, if they would materialise, had the potential to threaten "operational limits" (ENTSO-E 2012: 6). Operational limits are technical specifications of maxima/minima of, for example,

thermal limits, voltage limits, short-circuit current limits, frequency and dynamic stability limits. Aided by computer modelling, potential futures are imagined and help to identify and contain uncertainty about what combination of events would cause violations of operational limits. While these violations have not yet materialised, standardised measures are pre-positioning to pre-empt the possibility of potential escalation or cascading system failure.

The second protection scheme focuses on the system as a whole. It is put in place by TSOs to focus on 'out-off' range contingencies that cannot be narrowed down and will surprise. As the last line of defence before the blackout, the 'system defence plan' positions "mostly automatic measures to ensure fast reaction to large disturbances and to avoid their propagation through the system" (ENTSO-E 2012: 7). To ensure timely actions through automation, these mechanisms are highly and rely on standardisation. 'Low-frequency demand disconnects' are an example. These measures were responsible for the blackout in the preface's Emsland Case example (UCTE 2006). As the system frequency collapsed, they automatically disconnected customers, i.e. load, to stabilise the frequency and preserve some parts of the system. Standardisation for the system defence plan secures via preparing for a potential future and through containing uncertainty about, in this case, the TSOs ability to contain, halt and manage an escalating or cascading system. Beyond the system defence plan, European regulations 2017/2196 standardise preparedness procedures for the black-start, the re-energisation of a blacked-out grid (European Commission 2017c).

Technical and procedural standards for exceptional work together to pre-empt and contain an event from escalating or cascading. In the everyday, they remain in the background but are on standby, waiting to be activated. Like the above examples of protection schemes and system defence plans as procedural standards, an example from my field visit to TransnetBW illustrates the standards placed to protect their physical infrastructure (IEEE 2021, VDE 2006, Bundesministerium des Inneren 2005). The site of TransnetBW I visited during my control room visit and the TransNext Challenge is the most critical grid node as it harbours the control room as the underlying structure that enables and ensures the centralised governance of electricity flows. The physical security of TransnetBWs control room started well beyond its entrance, through layered defences protecting the 'castle's keep'. For its significance, the premise and main building were largely hidden from outside view by walls, fences, and green spaces. The fence surrounding their premise wasn't just of standard chain wire but of metal meshed matts seemingly much stronger. Thick concrete walls bordered the access ramp's solid and high steel gates. The operator I joined later explained that much of the physical security considerations for their new building originated from post-9/11 security standards. The access ramp, bollards, earth walls and ditches on the premise were built to stop potential vehicle-born improvised explosive devices (VbIED) or suicide bombers in vehicles while reducing the blast effect on the building itself (cf. van der Woerd et al. 2022, Hiermaier et al. 2017). In addition to these physical barriers, a strict access control regime was in place, and CCTV was omnipresent. It required me to be pre-registered, take a COVID test on site, and identify with my national ID card. The visitor badge I received was to be always worn visibly, and it restricted my access. To reach the control room, further security locks had to be passed.

Fences, gates, and CCTV are complementary standardised parts of the grid's physical security, operating in a duality of the everyday and the exceptional. Focusing on the potential threat from unauthorised and authorised entry into a facility, they aim to deter, hinder, control, stop, and detect it. By restricting access and directing the remaining flow of people, uncertainty about who enters is

excluded, while those seemingly familiar faces can be controlled and monitored more easily. The accreditation I received certified me and allowed me to become known, lifting me from a category of unknown, potential danger into one with a justified interest and some access rights. While the physical security architecture operates in the everyday, their primary task is to pre-empt exceptional events, such as terrorists or saboteurs compromising the control room. A senior security officer reflected in an interview: “What if ‘evil forces’ want to sabotage us? What if a suicide bomber wants to blow up the control room? What if we have a blackout and we are a lighthouse in an ocean of darkness?” (Interview 100521).

In the everyday, the uncertain threat is the (il-)legitimacy to access and the potential of a threat. In the exceptional standards that dictate the design of perimeter security (IEEE 2021), access control or explosive resistance (van der Woerd et al. 2022), imagine and assume the materialisation of a threat by default. By doing so, they do not question the need to secure, but only when the ‘defences’ will be needed and if they are strong enough. An imagined scenario informs the standardisation. To render the future known in this way allows uncertainty to be contained, a specific future to be pre-empted, and standards defined through backcasting. If we assume a 20t lorry at 60km/h is loaded with explosives and trying to breach the front gate, how strong must the gate be to withstand, and how strong would the blast wave reaching the main building still be? What are the procedures in place if an intrusion is detected? Once in place, the technical and procedural standards guaranteeing security in the exceptional can seem static and inflexible. They might either hold, break, or be circumvented, succeed or fail. When the reference scenario changes, the security standards risk becoming obsolete and might need to be reinforced or updated.

When becoming static, built-in, inflexible and almost forgotten, security standards for exceptional events risk losing some of their ability to contain uncertainty. This is more problematic for procedural standards requiring constant engagement and practice to maintain effectiveness. For this purpose, exercises, drills and training are not deployed “as a significant new form of knowledge” (Collier 2008). Nore are they deployed to “explore the contingency and complexity of an event” (Anderson 2010b). Instead, or better in addition to these, they are to uphold the idea and procedural knowledge necessary for the continued functioning of these security standards. Local fire protection standards that also apply to the TSOs serve as an example. They do not only consist of technical measures to prevent the start and spread of a fire but also a requirement for quarterly fire drills (Land Baden-Württemberg 2017, 2019). The fire drill should uphold the idea of constant potential danger and force the participants to re-engage with the standardised actions to be taken in the event of a fire. Likewise, the critical infrastructure requirements for auxiliary and uninterrupted power supplies (DIN CDE 0100-710, DIN EN 50171, DIN EN IEC 62040-1) require regular tests. These do not solely serve to confirm the technical functioning of the equipment but also aim to uphold an awareness of why they are there in the first place (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2019). To be reminded of what is at stake is to decrease the latency between recognising a potentially dangerous situation and acting on it in the right, meaning the standardised way (cf. Anderson 2017).

The previously discussed security standards for exceptional events provide a form of security that aims to contain and render inert potentially emerging threats through relatively rigid technical and procedural specifications. Yet, their ability to contain uncertainty will ultimately fail. Nevertheless, a form of standardisation that anticipates this moment of failure exists and secures uncertainty through standardised flexibility. As the failure or breakdown of processes or technical components is imagined

and made present, preparedness becomes a tool for pre-empting it**.** The private sector has developed tools to pre-empt the escalation or cascading of exceptional events by becoming prepared for them. Through preparedness, their emergence can ideally be halted, or at least the recovery to within a range of 'everyday' remains possible. They are specific standards for the continuity in the exceptional, yet only offer orientation as uncertainty propagates. They secure the grid, not by extending the scope of the eventuality they are designed for but by ordering the chaos of exceptional events and their response. Through this, they offer hope (cf. Anderson 2017) for (to regain) control and reversibility of the occurring damage. Although relying on technical standards explicitly specifying the characteristics of auxiliary power generators and other backups, these standards are primarily about procedures and organisational structure.

For the German transmission grid actors standards of business continuity- (ISO 22301, BSI 200-4), emergency- (ISO 22320, BSI 100-4), crisis- (ISO 22361), information security- (ISO 27001, BSI 200-1) or risk management (ISO 31000, BSI 200-3) regulate not just the everyday, but provide a structured way of knowing and engaging with exceptional situations. During my internship at TSCNET, I contributed to their professionalisation of business continuity management (BCM). Folkers (2017a: 105) calls BCM a "realpolitik of catastrophe". In this, he recognises that containing uncertainty in exceptional situations might require sacrificing everything but the business-critical processes. The designation of "business-critical processes" is a conscious act that the BCM standards call for (ISO 22301, BSI 200-4) and that I got to participate in at TSCNET. BCM is intended to identify vulnerabilities and evaluate those services that should be kept operational or recovered first in exceptional circumstances. When the business-critical processes are identified, BCM coordinates and aligns the existing plans to guarantee their continuity and quick recovery. When I arrived at TSCNET, they had recently suffered a local power outage (Hans 2021). During this outage, and in accordance with their existing plans, all services deemed unessential were shut down to preserve the remaining battery capacity of the uninterrupted power supply for the servers running their critical services. After this event, their awareness of the need to plan for continuity was heightened, and further potential futures were imagined and singled out to be pre-empted. As their new office was under construction, this event influenced its design. Among a range of measures, auxiliary power was implemented.

Even though business continuity management anticipates future events that are to be pre-empted, it surrenders the ideal of being able to avoid harm. Rather, it prioritises continuity and rapid recovery to prevent long-term consequences from interrupted services by pre-positioning procedural and technical standards. For the TSOs, this entails that they first try to pre-empt through standards and prevent through forecasts (next chapter) a blackout as best as they can, but if it should occur, they do not let it become prolonged and a catastrophe. TSOs are obliged to prepare, in a standardised way, for risks specified in a European transmission grid risks catalogue (European Parliament & Council of the European Union 2019b). Furthermore, they prepare and train for the 'black start' of the grid after a blackout, develop and rely on standardised procedures and technologies (black start capable power stations) to do so (European Commission 2017c, DUtrain 2022). In pre-positioning plans to pre-empt catastrophe, the BCM standards used in the power industry (ISO 22301, BSI 200-4) reconfigure the organisational structure and information flows. Furthermore, if a threshold of potential or actual threat has materialised, the "relocation" (cf .Erkens 2018) to 'hardened' alternative control centres is an option. Furthermore, for crises and through economic rationales, the German TSOs cooperate, pool and share standardised emergency equipment, such as auxiliary and fast-to-erect transmission towers (VDE FNN 2020). Security standards combined to ensure contingency do not maximise security

but by complying with the minimum level of security mandated by laws and regulations (Folkers 2017a, b) .Where the minimum level of security provision is exceeded, this is often a legacy of Cold War infrastructures, such as bunkered alternate control centres or underground auxiliary fuel storages, that escaped becoming part of the peace dividends (Friedensdividende). Combining different relatively inflexible standardised tools makes their overall response ability more flexible.

4.5 Conclusion

This chapter positions standards and standardisation as a fundamental security technique for the power grid and the security of the electric supply. While standards and standardisation appear in the literature (Brunsson & Jacobsson 2002b, Easterling 2016, Galloway & Thacker 2004, Lampland & Star 2009), they are largely absent in the debates on security and as a distinct security technique. Positioning standards and standardisation as a security technique is a novel and innovative contribution of this thesis to the debates on securing in the everyday and exceptional. Standards and standardisation 'secure by' pre-emption and preparedness as they 'work on uncertainty' by containing uncertainty via pre-positioned decisions. Thus, they 'relate to a future' that emerges when imagined and backcast present decisions from it, creating a reliability of expectation.

Standards and standardisation were demonstrated to be effective in addressing the technical and procedural aspects of the transmission grid, albeit with clear limitations, scopes, and bandwidths within which they operate, thereby providing some level of security. Negotiated by European regulators and industry lobbies, they represent coordinated expert visions about futures that are to be pre-empted and prepared for. Both pre-emption and preparedness draw from the creativity with which acceptable or avoidable futures are imagined. These future imaginaries then provide the basis for backcasting and shape the standards and standardisation that will be positioned to achieve or avoid an imagined future. As they act in the "future present" (Adam & Groves 2007), uncertainty about what might emerge is contained for as long as what is emerging stays within the range of what has been imagined. The future becomes known through the standard and standardisation of technical components or procedures. Through standardisation, a reliability of expectation about what might happen is formed.

Standards and standardisation are foundational for the functioning of the power grid, thus its secure operation (Hughes 1983, Taylor 1941). They are an infrastructure of their own, or at least are infrastructure-like (Star 1999). They permeate almost every aspect of the built environment and its organisation. They are layered onto each other, have legacies and histories, and are only replaced or updated in a modular fashion. They provide what might emerge (can) become known and, through this, contain uncertainty. As the language used by engineers to describe and imagine the grid, they are severely backgrounded and transparent in the everyday.

This chapter has shown that standards and standardisation are not merely technical artefacts but central to the anticipatory governance of the power grid. They operate through a logic of containment, working on uncertainty by bounding what is knowable and ensuring reliability within a predefined range. By defining what counts as 'normal' or contingent operation and delineating acceptable deviations, standards and standardisation stabilise infrastructural expectations and enable timely interventions. Whether embedded in data formats, reserve power protocols, or the physical barriers of a control centre, they contribute to the coordination and continuity of infrastructural life. Importantly, their (political) power lies not only in their technical design, but in how they prefigure futures and organise practices around imagined threats. In this way, standards and standardisation are cemented anticipatory regimes that secure and stabilise volatile flows by stabilising specific visions and excluding others.

By tracing how standards and standardisation operate across technical and procedural domains, and from the everyday to the exceptional, this chapter contributes to a growing body of Critical Security Studies concerned with how security is performed (Amoore 2014, Aradau & van Munster 2011, Collier

& Lakoff 2015). It has demonstrated that standardisation is a form of technopolitical intervention, one that enacts security through classification, pre-specification, and routinised coordination rather than sovereign decision. This shifts attention away from discourses of threat and toward the infrastructures, routines, and anticipatory devices through which futures are governed. Building on the thesis's broader biopolitical framing, the chapter has illustrated how securing the power grid involves the organisation of life through standards and standardisation: deciding what is safe enough, which events are tolerable, and how resilience should be enacted. In doing so, it not only addresses a blind spot in CSS but also strengthens the analytical bridge between security studies, infrastructure studies, and science and technology studies. By tracing how standardisation practices shape the epistemologies, routines, and material arrangements of grid operation, the chapter engages directly with infrastructure studies' interest in relationality and embeddedness (Larkin 2013, Star 1999), while also responding to STS concerns with classification, protocol, and the politics of design (Bowker et al. 2019, Lampland & Star 2009). Through this, it offers a situated account of how technical practices secure life not only in discourse, but in the infrastructural ordering of the everyday.

As the foundation for the technical and operational functioning of the power grid, standards and standardisation marked the first empirical engagement with techniques that secure the power grid. The following two empirical chapters focus on forecasting and training and rely on standards and standardisation. For forecasting and training the European legislations that standardise power grid operation provide the methodologies informing how forecasts are calculated or how often specific trainings should be completed.

In the next chapter, I shift to forecasting as a security technique. It will show how forecasting, although reliant on standards, works by reducing rather than containing uncertainty. Forecasts can reduce uncertainty as they engage with a knowable and calculable future. Yet, they are not opposing but supplementing each other to provide power grid security.

5. Forecasts as Security Technique

5.1 Introduction

The previous chapter presented standards and standardisation as an essential security technique for the power grid. Through imagining futures, these techniques allowed for the backcasting of actions to be taken in the present to avoid or bring about a desirable/undesirable future. They primarily allowed uncertainty to be pre-emptively contained in manageable pockets as actions in the 'now' are based on the expected. This chapter shifts the focus from the standards and standardisations imaginary mode of backcasting to the calculatory mode of forecasting.

Forecasts are a probabilistic security technique that 'secure by' preventing an unwanted future. They 'work on uncertainty' by reducing it and 'relate to a future' that can be known and altered. Through the calculation of the forecast, an emerging future becomes a potential threat and can be prevented. For the security of electricity supply, however, the aggregation of multiple forecasts, rather than a single forecast, aids in securing it. They are multiple in two ways. First, forecasts, as discussed in this chapter, prevent as they reveal what might happen for a specific metric, grid element and spatiotemporal horizon by projecting the past into the future. A multiplicity of metrics, elements, and spatiotemporal horizons relevant to power grid security are calculated. Secondly, calculating speculative and explorative iterations of the same forecast and modulating the inputs can identify the best path for preventing unwanted futures. TSOs and RSCs, such as TSCNET, play a crucial role in this process, deploying forecasts to maintain grid security.

This chapter contributes to ongoing debates within Critical Security Studies that explore how security is organised through mundane practices, calculative infrastructures, and anticipatory techniques. Rather than viewing security as a response to discrete threats or exceptional events, this literature understands it as a continuous process of governing uncertain futures (Anderson 2010a, Anderson & Gordon 2017, Aradau & van Munster 2011). Investigating forecasting contributes to this understanding by showing how the future is not only imagined or discursively framed, but also rendered operational through calculation and modelling, as well as (near)-real-time measurement and analysis. It highlights the infrastructural and epistemic work involved in making uncertainty actionable and preventing potential threats. By tracing how forecasts function within electricity transmission operations, this chapter grounds CSS concerns with anticipation and biopolitics in the technical routines of infrastructure governance. It advances the thesis's broader argument that security is materially performed, not through sovereign acts, but through the situated and routinised labour of securing circulations in the everyday.

Forecasting in this chapter refers to securing the flow of electricity through enabling prevention. In following Massumi (2007: 2) "prevention assumes an ability to assess threats empirically and identify their cause. Prevention operates in an objectively knowable world in which uncertainty is a function of a lack of information and in which events run a predictable, linear course from cause to effect." Prevention then aims to spawn action that moves potential emerging threats, such as imbalances of generation and demand (system adequacy) or 'network security issues', such as overloads, to become non-events. Prevention aims to render uncertainty safe by reducing it for specific spacetimes and metrics. Any emergent event holds the potential to escalate or cascade towards a blackout, to threaten the lives dependent on the grid as critical and vital infrastructure. The potential to affect the security of the power grid, however, depends on the metric and element forecasted and the specific spacetimes in which these become critical. Forecasting then intends to make known the relation of

when, where and why a particular metric (voltage, frequency, overloads, etc.) in a particular grid element (transmission line, transformer, etc.) becomes a likely threat to the continuous flow of electricity. In the words of the interviewed head of system security: “The security of the power grid is decided on the eve of tomorrow” through adequate forecasts (Interview 2). By forecasting what is likely to happen, a week, a day, or even hours in advance, potentially dangerous events can become preventable.

Recent years have seen an increase in the volatility of European and German power flows, given the growth in decentralised and mostly weather-dependent renewable generation required for electricity decarbonisation (Übertragungsnetzbetreiber 2024, Burger 2024, European Commission 2019). While forecasting is a sustained practice in grid operation, in part, this volatility is challenging for forecasts as their temporal resolution might not be high enough to represent this volatility and offer the ability to prevent. Thus, in combination with arguments about a shift in the scale at which the grid is to be governed and secured (from the transmission to the distribution scale), the literature on ‘smart’ grids identifies a shift towards ‘nowcasting’ (Folkers 2019b, Bulkeley et al. 2016a, Luque 2014, Bulkeley et al. 2014, 2016b). Following Kitchin (2019: 782), nowcasting is “using real-time data to predict present and very near future conditions”. Such a shift would imply that lives vitally connected and dependent on the power grid would be secured through ‘real-time’ management rather than the future (Amin 2010). Uncertainty about the future would not need to be reduced through forecasting and rendered ‘safe’ as in the present, what is happening could become known through sensing.

Engagement with ‘real-time’ in this chapter then serves two purposes. First, it identifies where ‘real-time’ is and what it is doing. This investigates the possibility that, besides forecasting, ‘real-time’ could, or should be, a focused security technique for power grid security and uncertainty management.

Secondly, as the contemporary literature on power grid security (Bulkeley et al. 2014, Folkers 2019b, Luque 2014) suggest a growing importance of nowcasting, to engage with ‘real-time’ justifies and demarcates this chapter's focus on the forecast. Given the temporalities through which forecasting works and engaging with how I encountered ‘real-time’ during my ethnography and participatory observation is helping to underline the significance of forecasting as a security technique.

To address and locate real-time in the current transmission grid, the first section of this chapter asks what and where ‘real-time’ is currently operating and contributing to the security of electrical supply. Through providing three examples from observations at the German TSO, TransnetBW, ‘real-time’ will be shown to multiple while complicating the separation of past, present, and future in the ‘close to’. In contrast to the forecast, which aims to prevent a future, ‘real-time’ will be shown to primarily function reactionary and focus on managing occurring events. If what is occurring in the present can be sensed, uncertainty about what is happening is lifted, and potentially remaining residual uncertainty can be ignored. However, rather than appearing as a security technique for the contemporary power grid, ‘real-time’ will be shown to rely on standardisation to respond to emerging events promptly.

In the second section, forecasts will be positioned as security techniques that differ from nowcasting. Forecasts secure life dependent on the vital electricity supply by reducing uncertainty for specific metrics, grid elements and spacetimes. Instead of being able to ignore, they reduce uncertainty. Through prevention and depending on the metric and element forecasted, the forecasts aim to move

the uncertainty about what is emerging to within the coping capability of matching standardised security techniques discussed in the last chapter.

Illustrating how forecasts aid in securing the flow of electricity, the third section will expand the previous section through the example of three distinct forecasts. Examining how planned outages (OPC/OPC), transmission capacity (CORE FB MC) and grid congestion (DACF) are forecasted illustrates how they secure specific futures. While these forecasts aim to make different elements of uncertainty known for their respective spacetimes, they all indirectly or directly prevent overloads. If the overloading of grid elements surprises and is severe enough, it can lead to escalating and cascading failure and the blackout. By making known when and where outages will occur, they lose their ability to cause overloads surprisingly. By making known how much transmission capacity can be used to exceed it, overloading becomes unlikely. Overloads can be prevented by making known when and where grid congestion will occur. In conclusion, I argue that, unlike standards, forecasts work by reducing uncertainty about what is happening by calculating likely futures. This opens a window of opportunity to prevent unwanted futures, thus aide in securing the power grid.

5.2 What and Where is Real-Time in the Current Grid?

Generally, real-time is an intangible term that primarily and qualitatively evokes the management of a present via an instantaneousness between measured, sensed data, information processing, and subsequent action (de Lange 2018b). In its temporal definition, 'real-time' remains a vague term as neither in academic literature nor in government documents is it regularly quantified as seconds or minutes. The recent increase in the general usage of 'close to real-time', its temporal vagueness, further complicates its temporal distinctiveness yet allows for its use in multiple environments.

Ideas of 'real-time' management contributing to the security of (electric) flows are regularly addressed in academic literature (Luque-Ayala & Marvin 2020, Kitchin 2019, 2014, de Lange 2018a, Bulkeley et al. 2016a, Luque 2014) and German government documents (Bundesnetzagentur 2011, 2017). Real-time is closely related to ideas of 'smart' and its various technologies (smart grids, meters, cites, etc.). It sits at the core of the operational logics of these supposedly 'smart' technologies, as it enables and functions through a temporality of constant corrective action in a "perpetual present" (de Lange 2018b: cited in, Kitchin 2019: 783). "By capturing a phenomena as real-time data, it seemingly becomes possible to model, understand, manage and fix a situation as it unfolds" (Kitchin 2014: 9).

For the German Federal Network Agency (Bundesnetzagentur 2011) the 'smart' grid is explicitly defined by the grid's ability to sense and manipulate the flow of electricity in an emerging present. Collocating with 'smart' grids, 'real-time' is positioned as a novel addition to the operation of the power grid twofold (Bundesnetzagentur 2011, Folkers 2019b). Firstly, it is seen as an answer to the relatively uncontrollable volatility of renewable generation. To harness renewable potential, the period of the generation forecast is shortened and collapsed into the present, increasing their accuracy. Secondly, these forecasts are used by 'smart' electricity markets to align not generation with demand but, inversely, demand with the momentarily available generation. This partly inverts the responsibility for power grid security, shifting it from the TSOs—who are currently legally responsible for balancing generation and demand (European Commission 2017a, b)—to households and consumers (Hodson 2023a, b, Bulkeley et al. 2014, 2016b, Strengers 2012, 2013).

So potentially, 'real-time' could be understood as a distinct security technique that secures life and the vital flow of electricity through the management of those events that are unfolding in the present. Yet, debates that would position 'real-time' as an additional security technique of the power grid were absent during my fieldwork. On the level of TSOs and RSCs at which I conducted my research, the non-usage of 'real-time' appeared as a caution against fantasies of 'real-time' being a 'cure-all' and a fashionable buzzword. 'Real-time' during my fieldwork did not surface as a novel nor a 'smart' attribute that reconfigures the power grid's conduct and security. If 'real-time' was mentioned during my ethnography at TSCNET, during participation in the TransNext challenge and my observations in the main control room of TransnetBW or interviews, it appeared as a more nuanced understanding of the grid's temporalities. Answering the question of what and where 'real-time' was located in the part of the transmission grid I engaged with locates it in three examples: The substation, reserve power activation and redispatch. Examining the temporalities of these examples will highlight the diversity and different temporal ranges of 'real-time'. Regarding power grid security, 'real-time' will surface as enabled by standards rather than as an independent security technique. To examine and demarcate 'real-time' aids in explaining the focus on fore- rather than nowcasts. Without this section, the question of whether forecasts are the right focus for how the contemporary German power grid is secured would still stand.

The first example of ‘real-time’ is the temporalities of the (transmission) substation and its protective equipment. Reviewing their layout, an employee of a German TSO explained, during the TransNext Future Innovation Challenge I participated in, that substation protection was about milliseconds. About the split second it takes for surge currents from an exemplary lightning strike (that hits the power lines relatively regularly) to migrate through the network and reach the substation. Similarly, large starting currents from industry consumers that briefly draw 'too much’ power can cause system stability issues that threaten to damage the equipment in grid nodes and junctions, and the substation. To protect their most valuable component, the transformer’s surge arrestors, disconnection switches and circuit breakers function at lightning speeds. They are almost entirely electromechanical and well-established mechanisms and security devices (see Figure 4). ‘Real-time’ operation in milliseconds for these devices is enabled through decentralised automation, enabled by standards and protocols. Being decentralised and automated, they do not require or rely on a centralised control room, as detection, diagnosis and response are performed locally.

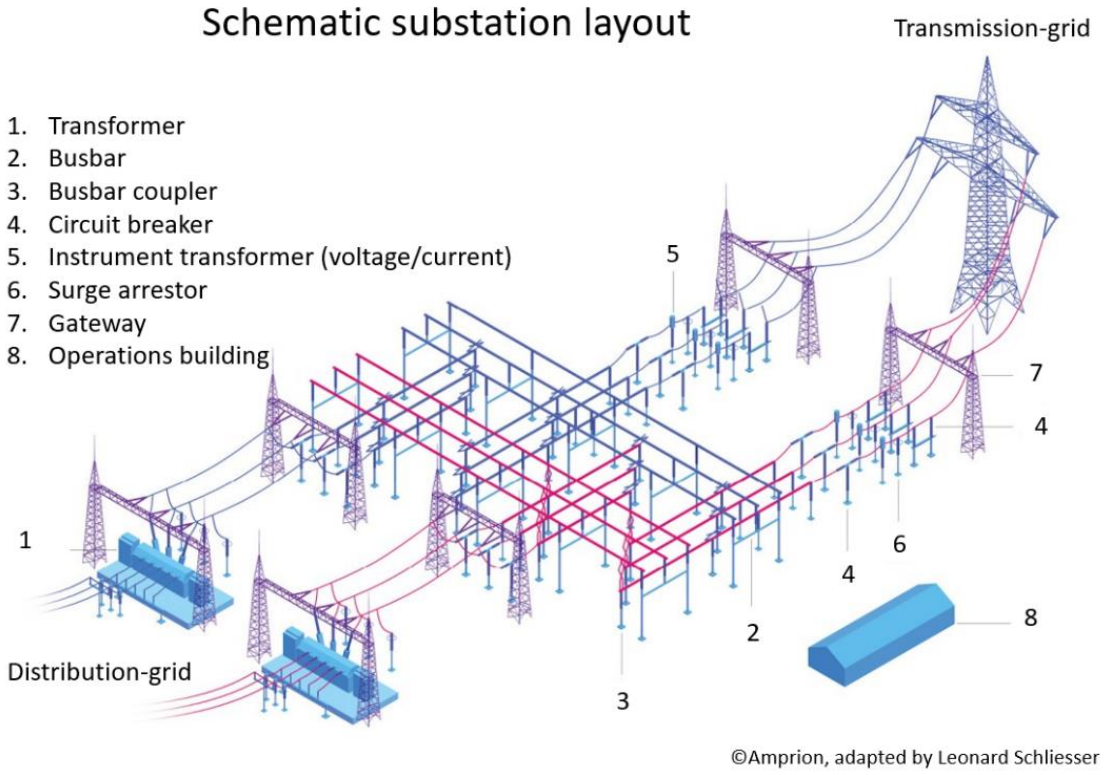


Figure 4 Schematic Substation Layout

Besides adjusting their parameters, TSOs and control room operators do not have the ability to influence the substation's automatic mechanisms. Nevertheless, for everyday operations, such as maintenance or adjustments to the grid topology, remote access is embedded to enable ‘switching’ operations. Switching operations have their own temporality that extends into minutes. Switching in substations is enabled and mediated through supervisory control and data acquisition systems (SCADA). Utilising an independent fibre-optic infrastructure, the converted electronic sensor readings, signals, and commands are transmitted and manipulated in a distant control room of a TSO. The operators in the control room are aware of the devices’ individual ‘switching times’ (Schaltzeit) – the latency between a given command and actual changes in the substation’s topology.

Reflexively, however, the speed of possible action is a potential threat to grid security. Speed negates the ability to thoroughly assess the implication of action and their potential to worsen a situation, to risk lives as well as the stability of the system (Roe & Schulman 2008, UCTE 2006). To be slow is safe, and to be safe is fast. Thus, even if substation switches can be remotely controlled and operated within seconds to minutes, it is not necessarily the speed of the devices and the control signals that determine the speed of the operation, but safety protocols. They, for example, reduce the operational speed to protect linemen working on the grid, as well as the flow of electricity itself. The lineman, for example, must be in direct contact with the switching operator in the control room to receive and confirm that the power is off. In reducing the speed of these switching operations, human errors are reduced. Time to recognise and to correct mistakes is given. Furthermore, taking grid elements offline for maintenance is typically the culmination of a longer planning cycle that involves thoroughly assessing the implications of a planned outage. Just because a plant requires some maintenance, it is not immediately switched off, but only after a longer process. The outage planning, coordination and inconsistency forecast will be introduced as an example later. Before any switching operation, numerical models must simulate the impact of topological grid changes and their impact on system stability, reducing the utility and possibility of 'real-time'.

'Real-time' in the substation and its secure operations are multiple as they range from lightning speed of milliseconds over seconds to minutes. Rather than being a novel attribute of a 'smart' grid, it is enabled and constrained by legacy technical and procedural standards, established technologies and their physically conditioned latencies. To ensure the substations and the control rooms' ability to operate even during a power outage or blackout, they are protected, not through 'smart' technologies, but established uninterrupted power supplies (UPS) and auxiliary generators. These again have a specified temporal interval in which they become activated. Depending on the UPS type (offline, line-interactive, online), their power is available continuously or within milliseconds (International Electrotechnical Commission 2022). Auxiliary generators, on the other hand, are slower and generally available within minutes of activation, depending on them being on 'hot' or 'cold' standby (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2019).

'Real-time' is also relevant for balancing generation and demand via the grid's frequency. The balancing needs to be nearly instantaneous to guarantee the stability of electrical flow. It further exemplifies and extends the temporal understanding of 'real-time'. For the different balancing services that will be introduced below, 'real-time' operates in intervals of decadal seconds and minutes. As explained in the last chapter and to counter potentially dangerous frequency deviations, the TSOs are required to, and rely on a suite of reserve power (see Figure 5) to contain the frequency within its acceptable margins (European Commission 2017a, b).

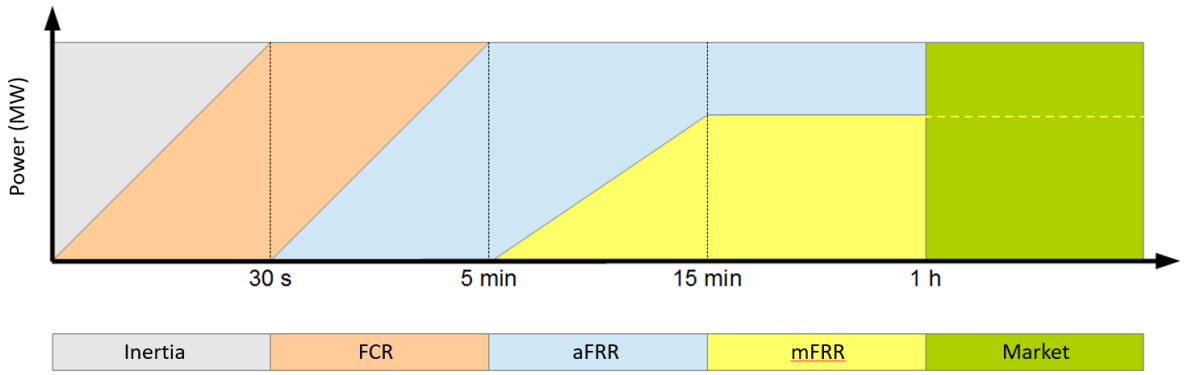


Figure 5 Idealised Reserve Power Activation. Adapted from Wikipedia

Besides the inertia of the generators weighing in the hundreds of tons and spinning at around 1050 rounds per minute in conventional power stations, the 'Frequency Containment Reserves' (FCR) are the fasted tools of the TSOs to stabilise frequency deviation. The following automated and manual 'Frequency Restoration Reserves' (FRR) are then intended to bring the frequency back within its 'safe' margin. The FCR are pre-contracted, certified and non-selectively intervene automatically (Übertragungsnetzbetreiber 2022). The protocols governing them ensure their speed. If a load frequency controller, an electrotechnical grid component at the FCR provider, senses the frequency wandering beyond the set measuring deadband (49.99 Herz (Hz) – 50.01 Hz), the FCR is activated. As the first line of defence against frequency oscillations and per 'System Operation Guidelines' (SO GL) the FCR must provide 50% of their concreted power within 15 seconds while reaching maximum output at 30 seconds if the frequency deviation equals or exceeds 200 Millihertz (mHz) (European Commission 2017a). The 'automatic Frequency Restoration Reserves' (aFRR) consecutively replace the FCR to replace the amount activated and make them available again quickly. Their activation must start within 30 seconds, and they should be fully activated within five minutes.

Although their activation is fast and enabled through their decentralised mode of operation, there still exists a lag between frequency change, sensing them, reserve activation, and their full availability. This lag partly resides in the physical properties of the individual electrotechnical components, like the load-frequency controllers and, in the case of the power plants, their ability to 'ramp up or down' generation. These automated and 'fast' means of frequency control are supported by 'manually' activated by 'Frequency Restoration Reserves' (mFRR). As they are not automatised, their actuation is slower, while they must deliver their contracted power output within the same 15 minutes as the aFRR (European Commission 2017b). The activation of FRR happens in succession to replace and 'free up' the FCR again. For these automated and manually activated reserves, 'real-time' is an interval of dozens of seconds to a quarter of an hour. The stabilisation and restoration of the grid's frequency, however, remain reactive.

Further complicating and extending 'real-time' to the border of a reactive present with a preventative future is 'redispatch'. As the third example of 'real-time' in the grid, it operates in a temporality that might still be considered 'nearly' instantaneous. The substation's security devices protected the grid from power surges. The containment and restoration reserves stabilised and restored the grid's frequency, and 'redispatch' addresses the potential threat of overloads that could lead to cascading power line tripping. Upon request by a TSO, power plants and large industry consumers alternate their operating schedules and their generation or consumption to avoid or respond to grid congestion.

Whereas large industries have for decades already contributed to providing curtailable power (abschaldbare Lasten), the made flexible (aggregated) household demand promises by 'smart' grid narratives is largely still not available for redispatch (Bundesnetzagentur 2011, Bulkeley et al. 2014).

In the following example of an observed redispatch process, the interval of responsive intervention that operates through 'micro horizons of futures' (Luque-Ayala and Marvin 2020: 130) is further extended into the close to 'real-time'. It highlights the difficulty of temporal bordering in grid operation. It highlights the difficulty of separating the future, acts of forecasting and preventative action from the present, 'real-time' operation, and reactions.

Accompanying a system balancer in the TransnetBW control room for an evening shift, the control engineer tasked with running forecasts (operational planner) came over. He asked for a positive (+) redispatch of 300 Megawatts to help the northern TSO neighbour Amprion to counterbalance impending, forecasted grid bottlenecks (Netzengpässe) in their control zone. It was around 21:50, and the power redispatch was requested from 2230 to 2400. As all power stations in the TransnetBW control zone were already operating at their maximum, the system balancer picked up the phone and called the southern TSO neighbour, Swissgrid. With a few words, the extra electricity was requested. Around 22:00, the operator from Swissgrid called back to confirm that they could provide the +300MW of redispatch for the requested interval. This relatively late request did not amuse the system balancer. First, this was due to Swissgrid having to do their security calculations (forecasts of what effect this power flow change has on their grid) before confirming that they could deliver. Secondly, the computer software with which redispatch was officially ordered was badly designed, thus slow to use; more of a 'redispatch prevention software', the system balancer joked. Although the redispatch was agreed upon and ordered within ten minutes and 30 minutes in advance, the felt 'rush' was 'inconvenient' for the balancing operator I joined. It was perceived as an unnecessary and potentially threatening situation for grid security (fieldnotes 281021). Without this, redispatch transmission lines could have become overloaded or violated their N-1 security margin, risking cascading failure in case of unforeseen events. If the request had come in just 15 minutes later, fulfilling the balancing operator explained would have been almost impossible.

In this example temporality of 'real-time' is extended to incorporate the 'close to'. It now extends beyond the temporal horizon of the abovementioned frequency control reserves or the substation's protective devices. As the forecast of grid congestion reduced the uncertainty of a potential impending grid bottleneck and crossed a threshold, the need for action in the present took effect. The forecast of gird congestion enabled its prevention in the present. The actions to prevent, however, possessed their own temporality as the telephone conversation between the balancing operator from TransnetBW and Swissgrid was instantaneous, while a lag remained between the request for redispatch, its confirmation, it's becoming an official order, and its fulfilment from 22:30 onwards. Similarly, to the switching operations in the substations, this lag is largely due to security protocols that are to ensure that intended preventive action does not exacerbate or create new problems.

Following these three examples, (close to) 'real-time' in the power grid is multiple. It is milliseconds, seconds, minutes and potentially up to an hour, while primarily functioning reactionary through different space-times, without being a novel ('smart') attribute of the power grid. 'Real-time' in the power grid is polyrhythmic while following cyclical time. It follows the rhythms of power flows and their frequency, the 'close to' projection of grid congestion. While the literature on 'real-time' and its related 'smart' initiatives position it as a technique securing various flows, including electricity

(Bulkeley et al. 2016a, Bundesnetzagentur 2011, Luque 2014, Luque-Ayala & Marvin 2020, Powells et al. 2014), I did not encounter it as such during and in the part of the transmission grid I engaged with. In these examples time is constantly advancing while the cycles of measurement, assessment and decision/non-decision continuously revolve.

Securing the grid in these timeframes relies on standardisation-enabled automation that contains uncertainty. 'Real-time' in the shortest timeframes can only operate not because what is ongoing is sensed and nowcasted, thus becoming known, but because the responses to the sensed are preprogrammed. In the 'close to', short-term forecasts trigger preventative action. How the estimates secure the flow of electricity in the everyday will be detailed in the following section.

5.3 Forecasts as a Security Technique for the Power Grid

In the previous section, 'real-time' in its various forms secured the grid at a point of certainty about what is happening. It was discussed as a potential security technique for the power grid that, unlike a forecast, operates in a sensed, thus known present and through its real-time management. The form of 'real-time' encountered by me, however, differed from 'smart' (grid) narratives found in the literature (Bulkeley et al. 2014, de Lange 2018b, Luque 2014, Luque-Ayala & Marvin 2020). 'Real-time' was shown not to be a novel, digitally enabled security technique operating on what is known and through constant corrective action in a "perpetual present" (Kitchin 2019: 783). Instead, 'real-time' was shown to be multiple and in its various forms already preexisting in the grid. Standardisation, rather than the addition of digital technologies, enabled 'real-time' to secure in the present.

This section will position forecasts as security techniques before the next section engages with three exemplary forecasts. In contrast to 'real-time', forecasts aim to secure not a perpetual present but an emerging future. In engaging with 'real-time,' the relevance of the forecast was highlighted, and 'real-time' was primarily shown to rely on standardisation to ensure instantaneous responses. In making known an uncertain future, the forecast can prevent these standards from being exceeded.

To prevent developing events from becoming a threat, forecasts aim to reduce uncertainty about what is emerging. Through the act of forecasting, emerging events become as a threat (cf. Campbell 1998a) to power grid security and can be prevented. "Through operational planning [forecasting]", the balancing operator I joined in TransnetBWs control room explained, "the big boulders [emerging dangerous grid situations potentially exceeding the standardised everyday coping capacities] are moved out of the way so that [standardised] operations can clear the smaller ones" (Fieldnotes 281021). The forecast reduces uncertainty about emerging threats for a specific metric, grid element and spacetime. It opens a window of opportunity for preventative action to lower the emerging threat to a 'safe' level manageable by the prepositioned standardised techniques such as reserve power activation.

Securing the grid through forecasting is not a recent development. During the early decades of electrification (1880 – 1930), 'load-following' was the default mode of grid operating before energy markets. Anticipation and predictions were essential to ensuring the balance between demand and generation (Hughes 1983). The load dispatchers would observe frequency gauges at the substation or later in the control room. Through experience and calculations, they could equate a frequency change to the amount of 'missing' or electricity in 'excess' while respecting the operational limits of network assets to transmit or transform power. Via telephone, they advise individual power plants to increase or decrease their power output as needed. "The load dispatchers was […] something of a historian", writes Hughes (1983: 214) that by analysing the hourly load records of the previous year, was able to "anticipate loads resulting from the social customs and industrial routines […]." With the advances of technology and the power grids becoming more complex, mechanical automation and (analogue) computers have taken over part of this work.

With the liberalisation and disentanglement of the vertically integrated monopolies of the electricity sector in the late 1990s and the creation of power markets, the forecast became ever more important (Lehtonen & Nye 2009). With market liberalisation and electricity transitioning from public goods to traded commodities, power flows increased and with them, the potential for emerging events to escalate or cascade towards a blackout. Additionally, whereas the network control centres previously

dictated how a power plant produces electricity, it now is (under normal circumstances) the energy markets that allocate and balance demand and generation.

The future addressed and secured by the forecast is pre-given (Adam & Groves 2007). The forecast "operates in an objectively knowable world" where a disability to forecast is attributed only to "a lack of information" (Massumi 2007: 2). The future that is to be forecasted is a function of what has been, and the forecasts' ability to prevent heavily relies on the past (Adam & Groves 2007, Massumi 2007, Kitchin 2019). The forecast depends on 'what was' in at least two ways: Firstly, and concerning the grid, the models that are used to forecast are derived from an understanding of how frequency, voltage and amperage used to interact in a specific space-time, paired with assumptions about the future. Secondly, the calculatory basis of the forecast itself is primarily past data that gets (linearly) extrapolated.

Within the grid models used to forecast and presented in the next section, no uncertainty exists about the interrelations between grid components and power flow. The models create a world and based on historical data, forecast a future that can 'objectively' be known and is coherent. To do so, the models used for grid operation might be complicated, but they are no black boxes. TSOs and RSCs are not only liable for their actions, but the potential for catastrophe mandates their ability to attribute outcomes to their inputs. Additionally, this aids the TSOs and RSCs in identifying and fixing bugs or errors in their models and software tools. The utility of the forecast is judged, after the fact, by its accuracy, based on the deviation between the forecast and the 'real world' developments. Suppose this deviation is sufficiently reduced to within the scope of standardised coping mechanisms. In that case, it prevents the grid operators and standardised security mechanisms from becoming overwhelmed by uncertainty and the potential for a threat to emerge.

A forecast only makes know a particular future. Thus, the power grid is secured by a multiplicity of projections. As the threat to the security of electrical supply is never singular but multiple, it is not a singular forecast that manages to secure the grid alone. Through layering and in aggregation, forecasts of various metrics, elements and spatiotemporal horizons can secure against a wide range of emerging and potential threats. A forecast is just a focused spotlight on a snapshot of the future. Like a sweeping and focused radar beam searching the horizon, the forecasts, depending on their metric, element, and horizon, require perpetual, or at least periodic, renewal to guarantee their relevance. Furthermore, as the blackout remains a latent potential that cannot be entirely ruled out, the cadenced forecast must become and is a permanent part of the securitisation of everyday electrical supply (cf. Anderson 2010a).

Forecasts depart and span from the 'close to real-time' and the short-term forecasts of the 'intraday' to years ahead. They focus on predicting specific metrics and elements that strongly relate and sometimes predetermine the required temporal resolution. The three exemplary forecasts discussed in the next section will highlight this further. Furthermore, the forecast creators' territoriality inherently binds the forecasts' spatiality. In the grid and complementing each other, the transmission system operators (TSOs) and the regional security coordinators (RSCs) primarily deploy the forecast as a security technique. They calculate forecasts for their area of responsibility and, depending on the forecast's purpose, include their borderlands, a buffer zone of various sizes. As the grid is 'tightly coupled' (Perrow 1984) electricity flows are interdependent, and distant changes might cause local (unanticipated) fallout. Thus, the TSOs might include or monitor a 'buffer zone' extending hundreds

of kilometres beyond their control zone. The RSCs provide some trans-European forecasts and coordinate the TSOs' action to ensure these interdependencies are catered for.

What is at stake if the calculated future, the forecast, fails to predict their targeted metrics? For the power grid, the failure of forecasts might not cause sudden darkness. Yet, it increases the level of uncertainty that potentially threatens to exceed and overwhelm the standardised capabilities of the present to manage what is or might emerge. This could directly threaten grid security or indirectly compromise the economic viability of market participants and TSOs. The blackout, in any case, remains a latent potential. Without the awareness about the (near) future generated through forecasting, the risk of being surprised by, for example, sudden imbalances of demand and generation, overloads, or power quality (voltage) issues increases, and the standby reserves might be used and exhausted more often. Furthermore, while the potential economic cost of grid management without forecasts is a severe risk (Schulman et al. 2004), the market side of grid operation and security is beyond the scope of this thesis. Nevertheless, without a steady stream of predictions, the operational mode of the grid must change. It then reverts from a mode in which the market - enabled by the forecasts - is mainly responsible for balancing generation and demand to 'load-following'. During 'load-following', deviation of the frequency to its ideal of 50 Herz alone dictates the balancing work of power plants (European Parliament & Council of the European Union 2019d). In the exceptional, some forecasts lose, while others retain their utility. In the exceptional, those forecasts retaining their utility primarily serve the TSOs in assessing what effects their intended actions might cause (European Commission 2017a).

In the following section, three distinct forecasts will be introduced and presented as securing their individual futures. As exemplary forecasts from the portfolio of TSCNET, they showcase a multiplicity of forecasts working on and with different temporalities and metrics. While they individually contribute to grid security, presenting three shows how they are secure by coming together and secure in layers.

5.4 Forecasts for Regional Security Coordination

The first part of this chapter complicated the grid's temporalities and the understanding of 'real-time'. The second part then positioned the forecast as a distinct security technique for the power grid. Extending and substantiating the arguments for empirically forecasting as a security technique, this section will present three example forecasts from the portfolio of TSCNET, a regional security coordinator (RSC). During my three-month ethnography at TSCNET, I engaged with and learnt about them. They are amongst the core services TSCNET provides to its customer TSOs. Through these forecasts, TSCNET coordinates the TSO's regional security and aids in ensuring the flow of electricity. By attending the various daily shifts at TSCNET, I could observe these forecasting processes directly and repeatedly while attending the operational managers' (OMs) daily shifts. Furthermore, as part of my initial 'OM' training, I like a real OM, learned the process descriptions, sequences of actions, EU Regulations and about the things that can go wrong.

The selected forecasts aim to prevent overloads that could lead to escalating or cascading system failure. While they share some procedural commonalities, all three forecast targets 'overloads' differently. The OPC/OPI and CORE FB MC forecasts indirectly address the potential of overloads by forecasting specific metrics and elements that relate to and affect the possibility of overloads. The

third forecast, DACF, determines when and where potential overloads will occur and prevents their materialisation. As presented in table four, each forecast has its own spatio-temporality while making known, thus governable, a specific metric/element. As a 'puzzle piece' of grid security, these forecasts tackle specific and potentially dangerous uncertainties. They each offer to reduce the uncertainty for a particular space and time and to a point sufficient for the temporal horizon they address. By preventing emerging futures related to their metrics/elements, they reduce uncertainty within the bandwidth of standardised security processes, such as the balancing reserves. For their specific temporal horizon, the forecasts prevent the management capacity of the everyday from being exceeded. Analysing three forecasts (Table 5) showcases how individual forecasts work on specific elements of uncertainty and metrics to secure a particular temporal horizon. Yet, the following example also shows that not a single forecast is relevant for power grid security, but their multiplicity and layering is.

Table 5 Exemplary TSCNET Forecasts for Regional Security Coordination

	Temporal horizon	**Temporal resolution**	**Geographical extent**	**Element of uncertainty**	**Forecasted metric**	**Object of prevention**	**Output**
OPI / OPC	(Yearly, monthly) Week ahead	21 timestamps for a week, 3 per day	Pan-European, TSCNET Customers	Whether and where **planned outages** might cause **overloads**	Ordering and making known **planned outages**, to avoid network elements becoming **overloads**	Preventing **uncoordinated outages** from cause **unintended** and surprising **overloads**	Report / Teleconferences
CORE FB MC	Day ahead	24 timestamps per day		How much **transmission capacity** can be provided to the electricity marketed	To maximise cross-zonal **transmission capacity** without causing **overloads**	Preventing the marked from not being able to **auction transmission capacity**	Publication on market portal
DACF	Day ahead	24 timestamps per day		Where **overloads** and **N-1 violations** will occur, and of what magnitude	To examine if and where the forecasted flows will cause **overloads or N-1 violations**	Preventing **forecasted overloads**	Report / Teleconference

5.4.1 Outage Planning Coordination, Outage Planning Incompatibilities (OPC/OPI)

The security of the electrical supply depends on the availability of power grid assets that generate and transport power. Without enough generators or transmission lines, electricity demand could not be met. Life and lives depended on the flow of electricity, would be disconnected from the grid and severely affected, or left to die (Folkers 2017b, Petermann et al. 2011b). Furthermore, any grid

element, generator, or loads (large consumers) going offline, whether for planned maintenance, upgrades, or retirement, changes the grid's topography and affects its power flows, potentially adversely. If grid elements, generators, or loads go offline, redundancies and over-capacities, which are the security margins in the grid, could be compromised, or overloads created. If this happens uncoordinatedly and unexpectedly, it could lead to escalating or cascading system failure and the blackout. However, even though the power grid consists of thousands of parts, some individual elements might become more critical to the overall system than others. Such an element might be one of only a few large power plants in an area of high demand, like in the southwest of Germany or a specific cross-border transmission line.

To become aware of when and where outages are planned and whether they become incompatible with the security of the electrical supply, the OPC/OPI process is conducted by the 'regional security coordinators' (RSCs), such as TSCNET. As a process, it consists of two dependent parts and is mandated by the system operations guidelines (SO GL)(European Commission 2017a). Firstly, through the 'Outage Planning Coordination' (OPC), the RSC, TSCNET, aggregates the planned outages of all 'relevant assets' for its area of operation. While potentially all grid components can affect the flow of electricity adversely, for this process, only those "whose availability status has a cross-border impact" are relevant for this process (Coreso 2024). These are grid elements, generators, and loads (large consumers) designated as 'relevant' by the individual TSOs and can lie inside or outside their control zones. Additionally, the list of 'relevant assets' provided by the TSOs also contains the threshold metrics that qualitatively and quantitatively allow for the later identification of the impacts of planned outages (European Commission 2017a). Secondly, TSCNET would calculate the regional 'Outage Planning Incompatibilities'(OPI). Relying on the aggregated data from the previous process and a 'common grid model' (CGM), TSCNET would forecast the flow of electricity. Through this forecast, they would seek to identify whether, when and where planned outages would be incompatible with grid security, each other, or any 'relevant assets'. This would be the case if assets became overloaded due to the possible outage-induced changes in grid topology, thus of electricity flows.

The OPC/OPI process aims to prevent outages from threatening the security of supply. The OPC part of the process is conducted over a pan-European scale, while the OPI is a regional operational security analysis. When it is a pan-European assessment, it is calculated between the European RSC, like TSCNET. If it is a regional analysis, it is catered to the RSCs' customers. In the case of TSCNET, these are 16 European TSOs. Through the geographical extent covered, the TSOs can become aware of the planned outages around them and coordinate and assess the impact of these outages on their control zones. Since the electricity sector liberalisation and the unbundling need to gain such awareness is not a banality, data that previously was shared easily within vertically integrated monopolies must now be compiled and aggregated from multiple sources.

Like its specific geographic extents, the OPC/OPI process secures specific temporal horizons, another element common across forecasts (see Table 4). Although I only observed the perpetual biweekly calculations during my ethnography at TSCNET, it is also conducted periodically, monthly, and yearly. While the monthly and yearly process results still contain much uncertainty, the weekly process was explained to me as "extremely important for TSOs" (Fieldnotes 221121). In the temporal horizon of a week ahead, the available data is good enough to forecast whether the outages on the horizon are likely to become a security issue. Through forecasting the outage incompatibilities, the element of

uncertainty about when and where planned outages are likely to occur and become a problem is lifted and rendered safe.

After the OPC phase is completed, the second element of uncertainty, the outage incompatibility, can be forecasted. TSCNET calculated it based on the aggregated outages and 'relevant asset' list, the 'common grid model', and projected load and generation data. The calculation is done for a temporal resolution of 21 'timestamps' over seven days. This daily resolution of three evenly spaced timestamps was explained to me by the TSCNETS indigenous OPI tool developer/maintainer as a compromise between data availability, its validity and the computational speed and resources required. Furthermore, the entire OPC/OPI process is embedded in and followed by other forecasts such as the 'short-term adequacy assessment' (STA). Thus, this resolution provides enough information to prevent events of a certain magnitude while more minor events can be forecasted and dealt with closer to the present. Each OPI computation lasts around three hours at this temporal resolution, while the entire process takes around three days to be completed.

When overloads are forecasted, the model is enabled to, within limits, conduct 'non-costly' 'remedial action optimisation' (RAO). By alternating and trying out different grid topologies, the model aims to minimise forecasted overloads. Should the RAO be unsuccessful in reducing the overloading of grid elements, the planned outage is cancelled, and the overloads are prevented. However, what counts as an overload that requires prevention is not trivial. The OPI tool developer at TSCNET explained that to account for data uncertainties and minimise false positives, the overload threshold is set to a grid element loaded above 103% of its rated capacity for this forecast. Only above this threshold is the power grid, and in extension its connected customers, defined to be in 'danger' and prevention required.

The RSCs, like TSCNET, create the OPC and calculate the OPI forecast, yet they are not directly involved in preventing forecasted overloads or outage planning. Ultimately, it is the responsibility of the TSOs to act on the OPC/OPI results (European Commission 2017a). Yet, this process closes with results being reported to the TSOs and a 'weekly outage planning conference' (WOPT). While aggregating planned outages and forecasting potential overloads is important, the consideration of results by the TSOs it essential. In the WOPT conferences, TSCNET operational managers would share the results and invite operational planners from the TSO to comment on and discuss the results and possible solutions. Through sharing and occasional arguments about the results amongst the TSOs, the uncertainty of whether the forecasted overloads would be addressed and lead to prevention could also be reduced.

The outage planning coordination and incompatibility OPC/OPI is a process that, for a specific geographical extent, temporal horizon and resolution, aims to make scheduled outages and their incompatibility with grid security known. By aggregating the pan-European planned outages and regionally calculating whether the altered power flows will likely create overloads, planned outages' negative uncertain impacts become known and can be prevented. Being integrated between forecasts with longer (months, years) and shorter (daily, intraday) temporal horizons, OPC/OPI reduces uncertainty to a level that is safe enough for its temporal horizon.

5.4.2 CORE Flow-Based Market Coupling

Compared to the OPC/OPI forecasting process, the CORE flow-based market coupling (CORE FB MC) more indirectly secures the grid by supporting the electricity capacity and power markets. In the everyday, and since the European electricity sector liberalisation in the late 1990th, the electricity markets should primarily ensure the balance between demand and generation (European Commission 2019). For the electricity markets to operate, they need to know how much capacity they can trade and use to transport their purchased electricity. The CORE FB MCs' addresses this element of uncertainty: transmission capacity. Measured in megawatts (MW), it is the amount of electricity that can pass through a power line of a given size while respecting its operational limits. However, due to its market orientation, only those transmission lines tying bidding zones together (roughly equating to countries) are of interest. Through its mode of calculation as 'flow-based' this "capacity is calculated and allocated taking into account the meshed nature of the transmission network and all possible paths through which electricity is flowing in it" (European Commission 2017d: 13). This way of calculating the capacity forecast will optimise the power flows while respecting the networks limitations. These limitations will be explained further below.

With the addition of growing amounts of renewable generation outside of consumption regions and liberalised energy markets, the power flows between regions have increased (Übertragungsnetzbetreiber 2024, Bundesnetzagentur 2011). Knowing how much electricity can be transported across borders is essential for two reasons. First, without specifying the capacity limits of transmission lines and transformers, overloads are likely as the market aims to maximise cross-border power exchange. Overloaded grid elements could lead to escalating or cascading system failure and, ultimately, a blackout. Secondly, knowing and maximising the flow of electricity, which is increasingly provided by renewable generation, supports the goal of electricity decarbonisation. If transmission capacity is available, renewable generators, such as offshore wind, must not be curtailed to prevent overloads. This is particularly relevant for Germany, as the offshore and onshore wind generation is clustered along its northern and increasingly its eastern seaboard. The CORE FB MC forecast is, thus, securing life and lives in a duality. It helps to ensure the smooth supply of electricity while supporting climate change mitigation by helping to maximise the infeed of renewable generation.

The name of this forecast consists of three parts that specify where and how it is functioning. Its geographical extent lies over the 'core' capacity calculation region (Core CCR). As one of several CCRs, CORE spans over central Europe and includes 13 countries (see map in table 4, page 72) and 15 TSOs (4 in German) that coordinate their cross-border capacity calculation (ENTSO-E 2024a). It coordinates the transmission capacity by forecasting this capacity and providing it to coupled national energy markets, thus 'MC', market coupling. The CORE FB MC is part of a wider European Union effort to create a European-wide 'Single Day-ahead Coupling(ed)' (SDAC) electricity market (European Commission 2017d). In line with the (neo-)liberal principles underpinning the European Union's Clean Energy for all Europeans initiative (European Commission 2016a) this market coupling should increase trading efficiency, the utilisation of (green) generation and promote more effective competition (ENTSO-E 2024d). Furthermore, and similarly to the OPC/OPI forecast, the more considerable geographic extent over which the transmission capacity is calculated aids in gaining a more realistic picture of how the wide-area flows of electricity influence each other. Through a more accurate forecast of power flows and transmission capacity, the chance of surprises, thus the potential for escalating or cascading events in the present is reduced.

The CORE FB MC temporal horizon lies a day ahead (D-1) while the process already starts two days in advance (see Table 4), as its data acquisition requires time. In this timeframe, all relevant data is available or forecasted and precise and accurate enough to be used as the foundation for the transmission capacity calculation of this forecast and the electricity markets. With a temporal resolution of 24 timestamps, it cuts a day into one-hour-wide blocks for which the transmission capacity is calculated. Within these hourly blocks, the transmission capacity is assumed to be steady. However, in reality, it will not be steady. Yet, this temporal resolution is standard for day-ahead forecasts. It only aims to reduce uncertainty, not eradicate it. It aims to reduce uncertainty to within a level that is deemed by the TSOs to be safe enough for this particular temporal horizon. Remaining uncertainty then can either be further reduced by follow-up forecasts with a shorter (intraday) horizon and higher temporal resolution (15-minute intervals, for example) or contained by standardised security techniques, such as redispatch, discussed in the last chapter.

For the CORE FB MC, the element to be forecasted is the maximised cross-zonal transmission capacity. This metric aggregates the individual capacity of power lines connecting bidding zones, called tie-lines. It is a complicated calculation that takes hours to complete and is calculated through three intermediate steps feeding into the final calculation. Like the OPC/OPI, it is based on the 'common grid mode' (CGM) and forecasted aggregated generation and demand values called 'generator load shift keys' (GLSKs). To reduce the computing time and power required, the transmission capacity is forecasted selectively. It is only conducted over 'critical network elements and contingencies' (CNEC). These are those elements for which their calculated 'power transfer disruption factor' (PTDF) is above five percent. This means that if network elements are almost not affected directly or indirectly by the forecasted power flows, they are ignored. What cannot be ignored and is factored into the calculation process is the 'long-term allocated capacity' (LTA). This capacity has already been sold in advance and now becomes a limiting factor.

To minimise the potential for overloads and a subsequent need for costly balancing in the present while maximising the availability of transmission capacity, a 'non-costly remedial action' (NRAO) is conducted, similarly to the OPC/OPI proceed. As the calculation of CORE is based on the "predictive estimations" (Schönheit et al. 2021: 5) available two days before COREs delivery date, a 'flow reliability margin' (FRM) is to prevent the accidental overloading of the transmission lines due to data uncertainties. Based on a stochastic analysis of past forecasted and observed power flows and in addition to a pre-defined 'risk-level' the FRM is probabilistically calculated as a dynamic value reflecting the expected uncertainty for the day ahead (ENTSO-E 2017). The FRM is subtracted not from a fixed value but from the 'thermal rating' of power lines. This fact recognises that the transmission capacity of a power line is dependent on its temperature, partly depending on the ambient temperatures and wind speeds along its path (Karimi et al. 2018). Rather than subtracting a fixed reliability margin from the overall transmission line capacity, the reliance on 'thermal ratings' allows for – within the temporal horizon and resolution of CORE – a more dynamic and potentially higher overall transmission capacity. The 'Remaining Available Margin' (RAM) is the capacity that remains after these considerations. It is the output value provided to the capacity market via online market platforms.

CORE FB MC is a forecast that secures the power grid indirectly by providing the market with values for the transmission capacity between bidding zones. This level of security provided is not static and depends on and changes with the quality and uncertainties of the input data and forecasts. Within the

boundaries defined by the temporal resolution (hourly timestamps), the capacity values provided are dynamic and can change, as are the levels of security provided. The 'flow reliability margin' allows for adaptation to a changing environment and varying levels of uncertainty by increasing or decreasing its margin to avoid overloads. Maximising the cross-bidding zone transmission capacity allows the optimum amount of electricity flow, supporting the infeed of renewable generation, thus reducing the electricity-mixes carbon dioxide footprint. Security for the CORE FB MC is concerned with and indirectly supports power grid security and the European Energy Union's ability to achieve its decarbonisation targets (European Commission 2023, 2016a, 2015). This forecast is securing a particular snapshot of a future and reducing uncertainty to within its temporal resolution and forecasted elements. A residual uncertainty about the potential exceedance of the transmission capacity remains. In the following forecast, this residual uncertainty is further addressed.

5.4.3 Day Ahead Congestion Forecast (DACF)

The previously discussed OPC/OPI and CORE FB MC forecasts have indirectly addressed the potential of overloads as part of their processes to identify outage incompatibilities and safely maximise transmission capacity. This section will engage with the 'day-ahead congestion forecast (DACF)' as TSCNET's most direct contribution to power grid security. Its element of uncertainty addresses grid congestion, which holds the potential to cause overloads. The 15 TSOs who are customers of TSCNET rely on the DACF outputs as they allow them to make known where and when grid congestion might occur and cause overloads, thus opening a window of opportunity to prevent it. While addressing the same temporal horizon (day-ahead) as CORE (see Table 5), it is a forecast calculated after the closure of electricity day-ahead markets. This means that the data availability for the DACF forecast is optimal as it does not, like CORE, rely on older forecasts. Furthermore, as the markets have closed, the remaining uncertainty in the input data is only the deviation between expected and actual power flows for tomorrow.

Like traffic on streets, the power grid is regularly plagued by congestion. Depending on its spatio-temporal scale, this congestion is, at best, a nuisance and, at worst, a significant risk to traffic/electricity flow and the power grid's security as it can cause overloads. Grid congestion originates from a combination of a limited 'safe' power line (road) capacity, as forecasted by CORE, the amount of electrical flow (traffic) trying to pass through it, construction sites (planned outages) that further limit flow and the behaviour of this electricity flow (drivers) in relation to environmental conditions and grid topology. Although the TSOs possess a suite of tools to manage acute congestion (for example, redispatch), preventing it is most economical while it avoids tapping into the grid's limited security reserves.

The grid congestion calculated by DACF is forecasted for TSCNETs customer TSO control zones and can be further traced to individual grid assets, such as transmission lines or transformers. Like with the other forecasts, the unique position of TSCNET as a regional security coordinator allows them to profit from the large geographical extent over which the forecast is calculated. This promises to represent actual power flows more accurately, thus reducing uncertainty between forecasted future and present and increasing situational awareness for the TSOs. As distant congestions can affect control zones far from their occurrence, this situational awareness is important for TSOs and goes beyond their bilateral coordination.

For the DACF, two metrics specify direct and indirect loading of network elements, possible congestion, and overloads. These are called 'load-flow' (LF) and 'contingency failure' (CF). While the 'load-flow' specifies a percentage of utilisation of a control zone and individual grid elements, 'contingency failures' concern the N-1 principal. CFs are also assessed through a percentage of (over) loading. The N-1 design and operational principal state that the power grid "elements remaining in operation […] after the occurrence of a contingency are capable of accommodating the new operational situation without violating operational security limits" (European Commission 2017a: 5). Contingency failures are essential to consider as they specify if, in a grid that is highly loaded but not overloaded, a failure of any grid element could cause a secondary escalating or cascading system failure towards a blackout. Without this analysis, there would be a false sense of security as the potential of escalating or cascading system failure in a highly loaded grid would remain undetected and could not be prevented.

The DACF simulates the load-flows on the modelled power grid and aims to reduce the uncertainty about when and where grid congestion and overloading might occur for a temporal resolution of 24 timestamps for hourly values. As for CORE, this temporal resolution is sufficient for the forecasted temporal horizon and is further reduced and secured by following forecasts and standardised security techniques, such as redispatch. The DACF is calculated using the 'common grid model' (CGM) and the net in- and electricity exports for each TSOs control zone. These values for the power exchange between control zones come from the electricity markets and are, not least, based on the transmission capacity provided by CORE. Between multiple model calculations (runs) and based on the forecast's intermediate results, the TSOs can calculate and optimise their internal power flows using their own tools. These internal results are then used to adapt TSCNETs model before the next run. This iterative process is repeated until the pre-scheduled 'daily outage planning conference', and if needed afterwards, until 24:00. At the end of the day, the day-ahead- seamlessly transitions into the fully automated 'intraday congestion forecast' (IDCF).

Through the iteration between forecasts and the model-improvement phase, the TSOs aim to reduce the forecasted load-flow and contingency violations via a mix of their own simulations and trial and error. Multiple iterative calculations were possible during the attended shifts as individual forecasting runs only lasted 10 to 15 minutes. The power flows in the electricity network are complex, and relationships between grid elements and variables are not always immediately recognisable. In practice and on multiple occasions during my shifts at TSCNET, this led to intended improvements, worsening the intermediate forecasts. Seemingly counterintuitively, these initial moments of 'failure' led to good results and prevented overloads in the following forecasting runs. It allowed the TSO to test and calibrate their tools in a modelled environment without risking power grid security.

For the DACF, what constitutes a threat to power grid security, namely grid congestion and overloading requiring prevention, is process-specific. Like in CORE, an (over) loading above 103% is recognised as 'overload' for standard grid elements. For tie-lines, it is 120%. These thresholds compensate for remaining data and modelling uncertainties. The TSOs can tolerate these forecasted overload levels as follow-on forecasts in the 'intraday' further reduce and secure electricity flow while standardised security techniques, such as remedial actions, are on standby. However, TSOs can also officially or unofficially declare a grid element critical to keep its forecasted overloads below a freely selected threshold. The German TSO Amprion, for example, an operational manager at TSCNET

explained during one of our shifts, is trying to limit the forecasted loading of its particularly important tie-line Vigy (France) – Ensdorf (Germany) to below 100% (Fieldnotes 080921).

While a daily and reoccurring forecasting process, the DACF requires attention and supervision by TSCNET OMs to function as a security technique. It involves supervision as the forecasting process is relatively sensible concerning the available data and quality issues. If data is missing or corrupted, the forecast might substitute this data, increasing its forecasting uncertainty. Thus, OMs would regularly inform TSOs about these issues or, if necessary, try fixing them themselves. During one shift, an OM manually corrected individual hourly '.txt' files. Ordered after the previously discussed legacy UCTE-data exchange format (ENTSO-E 2015), the numerical equivalents of the weekdays (4=Thursday, 5=Friday) were simply confused.

The DACF only becomes a preventative security technique for the power grid by combining its forecasted congestion and overloads with the expertise of the operators at TSOs and OMs at TSCNET. While the forecast delivers numerical values as its load-flow and contingency failures, these outputs of potential congestion require further interpretation and judgment. While TSCNET and the TSOs have agreed upon overload thresholds, the meaning of 'overloaded' changes in different circumstances. On a calm day with low grid traffic, the grid has enough margins to accommodate some overloads. If, however, as during my time at TSCNET, autumn storms with high expected wind speeds, thus wind generation and possible powerline failures are forecasted, the TSOs might be more cautious and more eager to reduce the forecasted overloads as best as possible. Therefore, like in OPC/OPI, the TSOs and TSCNET convene each evening to discuss the forecasted overloads in a 'daily outage planning conference' (DOPT). TSCNET OMs share the results and overloads, invite the TSOs to comment, and share bilateral or multilateral agreements to reduce specific overloads. A shared situational awareness is formed, reducing the likelihood of the TSOs being surprised by unexpected overloads, enabling them to jointly prevent forecasted overloads.

5.5 Conclusion

In the previous chapter, standardisation helped to secure the grid pre-emptively through an imaginary mode of backcasting. This chapter contrasted this with the calculatory mode of forecasting, which aims to secure the power grid through prevention. Before engaging with the forecast and due to its prominence in the literature on 'smart' grids (Bulkeley et al. 2016b, 2014, Luque-Ayala & Marvin 2020, Kitchin 2019, de Lange 2018a) and 'real-time' as a form of nowcasting and potential forecasting rival was addressed. In contrast to the preventative technique of forecasting, 'smart' and 'real-time' narratives propose the reactive management of increasing volatility through and with uncertainty in a perpetual present (Luque-Ayala & Marvin 2020, Kitchin 2019, de Lange 2018a). Rather than being novel and 'smart', 'real-time' in the current German transmission grid was shown to primarily rely on standardisation to secure against the potential threat from lightning strikes, enable frequency control and against the potential of overloaded power lines through redispatch. 'Real-time' in these examples extended from milliseconds to an hour, from the instantaneous to the close-to 'real-time', bordering the boundary between present and future.

In contrast to the idea of nowcasting and the real-time management of the power grid, forecasting was then positioned as a security technique that operates through a knowable, predictable future. From a historical perspective, the forecast was identified as an 'old' rather than a novel security technique. In Hughes's (1983) historical descriptions of the power grid, anticipation and calculatory forecasts helped to balance demand and generation while remaining within the physical limits of the grid. The importance of the forecast was described to have increased with the (neo-)liberalisation of the power industry in the (late) 1990th as the integrated monopolies of power generation and transmission were broken apart. The forecast was then introduced as a security technique that secures by reducing uncertainty about what is emerging, thus opening a window of opportunity to prevent what is emerging from escalating or cascading. A multiplicity of forecasts exists within the grid that span from close to 'real-time' to years ahead while operating at different scales. Each forecast identifies, articulates, and thus creates (Campbell 1998a) a potentially dangerous future and an object of prevention. They reduce uncertainty to within' safe' limits for a snapshot of the future and a specific metric. An excess of 'event' (Anderson & Gordon 2017) is prevented from exceeding the presents standardised coping capacity (reserve power, for example).

While slightly differing in their temporal horizon, resolution, and geographical extent, each exemplary forecast presented here targeted a unique element of uncertainty (planned outages, transmission capacities and overloads). While these were unique, they were all indirectly or directly related to the common problem of overloads. While a momentaneous overload might not be a significant issue, it can be the straw that breaks the power grid's back, causing a blackout.

The OPC/OPI process and forecast coordinated planned outages and, through compiling them, enabled the forecasting of potential overloads. It is the forecast with the greatest distance to the present and the 'roughest' temporal resolution of three timestamps per day and, subsequently, 21 per week. While uncertainty remains, the forecasts make outage incompatibilities known for their horizon and resolution. The CORE FB MC and the DACF process share the same horizon of a day ahead and resolution of 24 timestamps per day. They differ in their element of uncertainty (transmission capacity and primary/secondary overloads) and the aim of the forecast. While in DACF, the intention is to prevent overloading directly in CORE, the goal is to forecast transmission capacity as an input variable for the capacity market. They all have in common that through the unique position of the

RSC, TSCNET, these forecasts provide the TSOs with a situational awareness that they individually would lack. Furthermore, by sharing and discussing the forecasted results with the TSOs in various video conferences, coordination among the TSOs can be improved, and misunderstandings and misalignments become preventable.

Additionally, the forecasts discussed share that they are embedded in, preceded and followed by other, additional forecasts with longer and shorter temporal horizons and greater and lesser resolutions. The requirement for the reduction of uncertainty increases closer to the present until standardised processes, such as the reserve power activation, can contain the residual uncertainty. Starting the process of planned outage coordination, for example, a year in advance, allows TSOs to coordinate and plan together, reducing uncertainty and the potential for overloads. Forecasting for the day ahead or the intra-day minimises the chance of an unforeseen event escalating or cascading into a blackout. Data reliability and availability increase closer to the present, and more accurate and precise forecasts maximise the TSO's ability to prevent. The need to rely on pre-emption and standardised security techniques can be minimised through these forecasts. As a security technique, forecasts do not operate in isolation but rather in layers of various temporal horizons and resolutions.

This chapter contributes to Critical Security Studies by demonstrating how forecasting functions as a security technique that renders uncertainty actionable and enables prevention. In doing so, it advances a biopolitical understanding of security by tracing how threats to circulations are made governable through calculative practices (Foucault 2007, 2008). Unlike discursive constructions of threats (Campbell 1998b) through, for example, standards and standardisation, forecasts do not imagine catastrophe. Instead, they make an emerging future known through probabilities, thus producing futures that can be acted upon in the present and, if necessary, prevented. (Ewald 1991, Adam & Groves 2007). This contributes to debates in Critical Security Studies on the infrastructural and epistemic enactment of security, by showing how forecasting stabilises circulation through technopolitical routines embedded in infrastructures (Amoore & De Goede 2008, Dillon 2007). Forecasting exemplifies how security emerges not only through discourse but through the entanglement of infrastructure, data flows, and technopolitical routines (Barry 2001, Neal 2019). By examining forecasting as an everyday form of grid governance, the chapter extends CSS work on mundane security practices and demonstrates how infrastructures are configured to manage uncertainties differently.

The forecast itself, however, only gains its meaning in relation to the elements it makes known and through the assessment and judgment of its computations by well-trained and experienced operators and OMs. Their training as a third security technique for the power grid will be addressed in the next chapter.

6. Training Between the Everyday and Catastrophe

6.1 Introduction

This chapter examines training as a distinct security technique that manages uncertainty in the operation of the German transmission grid. Building on the analytical framework introduced in Chapter 2, this chapter examines how training enhances power grid security by enabling operators and operational managers to anticipate, interpret, and respond to uncertainty. Unlike standards and standardisation and forecasting, which aim to contain or reduce specific uncertainties, training equips actors to manage residual uncertainty, shift between modes of knowing, and maintain vigilance for events that defy procedural containment. In doing so, the chapter contributes to ongoing debates in Critical Security Studies by demonstrating how security is enacted not only through technical control but also through the cultivation of embodied expertise and adaptive capacity within infrastructural systems**.**

Training in this chapter will be presented as a security technique for the power grid, as it manages uncertainty and helps secure against an uncertain future. The future that training engages is inherently uncertain and through different ways training aims to foster the management of uncertainty. Training secures the power grid in three ways. Firstly, through training, the TSO and RSC TSCNET personnel become proficient in the tools used for everyday and exceptional grid operation. Training enables them to pre-empt, prevent, know, interpret, and use standards and forecasts while proficiently using their software tools and backups. Through training they learn what to do when and how in a specific context. This enables grid operation and aims to reduce (human) error. Secondly, training is supposed to build experience as a distinct form of knowing required to react to emerging situations and teach to anticipate, remain vigilant, and be precautious. Specifically, for exceptional grid states, training is to prepare the TSOs operators and RSC/TSCNET OMs to operate beyond what is standardised or forecasted and in conditions of progressing uncertainty. Training fosters a capacity within the operators and OMs to switch between different forms of knowing and securing as the situation requires. Layered and combined, standards and forecasts can contain and reduce uncertainty for most of the everyday and the exceptional. However, this might not be sufficient to secure the grid in extreme situations that could lead to or be a blacked-out grid. In situations that exceed the level of eventfulness addressed by existing standards and forecasts, the required management, mitigation, and recovery capabilities are achieved through training. Thirdly, as the moment and form of (potential) failure is unknown, training is needed to sharpen the operator's and OM's attentiveness to potential failure and foster precaution and vigilance. Furthermore, as the exact boundary between the everyday and the exceptional is transparent, the operators try to maximise their 'distance' from it.

In engaging with how training operates as a biopolitical security technique that manages uncertainty in everyday power grid operation this chapter contributes to Critical Security Studies (CSS). Building on recent debates in CSS that foreground mundane (Nyman 2021, Anderson & Gordon 2017), anticipatory (Adey & Anderson 2012, Aradau & van Munster 2011, 2012), and infrastructural (Adey et al. 2015, Collier & Lakoff 2015) practices of security, this chapter examines how training enables operators and coordinators to manage and navigate uncertainty. Training does not eliminate uncertainty, but rather cultivates vigilance, improvisation, and expertise. Training engages with uncertainty not through discursive securitisation or sovereign intervention, but through the development of operational capacities that allow for the flexible usage of different security techniques, depending on the prevailing uncertainty. In doing so, it advances the thesis's broader

argument that security in critical infrastructures is enacted through the dispersed and recursive labour of infrastructural actors. The chapter further extends the biopolitical framing of security by showing how life is secured not directly, but via the continuous reproduction of expertise and readiness among those tasked with maintaining the infrastructure that sustains life. As such, training does not aim to neutralise a specific threat but cultivates the capacity to manage a spectrum of uncertainties, including those that exceed standardised or forecasted scenarios. It sustains grid security by enabling operators to act effectively under conditions of volatility, through experience, precaution, and vigilance. Training thus extends the anticipatory logic of infrastructural security beyond calculable or imaginable threats, equipping actors to intervene when uncertainty resists containment or reduction.

Training requires a "special group of professionals" that, through their "commitment and dedication", steer the electricity network as "reliability professionals", write Roe & Schulman (2008: 6). In the style of Roe and Schulman and through their training, I propose that TSO operators and TSCNET OMs become 'uncertainty managers'. As uncertainty managers, the TSCNET operators observed throughout my ethnography and the balancing operator at TransnetBW disproportionately impacted the secure flow of electricity. They developed and applied standards, used, debugged, and switched to backup tools for their forecasts. They trained for the exceptional and displayed vigilance and precaution as they engaged and openly discussed minor events or failures. Through training, the operators and OMs ensure and are proficient in everyday operations while preparing for exceptional situations and remaining vigilant and precautious about the possibility of failures. In exceptional situations, when uncertainty bursts out, and, for example, a re-start and recovery of the grid is required after a blackout, it is the well-trained operators and OMs that are able to perform the "complex adaptive governance" (Carnes 2011: 4) required in these power grid states. In exceptional and extreme situations, they are prepared to sift their mode of operations, to operate through and with uncertainty.

While standards and forecasts engage a particular form of uncertainty, 'safe uncertainty' and 'known unknowns', as discussed in Chapter 3, training acts as a hybrid. Depending on its intent and form, training supports and aims to secure against uncertainty throughout its spectrum. While standards, standardisation, and forecasting contain and reduce uncertainty and thus are necessary to operate the grid securely, they alone are insufficient. Their effort to contain and reduce uncertainty still leaves behind residual uncertainty. By this, I mean that due to the complexity of this infrastructure, surprise as a yet unknown future always remains possible (Kavalski 2009). Dillon & Reid (2009: 85) might add that this residual uncertainty also stems from the "continuous unfolding potential" of life itself. In any case, training particularly addresses residual uncertainty as it equips the operators and OMs to manage uncertainties and perform well in complex and volatile environments. Training emerges as a security technique distinct from, yet related to, standardisation and forecasting by enabling and preparing operators and OMs to secure against and manage the grid's volatility, i.e., uncertainty.

After highlighting a void in the existing literature on training as a security technique, the first section focuses on how training comes to matter. It conceptualises training and draws from highly reliable organisation/system literature to position training more explicitly as a security technique. Training functions as a security technique as it manages uncertainty by training operators and OMs to use their tools proficiently, reducing (human) error and teaching them to rely on their experience when necessary. Training in this chapter is a process as well as an outcome of relating and managing knowledge, expectation, and thus uncertainty. To learn is to know, to expect, and to be certain while

simultaneously creating an “awareness of the limits of expertise” (Giddens 1990: 125, Endsley 2006). Training static- and dynamically mediates the forms of knowing while framing how knowledge is created, maintained, and comes to matter. It relies on pre-existing knowledge received through formal education while imprinted by the individual experience and character. What has been learned through training becomes the backdrop through which the operators and OMs relate and make sense of an emerging present and an anticipated future. It enables them to become vigilant, be cautious, detect change, and, in doing so, prepare them, if required, to intervene in emergent events to stop them from escalating or cascading.

Building on this conceptualisation of training, in the second and third sections, I present empirical examples, first of training for and in the everyday and secondly for the exceptional. They draw primarily on my experience at the regional security coordinator (RSC) TSCNET and from various engagements with the German TSOs. Training here differs in its reliance on codified and experiential knowledge. The everyday training prepares the OM and operator to correctly deploy the code, standards, and procedures while incubating their ability to prevail in the exceptional. It prepares them as it trains and tests for comprehension rather than encyclopaedic knowledge, for wariness and attentiveness for the (potential of) failure, and the boundaries of one’s knowledge and capabilities. Faced with (the possibility of) an event becoming exceptional, training provides the tools for operators and OM to transition from a primary reliance on codified to experiential knowledge and improvisation. Furthermore, a new group of actors, ‘contingency managers’, appear in the exceptional, who relate to and negotiate the varying authority and sometimes conflicting vision of specific continuity regulations and standards. In conclusion, I argue that training, besides standards and standardisation as well as forecasting, is an important power grid security technique. Differing from the latter two, it functions by facilitating uncertainty management through formal knowledge and relying on experience and experiential knowledge.

6.2 How Training Comes to Matter

6.2.1 Training in the Literature

When consulting the existing geographic and infrastructural literature, there exists a lack of writing on training as a specific security technique. Although a vast body of geographical literature exists around knowledge production (Haraway 2016, Rose 1997, Foucault 1991) and its management in a corporate context (Cohendet & Amin 2004, Hinchliffe 2000), training is rarely the focus. This remains the case despite non-representational thinking becoming established and emphasising the value of experience, practice and doing (Anderson & Harrison 2011, Thrift 1996, 2007).

Nevertheless, a niche of a particular form of training exists in the literature on emergency preparedness exercises (Anderson & Adey 2011, Anderson 2010b, Collier 2008, Lakoff 2007, 2008, Aradau & Van Munster 2007). These position emergency preparedness exercises in the aftermath of and as a response to 9/11 and exceptional and extreme events. They address unpredictable events via preparedness and through training and developing the expertise of emergency managers. As a particular training technique, exercises rely on and promote affectual and possibilistic rather than calculatory probabilistic techniques to engage with an uncertain future (Anderson & Adey 2011, Collier 2008). While the experience gained in exercises might not primarily apply to the everyday, it provides a reference framework for normal incidents and exceptional situations. For the idea of training as a security technique, the ability of the TSO operators and TSCNET OMs to foster their experience is essential. When events reduce or compromise the forecasts or standards' ability to reduce and contain uncertainty, the operators and OMs must remain able to secure the grid and find creative solutions.

Training does appear more frequently in, for example, business literature on management training and human resource development (Queiro 2021, Elnaga & Imran 2013, Salas et al. 2012). In this literature, the link between the welldoing of a company and its labour force has been well-established (Kraiger 2003, Sánchez et al. 2003). However, this literature does not explicitly concern and occasionally even opposes ‘security’ or reliability of an organisation or its operation (Weick & Sutcliffe 2015). Rather, training here is discussed and related to requirements for the maximisation of employee performance or efficiencies of interrelated proxies such as sales, perception, or credibility while minimising complaints or wastage (Walters & Rodriguez 2017). Nevertheless, training as a general security technique for and in the everyday and the exceptional remains without much attention.

A set of interdisciplinary studies concerned with the engineering, organisational design, and management of 'High-Reliability Organizations'(HRO) exists and indirectly relates to training for security. As a term originally coined by Karlene Roberts, Gene Rochlin and Todd LaPorte (Rochlin et al. 1987), this literature tries to answer why and how some organisations, like those operating critical infrastructures, such as the power grid or nuclear power plants, can achieve high operational reliability and minimise their (catastrophic) failures. The general importance of ‘training’ as a distinct security technique is recognised here, yet it is not the primary concern. For example, Roe & Schulman (2008: 6) analysed the California energy crisis. While addressing broader structural concerns of organisations and the California energy market, they also attribute the "reliability professional", a well-trained and experienced operator of the lower middle management, a disproportionate contribution to the system's overall reliability. In paying attention to the design of HRO, this literature points towards not only their unique structural features (Schulman 2004, Sagan 1993) but also how they "think and act

differently" (Weick & Sutcliffe 2007: X). Training is, however, only indirectly present through a focus on organisational culture for high reliability (Weick 1987).

In writing about “managing the unexpected” in highly reliable organisations, Weick & Sutcliffe (2007, 2015) advance five collective principles of how the organisational structure and performance of the employees of these organisations matter. The first three, a “preoccupation with failure”, a “reluctance to simplify”, and a “sensitivity to operations”, are “anticipatory principles” (Weick & Sutcliffe 2007: 43 ff.). They highlight that much of the ability of HROs, such as TSOs, depends not on error-free operation but on their way of constructively engaging with (the potential for) failure, including the management of expectations. Principals four, a “commitment to resilience”, and five, “deference to expertise” are principles of containment (Weick & Sutcliffe 2007: 65 ff.). They are positioned as responses to emergent events, halt their progression, and recover from any disruption quickly. At the core of these principles of organisational culture lies the idea that “reliability is a dynamic nonevent” that requires curating ongoing adaptability and cultivating resilience to sustain continuity in an environment of constant potential danger (Weick & Sutcliffe 2015: 17). It is mainly through training that the organisational cultures of HROs, such as the TSOs and TSCNET, are shaped, and their ways of thinking, knowing, and acting are aligned to uphold operational security.

6.2.2 Training as a Security Technique

How training matters for power grid security will be explored in this subsection, along the following two main questions: Firstly, what is training, and secondly, how does it secure? Training as a security technique, and supported by my empirics, will be shown to be multiple. It engages TSO operators and TSCNET operational managers (OMs) through various career stages while building different sets of knowledge that mediate the encounter with uncertainty differently. As a security technique, training secures by enabling and preparing the operators and OMs to pre-empt and prevent, building experience and preparing them to shift between operational modes, and fostering vigilance and precaution.

Training is multiple. It concerns the initial and continued development of operators and OMs. In these two distinct temporalities, training relies on and fosters different forms of knowledge. Initially, it equips the novice operator or OM with the fundamental ability to use job-specific tools and understand and follow the organisation-specific protocols. At the regional security operator (RSC), TSCENT, in the beginning of my ethnography, I experienced this initial training as a hybrid. Together, with a new novice OM, I was (partly) put through their initial training as well. Initial training at TSCENT relied on the formal, codified academic education provided by institutions such as universities. In contrast, the initial training amended it to be apprenticeship-like, relying on and building experiential knowledge. The OM that started with me possessed a master’s degree in power engineering. This was proof of an institutionalised education at a university that developed formal and codified knowledge about the power grid's composition, operations, and underlying physics. While a pre-requirement for the job as operational manager (OM) and beneficial for understanding the basics of work at TSCNET, that OM was not yet trained or qualified for their specific services and lacked experience in them.

As part of the initial apprenticeship-like training at TSCNET, we were both assigned a mentor and learned to operate their individual services (like the forecasts detailed in the last chapter) in a duality. While studying TSCNET's individual services' formal documentation and process descriptions, we

shadowed experienced OMs during their shifts. The focus of this initial training was first to study and acquire the formal knowledge about processes required and then apply these during operations, thus building experience and preparing for solo operations.

Throughout the three-month initial training process, the OM and I gained experience and became increasingly independent and confident in operating the various services at TSCNET. A final qualification examination was necessary to become licenced for solo operation. However, I was not required to take this examination as I was only a researcher. While this examination was performed at TSCNET by senior OMs and their head of operation, the requirement for this pass-or-fail examination is part of the European standard operational guidelines. "[…] Operational training and certification are required in order to guarantee that […] employees […] are skilled and well trained […] to operate the transmission system in a secure way during all operational situations" (European Commission 2017a: 2). The TSOs head of system restoration and security interviewed by me and the balancing operator I joined for a control room shift highlighted similar forms of initial training processes for their TSOs. Yet, the end of the initial training is only the beginning of the continued training of the TSO operators and TSCNET OMs.

As a periodic and continued process, training resharpens and further develops skills while building individual and collective experience. The continued training, as I experienced it, is directed at sustaining the operator's and OM's qualifications while providing advanced education and training. It aims to maintain their qualification as they must periodically re-qualify and participate in "a continuous training programme" (European Commission 2017a: 46). Furthermore, they should prepare for operations beyond the everyday through continued advanced education and training. For the operators at a German TSO, for example, the interviewed head of system restoration specified the yearly interval for exercises of power grid restoration and the blackstart. Other training, according to the system balancer I shadowed in TransnetBWs control room, is carried out quarterly. During my ethnography at TSCNET, I took part in continued trainings for specific services or general awareness building. These were internal seminars and workshops, occasionally also for TSO system planners. Generally, they were concerned with TSCNET forecasting tools, introductions to new processes, or updating existing ones. Additionally, and as mandated by the SO GL, soft skills, such as language proficiency (the contact language between RSCs and TSOs is English), or "behavioural skills with particular focus on stress management, human acting in critical situations, responsibility and motivation skills" (European Commission 2017a: 45) should also be trained. At TSCNET, this, for example, included a multi-tire cyber security course in which I participated.

Two classes of knowledge coexist in the initial and continued forms of training and mediate the operator's and OMs encounters with uncertainty differently. Codified knowledge is formalised, written down knowledge gained through institutionalised study. For the position of operator or OM, codified knowledge is a prerequisite. It is the knowledge of the profession or trade gained primarily through university education. At TSCNET, the codified organisational knowledge supplements and builds upon this foundation. Especially at the start of the initial training, learning from and about legislation, process methodologies, and handbooks lays the foundation for building experience. As codified knowledge is standardised, it provides the operators and OMs with certainty about what to do when and in what ways. Codified knowledge contains uncertainty about what needs to be done, when, and how.

Experiential knowledge of the individual and collective originates from ‘doing’ and (anecdotal) remembering, including from mistakes and failure. It supplements and builds upon codified knowledge. The anecdote most frequently appearing throughout my fieldwork was the Emsland Case, which became this thesis preface. It forms part of the collective memory of the professionals in the transmission grid. It was used as an example in four out of my five interviews, serves as the foundational ‘myth’ of TSCNET and was the impetus for the German parliament to request the “What happens during a blackout” Petermann et al. (2011b) report.

For the novice OM and myself starting at TSCNET, the more senior OMs' experience helped navigate and make sense of the module descriptions and handbook instructions about TSCNETS' different services and forecasts. Learning from them meant not having to make their mistakes while growing a stockpile of personal experience.

Experiential knowledge also standardises and provides a certain reliability of expectation. Expectations about a future are formed through the reference framework of past experiences. These expectations then inform judgment and action in the present. In the everyday and during my shifts at TSCNET, the experience of the operators would fill in minor uncertainties left unanswered by the process handbook. Through growing experience, the novice OM and I, learned what buttons to click where and in what sequence. Furthermore, we gained a sense of the correspondence styles of the TSOs that participated in the regular forecasting process supporting video conferences.

Training at TSCNET and the TSOs, as I experienced it, was sequenced. It is the initial learning process to become qualified for grid operations, while further continued training is to develop the operator's and OMs' skills and grow their experience. But how does training secure? Training secures, I propose, by managing uncertainties. Training does not (like standards and forecasts) engage with a specific future that might or is emerging but manages a multiplicity of possible but inherently uncertain futures. It acknowledges the strengths and weaknesses of standards, standardisation and forecasting to secure against specific futures and enables and prepares the operators and OMs to deploy them. Yet, it also assumes the possibility of their failure to contain or reduce uncertainty and prepares the operators and OMs for it. Preparedness generally does not aim at stopping a future event from happening but “prepares for its aftermath” for mitigating or halting its effects on circulations (such as electricity) (Anderson 2010a: 791, Lakoff 2007).

Three ways of how training secures were identified through the engagement with the initial and continued training. Firstly, training secures in and for the everyday by enabling and preparing the operators and OMs to - and how to - use the grid's pre-emptive and preventative security techniques, namely standards, standardisation, and forecasting. Through the initial and continued training, they become equipped with the organisational and process-specific codified and experiential knowledge that allows them to securely operate the grid in the everyday. It lays the foundation for them to contain and reduce uncertainty effectively. Without their initial training, operators and OMs would be unable and not legally allowed to operate at TSOs or TSCNET. Without their continued training, they would lose sight of process updates, new developments and miss their re-qualification requirements. After the initial three-month training period at TSCNET, the OM, I started with felt comfortable during his shifts and passed his examination with flying colours. Furthermore, the continued training at TSCNET had its own rhythm. It was a requirement, as during my ethnography, multiple new services, tools, and data formats, such as CORE FB MC forecasts or the Common Grid Model Exchange Standard (CGMES), were introduced or reached development milestones.

Secondly, training secures by providing the operators and OMs with opportunities to (securely) build their experience while training them on when and how to rely on their experiential knowledge. Experiential and codified knowledge relate to distinct operational environments and conditions in which they dominate. It is then the operator's and OM's job, through their training, to become able to switch between these as required and creatively re-combine existing knowledges to tackle a novel situation with new uncertainties. To rely on experience, if only to supplement codified knowledge, is required as what is standardised or forecasted does not perfectly contain or reduce uncertainty. Residual uncertainty about processes or the interpretation of results remains, requiring experience to be managed. Furthermore, the possibility of events emerging outside the detection range (scope) of forecasts or lying beyond imagined futures informing standards and standardisation remains.

Experiential knowledge in the everyday is not replacing codified knowledge but amends it. Learning through experience was necessary at TSCNET as the codified knowledge of the individual services described in their handbook and model descriptions was procedural, explaining sequences of actions and overall goals, but not down to the exact 'click-this-button-level'. In principle, this is unproblematic as it avoids the reflexive risk of standardising too much and being too detailed, thus curtailing flexibility (Hanseth et al. 2006). Yet, it requires future operators and OMS to rely on and build experiential knowledge to fill the remaining gaps. To securely build experience during the initial training and for the everyday, the novice OMs at TSCNET were guided by a mentor. The initial training at TSCNET was apprenticeship-like and on-the-job as, at least for TSCNET, no simulators or training agencies were available for this job. The mentor's role is to aid in building the novice OMs' experience, ensuring the on-the-job training on live tools is conducted securely. This meant that the sequences of actions needed for forecasts, like DACF, were talked over before the novice OM was allowed to perform them. By relying on the expertise of their mentors', the mistakes made in this exercise did not negatively influence the outcome of the actual forecasts and could be corrected. Over time and with growing experience, the novice OM would be allowed to primarily perform the processes under the watchful eyes of the mentor, requiring less intervention and having fewer questions.

The reliance on experiential knowledge increased for events that require a deviation from 'normal' everyday operation. As discussed in the past two chapters, everyday operations are highly standardised to contain uncertainty and pre-empt the possibility of being unable to respond appropriately. Furthermore, forecasts 'make known' what is emerging and usually prevent the standardised security from being exceeded or overwhelmed. Yet, if what is emerging and forecasted does not fit into the imagined, standardised categories, the experience must manage this outburst of uncertainty, this excess of eventfulness. As the power to forecast or pre-define what should be done decreases from 'normal incidents' to exceptional situations, this excess uncertainty requires different levels of experiential knowledge.

While the initial training at TSCNET primarily focuses on the novice OMs' ability to operate in the everyday, it already includes preparations for situations that require a deviation from 'normal' operation. Accompanying the learning about and training on the individual processes were also always verbal exercises or real-life applications of backup processes. Besides talking through, for example, the next steps of the DACF, the mentors would also ask, 'What do you do if this process fails in XY way…'. While these contingency scenarios were also part of the operational handbook and TSCNET's Matura question catalogue that I received at the beginning of my ethnography, they were, in part, formulated more generally and abstractly. To combat the uncertainty about what to do, they required

the OMs to rely on their experience to diagnose the problem and find appropriate and timely solutions. 'Normal incidents', as backup procedures, were part of the initial training process I experienced at TSCNET. Exceptional events, such as a blackout, were not.

In the continued training of the TSOs, exceptional events, such as blackouts or the continental Europe synchronous area Separation on 08 January 2021 (ENTSO-E 2021b), are trained for. In contrast to TSCNET, they are directly involved and responsible for operating the grid and upholding supply security. Besides in-house training at the German TSOs, an "independent training and service centre for power system control" is regularly used for simulator-supported trainings of grid state beyond the everyday (DUtrain 2022). The importance of these trainings for building experience was highlighted by the balancing operator I shadowed in TransnetBWs control room, who pointed out "that under the strain of these situations, you do things that you usually wouldn't have done" (Fieldnotes 281021). For that operator, gaining experience was necessary to manage the residual uncertainty about the codified procedures for exceptional grid states and reduce the uncertainty about how one would react under the stress and pressure of these situations.

Thirdly, training secures the everyday flow of electricity by fostering the operators' and OMs' precautions and vigilance regarding the possibility of failure. Training prepares them to be critical of and reflect on their experiences and expectations while actively engaging the possibility of something going wrong or failing. It prepares them to manage and be aware of the residual uncertainty that cannot be contained or reduced, thus might surprise. Precaution and vigilance let the operators and OMs look out for pre-cursors of events in an embryonic form that can be prevented. As discussed in Chapter 2.2 on uncertainty, precaution addresses a sense of false security, which signals the ignorance towards the possibility of other as a potential threat to be averted. Vigilance, on the other hand, operates in an area which seemingly lacks uncertainty. What is, has, and might happen seems known now, yet uncertainty about the duration of this clarity remains. Both precaution and vigilance aim for the operators and OMs to reflect on their (intended) actions and operational environment to avoid and be prepared for potential contingencies. Reflectivity is particularly important regarding the reliance and use of experiential knowledge. Experience shapes expectations, and expectations are a double-edged sword during (normal) operations. When appearing as overconfidence, they can lead to miscalculations. The Emsland Case is a case in point, as it was the overreliance on "empirical assessment" rather than on mandated "load flow calculations for checking the N-1 criterion" that led to a misjudgement of the situation and turned what could have remained a normal incident into a failure cascade (UCTE 2006: 19).

In the initial training at TSCNET, precaution and vigilance were shaped through the mentoring process. The novice OM was required to verbalise possible contingencies and backup procedures regularly, learned to double check their action, and, if required, ask for help and checks via four-eye-principal. Verbalising possible contingencies and backups did not just serve to become familiar with and build experience around them but also to foster an alertness about what could go wrong and to expect it. Furthermore, through their apprenticeship-like initial training, the OMs would learn to speak up if they were unsure or wanted reassurance. The (novice) OMs, as I experienced it, trusted their colleagues to provide help if needed and regularly asked or offered it. During the continued training at TSCNET, the OMs regularly received training on contingency procedures or read up on them during calmer shifts. As situations exceeding the everyday are relatively rare, this active and periodic re-engagement with the possibility of failure helped to uphold their precaution and vigilance. Through their initial and

continued training, the OMs can react without tense excitement should an event emerge and exceed the everyday.

This response was displayed as unexcited 'cool professionalism' and became evident toward the end of my ethnography as the French TSO, RTE, declared a 'critical grid situation' (CGS). "A Critical Grid Situation is a potential emergency state, identified in the operational planning phase. During a Critical Grid Situation, the available regular countermeasures are exhausted, and therefore, TSO(s) are required to take regionally coordinated extraordinary countermeasures" (ENTSO-E 2022b). During my shift, a system adequacy issue was forecasted in France. Due to strikes and ongoing COVID-19 delayed maintenance, nuclear power plants were still offline, and a cold front was forecasted. In France, most people heat with electricity; thus, a change in just a degree of temperature leads to an increase of about a gigawatt of electricity demand. A substantial 18GW of generation was forecasted to be missing from Sunday to Monday to meet demand. The OMs response surprised me. For me, this was worrisome but exciting. For the OMs, it wasn't routine, but their reaction differed. As each individual OM was notified of the declared CGS, as per their protocol, their reactions were sober and unexcited. To be prepared for the possibility of an emergency grid situation, they reviewed the handbooks and procedures and discussed the now-altered communication protocols.

The risk of this 'cool professionalism' entails becoming complacent and overconfident. To counteract the TSO, TransnetBW promotes precaution and vigilance. These terms were explained to me by an executive during the TransNext challenge and the balancing operator during my control room observation to work similarly at TSCNET. He explained that attentiveness to the possibility of an event threatening grid security is instilled in every new employee on their first day. They would gift and encourage to read Mark Elsberg's (2012) novel 'Blackout' (Figure 6). While fictional, it is based on a report by Petermann et al. (2011b) to the German Parliament about "What happens during a blackout". It is intended to ground new employees by highlighting what is at stake if they let down their guard. It can do this, as its technical depiction of a blackout and its aftermath is, according to multiple conversations about the book (I have read it, too) with TSO and TSCNET personnel, assessed to be relatively accurate if a bit too optimistic.

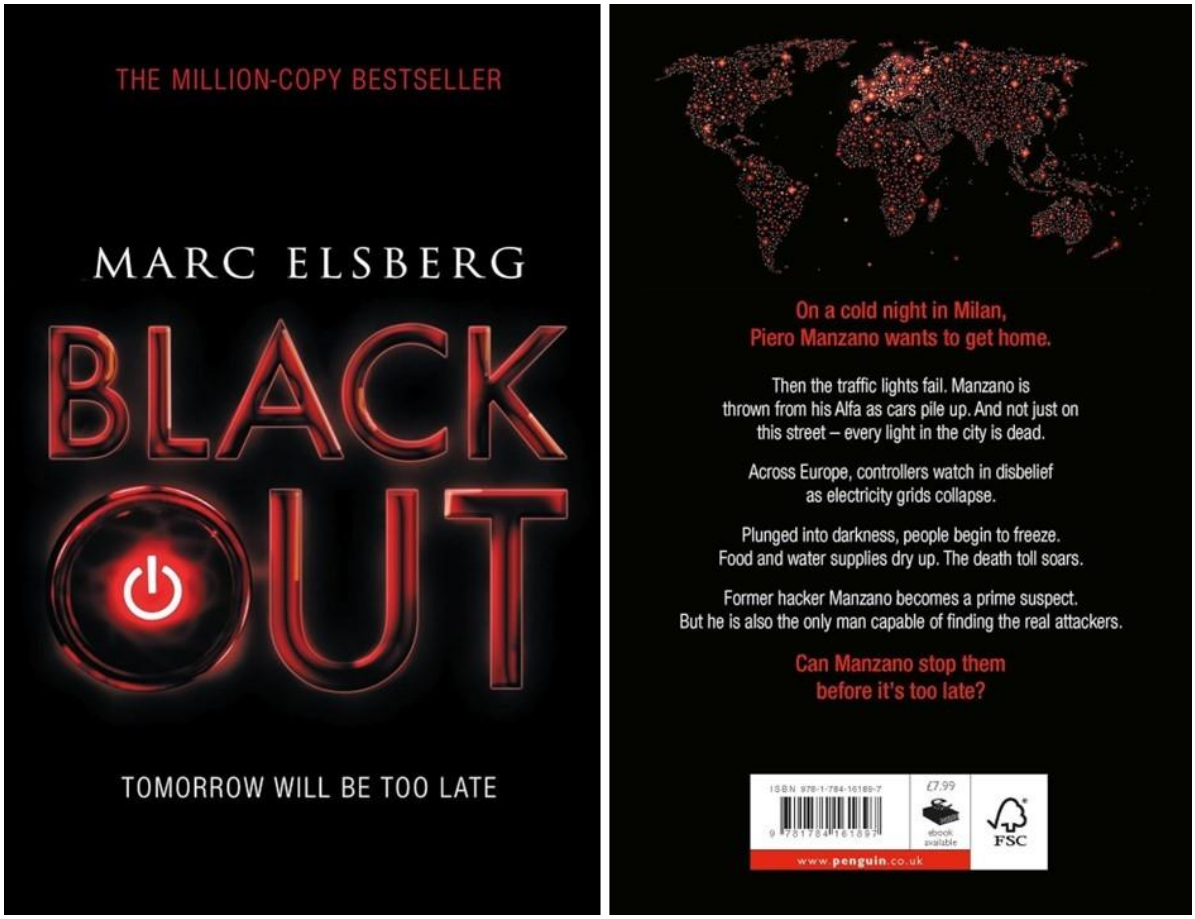


Figure 6 Blackout by Marc Elsberg, a Technical Novel Intended to Foster Vigilance and Precaution

6.3 Training for and in the Everyday

The previous section detailed how training comes to matter as the management of uncertainty. This section continues with these ideas while illustrating them with more empirical observations. In responding to the complexity of the power grid, its operation, instability, and latent potential for catastrophic failure, training secures through a multiplicity. To train for the everyday means for the grid operators at TSOs and the operational managers (OMs) at RSCs, at TSCNET to learn to keep everyday oscillations in check, remain in control, or recover the system to below thresholds of escalation or cascades. Furthermore, the (initial) training for and in the everyday seeds the ability of the TSOs and TSCNET to prevail in the exceptional. Through their initial and continued training, they become uncertainty managers who prioritise comprehension over encyclopaedic knowledge, are attentive to (potential) failures, and are aware of their knowledge limitations and capabilities. Drawing from my ethnography and participatory observations, this section will illustrate this.

When I joined TSCNET in early September of 2021, I started together with a new OM candidate. I partially shadowed the candidate's pathway, focusing on the evening shifts, especially the DACF process (see Chapter 5.4.3). I eagerly absorbed the same training materials they were going through while being attentive and observing during the shifts in the coordination room. I soon achieved a good understanding of the routines of these shifts. Halfway through my internship, an OM commented that

I probably could do the job by now, as it was primarily "just clicking buttons in the correct order". Later that week, however, and during a DACF-iteration model, changes needed to be made for a substation, and I realised how little I knew about grid components and their functions. The workings of phase-shift-transformers (PSTs) or the layout/design of substations are a case in point here. While I had to quickly pick up this basic knowledge, the three-month training period focused on something else for the OM candidates.

For the OMs, the initial training was about securing through becoming enabled to utilise TSCNETs protocols and individual forecasts. It was not about building basic power grid knowledge. The OMs studied the 'right' sequence of actions and their backup procedures in a hybrid format that also intended to foster experience. Their initial training relied on formal documentation, process descriptions, and shadowing seasoned OMs. Apprenticeship-like, they were provided with a mentor who guided them through their training. Nearing the end of their three-month period and in agreement with their mentor, the OM candidate scheduled their 'matura'. As an oral and open book qualifying examination, the OMs are questioned by a small panel. They are assessed based on their ability to comprehensively answer questions from an examination sheet covering all provided services, procedures, and backups. This file contains around 120 individual queries and is provided to each OM candidate at the start of their employment. Having received and studied this file myself, the questions range from basic descriptive questions—such as "What is process XY, what role does the OM play in this conference call, or where can you find XY"—to more sophisticated questions like "When X happens, what do you have to do", or "when process XY fails in Z way what do you have to do to fix it".

Although not explicitly stated by the OMs, the initial training process, its final exam, and the following continued training are important for the OM's ability to secure via their established procedures and experience in at least two ways. Firstly, besides forming the ability to work with and correctly deploy their tools (standardised procedures and forecasts), their training is positioned to build and validate comprehension rather than assessing encyclopaedic knowledge. Comprehension is important for their ability to manage uncertainty, as it allows them to see a bigger picture and understand their actions not in isolation but in the broader edifice of power grid security. Secondly, it fosters attentiveness to (potential) failure and the boundaries of one's own knowledge, understanding, and capabilities. The design of the 'matura' as an open-book examination acknowledges that an individual might not know or remember, especially in a stressful situation. Thus, as long as the examinee can reflect on his inability to answer a particular question and can refer to the right expertise or handbooks, not knowing is not considered too problematic.

The limitation of knowing can originate from the external environment or internally. The external and internal limitations here are recognition and attribute of systemic "chaotic uncertainty" (Keohane & Nye 2000) that inevitably surprises. In interactions with TSOs and TSCNET personnel, this awareness of surprises occasionally surfaced in references to Murphy's law, which states that "anything that can go wrong will go wrong [eventually and most likely during the worst possible moments]". Citing Murphy's law or describing the grid in a human language as 'moody' or 'temperamental', the power engineers implicitly refute the "elimination of complexity" and the privileging of "simplicity and reduction" (Montuori 2003: 239, cf. Weick & Sutcliffe 2007). In one such instance, the software tool AMICA acted up to calculate the day ahead congestion forecast. "AMICA being AMICA again and doing what it wants" (Fieldnotes 201021), the OM on shift noted. As the overloads were not resolved at the

end of the shift, the handover to the next shift started with a brief comment: “It’s one of those [moody] days where AMICA is not your friend” (Fieldnotes 201021), meaning the grid is trying to foil the OMs job to reduce uncertainty and overloads through forecasting. In deploying such language, the operators and OMs recognised that while the individual’s formal knowledge (received through academic education and the study of ‘process handbooks’) is important, it alone is insufficient to contribute to the reliability and security of operations. Although processes and procedures are highly standardised, they can fail (like AMICA did during that shift) to guide the OM or operator in their actions, as they can lack specificity or have been unable to account for emerging contingencies. Invoking affectual descriptions of the grid, the operators, and OMs, thus, highlights a tension between the reliance on standardised, formal, and experiential knowledge in the everyday.

The apprenticeship-like initial training at TSCNET served as a platform where not just formal learning about processes and procedures but trial-and-error learning – within acceptable limits - was enabled. Trail-and-error learning is generally a specific way of learning that enables TSO operators and TSCNET OMs to experience the behaviour of the technical system, oneself, and colleagues through experimenting, simulation, or scenarios. The mentor or senior OMs, the candidates shadowed would ensure that mistakes compromising the uninterrupted service provision were prevented or swiftly corrected. Through training, to trial and err, trust is built while expectations are calibrated (Weick & Sutcliffe 2007). Moments where trial and error are possible present opportunities to learn about the system and from each other in an exploratory way. Yet when operational stakes are high, like in grid operation, there only exist a few opportunities to learn through trial-and-error (Schulman et al. 2004: 111). Besides the supervised and mentored first steps of OM candidates, these occasions range from informal meetings where ideas and action pathways were discussed between peers to modelling and simulation, such as the iterative DACF forecast described in the previous chapter. Not least, (emergency and crisis) exercises offer a more profound yet more resource-intensive opportunity and will receive more attention in the next section.

As an important component for trial-and-error learning and a legal requirement, each performed task during the operational shifts at TSCNET needed to be logged, and the OMs followed protocols. Through protocoling, what occurred and what tasks were performed partially lifted future uncertainty about the past. The protocols then served as an opportunity for future learning and a repository of past experience. As part of the initial training, the OM candidates and, to some extent, myself, learned to fill out the operational logbook templates. These were not only to be archived but aided the daily shift ‘handovers’, providing an overview of what has happened and was done. By relying on and filling out the logbooks rather than studying protocoling, the OM candidates quickly realised how much information was required. Through informal but periodic feedback about their protocols, the OMs constantly re-evaluated their performance and adapted and updated their styles of protocoling so that misunderstandings were kept to a minimum. For me, the stored logs were a particularly valuable window into past events, such as the system split of January 2021 and a local power outage in Munich from the 21.05.21 affected TSCNETs services. Similarly, they were periodically reviewed by the head of operations and used for training or specific event analysis.

Even though everyday procedures and protocols contain uncertainty within a margin**,** residual uncertainty remains, while the operators and OMs themselves only possess a limited cognitive ability and capacity to process information. Initial and continued training, thus, facilitates the sharing of the burden of the individual and collective limitation through strategies of error culture, peer support and

broadening and changing perspectives. These support mechanisms enable the management of not just the residual uncertainty of standards and protocols but also that of limited human performability.

Partly a requirement for trial-and-error learning, an error culture where mistakes and errors are attributed without assigning blame is not a novel but an established attribute of highly reliable systems (Rochlin 1989, Carnes 2011, LaPorte & Consolini 1991, Weick & Sutcliffe 2007). Nevertheless, it can be difficult to implement and maintain as it relies not just on training but also on the acceptance and willingness of individual and collective fallibility (Schulman et al. 2004). Besides training to, for example, follow the correct reporting procedures, error culture requires the 'right' character of the operator and OM. For example, the TSO balancing operator I joined for a control room shift highlighted that new operators occasionally retire during their initial training period if they do not display integrity, humility and reflectiveness.

To be critical of not just the actions of others but also your own is accepting responsibility and requires integrity. At TSCNET, where mistakes were made, the individuals often addressed and named them as such. When not recognised by the OM, peers highlighted them in a supportive fashion and corrected them. In a particular instance and outside of the initial training, the head of operation talked to the involved operators before virtually convening all OMs to discuss and learn from what happened together. In a different instance of continued training for cyber security and awareness, fake fishing emails were distributed internally. Most employees opened it, and almost half of them clicked a phoney and ‘infected’ link. As a measure to startle, raise awareness and not to assign blame, the ways to recognise and examine emails were collectively discussed and trained for. The individuals clicking the link were also directed to an explanation page for their error. Similarly, the post-event analysis and reports on, for example, the 2006 or 2021 European system splits (ENTSO-E 2021b, UCTE 2006), if through a very technical language, demonstrate a willingness to learn from large-scale system disruptions. During my ethnography at TSCNET and participatory observations at the TSO, TransnetBW, the openness to talk about, its regularity and the willingness to address these events (without me inquiring about them) surprised me. For me, this highlights a culture where it is accepted and positively connotated to engage failures and near-missed constructively.

A further support mechanism that helps to suppress residual and individual/collective uncertainty is the OMs and operators' reliance on each other for peer support. During the initial training of OMs at TSCNET, the mentors fulfilled this role while other colleges regularly 'chipped in' to reword explanations or freely share their insights. Outside of the initial training, these instances were seemingly banal and unofficial moments in which a colleague would ask for help or clarification. Help would then often come from 'process leads'. For the individual processes, like the DACF, senior OMs were designated as 'process leads' and assigned with the cyclical updating of the individual process descriptions and process development. Deferred to as experts (cf. Weick & Sutcliffe 2007, 2015), their peers recognised their in-depth knowledge of a particular process, thus their ability to alleviate their uncertainty for a related matter. To draw on local expertise similarly while changing the perspective as the third support mechanism, TSO and RSC (TSCNET) regularly exchanged personnel. This change of perspective that became interrupted through the COVID-19 pandemic not only recognised each other's expertise but fostered understanding and coordination. TSCNET OMs joined their counterparts in the planning departments of the TSO and vice versa and became acquainted with their perspective. As some OMs shared with me, this process, for example, helped to raise awareness and solve occasional data quality issues they regularly encountered when preparing their forecasts. As part of

the continued training process, these exchanges helped deepen comprehension of their process and enabled attentiveness to the limitations of their own perspectives.

So far the reliance on a trained OM or operator is without alternative. While the training process might be time and financially intensive, automation or 'smarter' technologies might reduce the reliance on or workload of human OMs or operators. However, they cannot and should not replace the trained OM or operator. The possible (future) contribution of automation for data management, forecast and report creation at TSCNET was generally pointed out, yet an acute awareness of its limitations accompanied it. During an evening shift with the head of operations and in conversation, this limitation was primarily framed around the requirement of OMs to be familiar with processes, thus their ability to handle contingencies. "If you are involved all the time, then you don't have to read the process description anymore; you are more aware of what is going on and can fix upcoming issues quicker" (Fieldnotes 121021). On the other hand, and reflexively, it was suggested that if processes were fully automated, comprehension for and attentiveness to operational details would be lost, and the time required to deploy (semi-) manual backups would be significantly prolonged while generally increasing error probability in these (backup-) processes. When reliable, secure operations take centre stage, the tension between standardised and experiential knowledge to secure uncertainties favours the trained OM or operator. Through their comprehension of the system, attentiveness to potential failures, and awareness of their limitation of knowledge, understanding, and capabilities, they are trained to manage the residual uncertainty that automation and standardisation can only partly contain.

Through their initial and continued training, TSCNET and TSOs are organisations of institutionalised learning. They profit and rely on it to achieve and ensure the uninterrupted flow of electricity. Although training is required and framed today through EU regulations (European Commission 2017a) its ability to function as a security technique can become compromised. It can become compromised if other rationales, like automation or financial pressures reduce the operators training time. Besides the caution from TSCNETs head of operation about the need to be engaged with the process to remain trained to secure and manage uncertainty sufficiently, the TSO balancing operator I visited in TransnetBWs control-room had a similar caution.

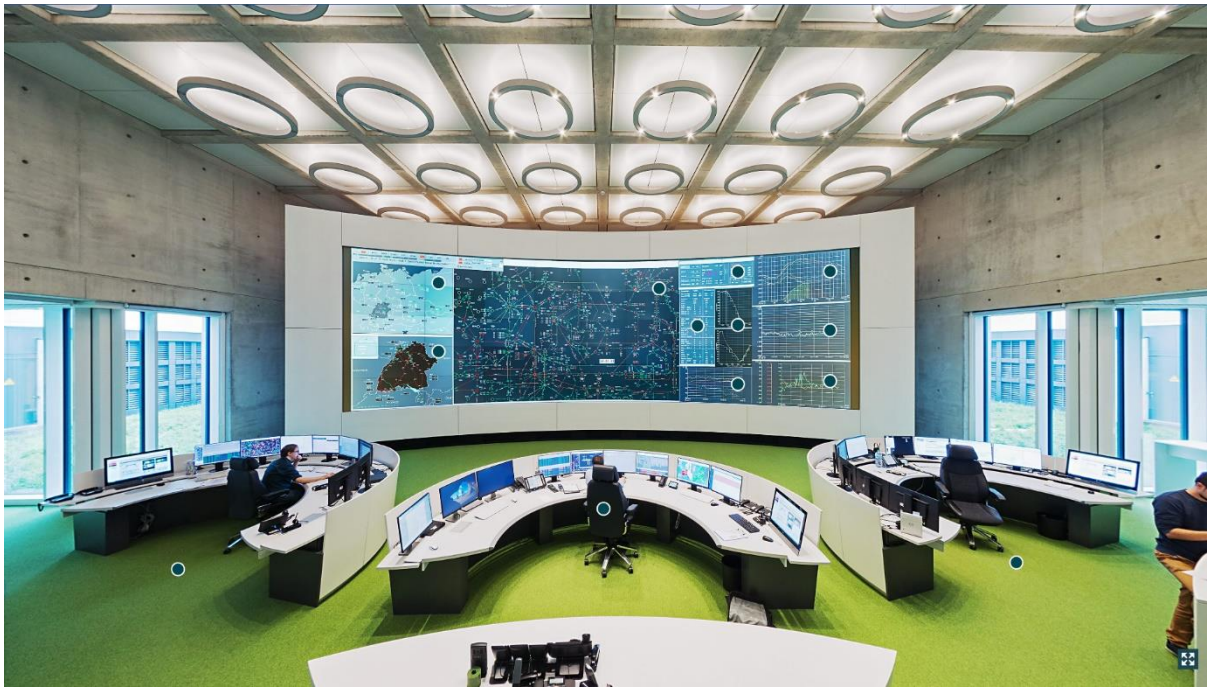


Figure 7 TransnetBW Main Control Room Wendlingen. Source www.transnetbw.de

When I joined the balancing operator for a control room shift (workstation on the right in Figure 7), a change in the initial training was pointed out. This was associated with a decline in the operator's ability to handle 'normal incidents' and exceptional situations. Paraphrasing and translating that conversation, it was explained that "*previously an operator trained for one year, and 'learned' the trade of all department. The operator would thus have a good understanding of the tasks and difficulties of each specific job. Now they only get trained in one department – to save costs - for six months, missing the opportunity to fully understand the work of the others. This rationalisation of training, to the point where operators are good at one thing but have a limited systemic overview, can be problematic as they reach their limits quicker when confronted with adverse circumstances*" (Fieldnotes 281921). For this balancing operator, the late redispatch request detailed in the last Chapter (5.3) was then, in large, a consequence of this rationalisation away of training and subsequent 'ignorance' of the operational planner towards the requirements of balancing. While training is a security technique for power grid operation, its ability to foster train the operators and OMs as uncertainty managers, thus the quality of the security that it produces depends on the available resources for it. While this might not significantly impact everyday operations, it can adversely affect the response to normal incidents and exceptional situations. How the latter are secured by training is discussed next.

6.4 Training for the Exceptional

Training for the exceptional becomes a security technique distinct from standardisation and forecasting. It does not focus on preventing what is emerging to become events but on their management, mitigation, or timely recovery. Training for the exceptional primarily prepares capabilities and capacities that are only tangentially resources of and in the everyday. Training as capability- and capacity building address the TSOs and TSCNET's 'contingency managers' and their operators and OMs. Contingency managers are a new category of personnel whose job is to imagine, plan and prepare for what might happen. In contrast to the operators and OMs, they, for example, focus on fulfilling the legal or insurance requirements for formal business continuity, emergency and crisis management, or information security management.

Training beyond the everyday is, for a select group of contingency managers, a process of sense-making through expertise that allows them to relate international, national, and internal laws, regulations, and standards to their varying authority and sometimes conflicting visions of each other. Secondly, and beyond what is standardised, the operator can manage the uncertainty of an evolving incident ad-hoc, relying on experience and improvisation. To make sense of, select, and apply various contingency strategies and correlated standards effectively, it is not enough to have formally studied them. Instead, in "deference to their expertise" (Weick & Sutcliffe 2007, 2015), a small circle of senior employees selectively establishes and maintains the corporate contingency architecture. At both TSCNET and TransnetBW, this was a select group of senior managers who, during the COVID-19 pandemic, operated outside their regular business architecture and through an emergency and crisis organisation (cf. Hofinger & Heimann 2016, Kemmer et al. 2021, Kühn 2021). In these standby organisational structures, they bring together the senior expertise of their organisations, which is usually siloed and dispersed during everyday operations.

The contingency managers I engaged with were characterised by in-depth knowledge of their organisational processes and the regulations that govern them. They gained this from long-term employment with their organisations, where they usually worked in multiple (operational) positions while maintaining a good network within and outside their organisations. As such, they possess not just comprehension of the everyday processes but also first-hand and anecdotal experience. Mainly originating from their network and anecdotal experiences, they maintain a repository of stories about near-misses, close-calls, and actual exceptional events, as well as best practices that are affectionately retold and form part of their collective memory and understanding. Through these anecdotes, such as the Emsland Case in the preface, they gain knowledge of incidents beyond official reports, with more detail that enables and trains them to pay attention to where and how failure occurred and could occur. While at TSCNET and in the process of professionalising their emergency and crisis management, this anecdotal knowledge of the extraordinary was drawn on in exchanges with TSOs. As a voluntary public-private partnership, the 'UP KRITIS' provided a formalised repository for what they called "scenario portfolios" that drew on the collective experiences of their critical infrastructure operator members. Via the pool of different scenario portfolios, the members of 'UP KRITIS' profit from the collective experience of receiving 'blueprints' (electricity, heating, water, IT outage, personal shortage, compromised building), to measure and orient their preparation and expectations against. For the contingency managers, this pool of collective experience provides a learning opportunity that extends their personal experiences. It allows them to expedite their training and preparedness for scenarios they have not yet experienced themselves but can now 'play/think through', profiting from the experience of others.

The experience of 'contingency managers' forms over time and allows them to navigate the security landscape. To become "inducted to the [this] shared knowledge of […] planning procedures" (Abram 2014), to break apart the amalgam of regulations and standards and understand their authority, interrelation, and visions takes time. Yet, this understanding enables the 'contingency managers' to reflect on what is expected of them (legally) by their organisations and to assess their ability to plan realistically and the level of resilience to exceptional events. Large parts of the TSOs and TSCNETs' ability to continue operating, for example, rely on various means of uninterrupted and auxiliary power supplies. While the duration, or possession of an auxiliary power supply, can be mandated (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2019, Bundesamt für Sicherheit in der Informationstechnik 2016) the assessment of their dimensioning, use of renewable power (cf. Rutherford & Marvin 2022) and integration into the existing contingency plans is a contingency manager's job. Furthermore, maintaining this infrastructure on standby is costly, while providing only a finite amount of extra power and security, depending on the fuel, lubricant, and spare part logistics. Batteries have a finite lifespan and need to be replaced, while even the fuel for auxiliary generators needs to be used or exchanged regularly (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2015, 2019).

Through the experience and expertise gained through their training, contingency managers can navigate the trade-offs of planning for and managing the exceptional while managing uncertainty. Through their training, they can prioritise chronically scarce resources depending on legal responsibilities, executive preferences, or perceived (economic/societal/moral) obligations. As an organisation, TSCNET and its contingency managers stand out. Through providing forecasts to the TSOs, TSCNET is not 'directly' involved in the management of electricity flows, thus not a critical infrastructure by the German Federal Office for Information Security (BSI) definition, not bound by the same legal obligations as the German TSOs. Nevertheless, they understood themselves as critical for day-to-day grid operation through their executive's priority and the shareholder TSOs' emphasis. Their contingency planning originated from the requirements for information security and grew to reflect 'UP KRITIS' scenarios while incorporating selective aspects of various legislation and standards. The experience, partly shared by TSOs, enabled the 'continuity managers' to navigate and negotiate this diverse and sometimes ambiguous and uncertain regulatory landscape.

Training for the exceptional is more than the ability to know everyday and 'emergency' codes; it is building and nurturing the ability to manage uncertainty through experience and improvisation. While this holds true for the select group of 'emergency managers', it also encompasses the TSO operators and TSCNET OMs. As the managers on the frontline of grid operation, they are the first (human) line of defence should an event exceed the everyday. If uncertainty correlates with an event's magnitude, so does the need to improvise. Yet, improvisation originates from knowledge and understanding, from comprehending the system and what needs to be done and is desirable. For the operators and OMs, this entails familiarity with formal emergency protocols and procedures, primarily gained through training and exercises. Although I was unable to participate in or observe these trainings myself, their rough structure can be reconstructed through conversations and interviews, public network code (European Commission 2017c, a) and promotional materials of their training provider (DUtrain 2022).

Training for "all system states", for the "safety and security of persons […] and other equipment in the transmission system operation", for "stress management" and "human acting in critical situations", and "to exceptional operational situations" (European Commission 2017a: 44 f.) is qualitatively

described by the system operational guidelines (SO GL). Nevertheless, as with training for the everyday the TSOs and TSCNET remain responsible for operationalising it through in-house ‘training coordinators’. Although the TSOs possess individual training tools, they partly outsource their training to 'DUtrain'. This is because the SO GL explicitly calls for “offline” (European Commission 2017a: 44 f.) training through simulation. As a quasi-monopolist, the company 'DUtrain' provides system operators of the electricity and gas industry with "simulator-based operator training courses" and references 23 central European TSOs and three of the six RSCs as customers (DUtrain 2022). Here, the TSO and RSC personal training is augmented by real-time simulations of the grid and their workstation. They train with peers and across network scales (RSC-TSO-DSO etc.) multiple times a year. Due to the time constraints and resource intensity, these trainings generally exclude the extremes of blackout and black start yet still focus on exceptional events short of them, for example, system splits, frequency or voltage deviations. The blackout and black start training are, according to the interviewed TSO head of system restoration (interview 1), conducted as per the minimum legal requirement (European Commission 2017a) and every three years. Doing so provides an opportunity for the TSO operators to learn not only how to manage uncertainties but also their expectations and limitations.

For both the contingency managers and the operators/OMs, a limit exists on how much they can train and exercise for the exceptional. This has partly to do with the disruptiveness of exercises for their everyday jobs, the time required, costs and availability of facilities and other TSOs/DSOs and government agencies to train with. Furthermore, as the exercises and simulations primarily rely on imagination to frame the scenarios, they are inherently limited by it. For the simulations at DUtrain, this limitation through imagination is generally reinforced as their models and facilities similarly limit the possibility. These two limitations, however, are only of secondary interest as what these trainings set to achieve is not the elimination of uncertainty but offer the possibility to train for its management safely. Besides testing for a comprehensive understanding of the relevant procedures and code, to train the ability to cope with unexpected disturbances and learn from these experiences. For the balancing operator I joined at TransnetBW, these trainings for the exceptional were particularly valuable to become trained to expect surprises and to foster the ability to cope with stress and to become aware of its effects. "Under strain, you do things that you usually wouldn't do" (Fieldnotes 281021). The affectual experience of the exercise provides a safe space to experience failure. Failure in this controlled training environment is unproblematic and even intended, as it provides an opportunity and space to learn, not just from mistakes but from your reaction to stress and surprise. To train through and with failure is calibrating the operators' and OMs expectations while building their capacity to become familiar with and learn to manage surprise and overextension. To trial and err in training creates the capacities and nurtures the capabilities to prevail in the exceptional. It means relying on codified and experiential knowledge differently and transitioning between them as the situation mandates.

6.5 Conclusion

This chapter has examined how training operates as a security technique within the German transmission grid. It contributed to the broader aim of this thesis: to understand how uncertainty is managed in the everyday governance of critical infrastructure. It demonstrated that training secures the grid not by containing or reducing specific uncertainties, i.e. potential threats, but by cultivating the embodied capacity of operators and operational managers (OMs) to act under conditions of partial knowledge, residual uncertainty, and complexity. In doing so, training complements the anticipatory logics of standards and standardisation, as well as forecasting, while extending the reach of infrastructural security into situations where procedures or predictions fail.

Empirically, the chapter identified three key ways in which training functions as a security technique. First, training secures in and for the everyday by enabling operators and OMs to use tools such as forecasts and standardised procedures proficiently. This involves the development of both codified and experiential knowledge, allowing actors to operate securely under normal conditions and within routine temporalities. Second, training secures through the cultivation of experience, preparing actors to improvise and respond when standardised scenarios or forecasts fail to contain or reduce uncertainties. This was shown to be crucial for navigating 'normal incidents' and for transitions of operational practices when faced with exceptional grid states. Third, training secures by fostering vigilance and precaution, encouraging operators to remain alert to embryonic failures and to recognise the limitations of their tools and their own expectations. Together, these three functions highlight that training does not simply transmit knowledge but creates the reflexive capacity to manage multiple forms of uncertainty.

Building on the framework developed in Chapter 2, these findings can be read through the three analytical categories of ‘work on uncertainty’, ‘relate to a future’, and ‘secure by’. Training works on uncertainty by preparing actors to respond to what remains unknowable despite other techniques. It relates to the future not through calculation or imagination, but through embodied anticipation, developed via the three different ways training secures. It secures the reliability of the grid operation through procedural fluency, improvisational skills, and a collective error culture. Training, in this sense, extends the anticipatory logic of infrastructural governance (Amoore 2013, Anderson 2010b, Aradau & van Munster 2011), not by narrowing uncertainty, but by equipping actors to manage it.

Two types of actors were shown to be central in enacting this security technique: ‘uncertainty managers’ and ‘contingency managers’. The former—primarily grid operators and OMs—are trained to anticipate and manage both expected and unexpected events. Their expertise is cultivated through apprenticeship, mentorship, and experiential learning, which enable them to transition between different forms of knowledge as circumstances demand. The latter—contingency managers—are tasked with ensuring organisational preparedness across scenarios that exceed the temporal and procedural logics of everyday operation. These actors engage with regulatory, logistical, and material dimensions of emergency planning and continuity management. Together, they represent the human infrastructure through which the anticipatory governance of electricity is rendered operational.

The chapter thus contributes to Critical Security Studies by advancing a practice-oriented account of infrastructural security that moves beyond discursive threat construction (Campbell 1998b), sovereign decision-making (Agamben 2005), or exceptional logics (Agamben 2005, Dillon & Reid 2009). Instead, it demonstrates how security is enacted through the dispersed, embodied, and often invisible labour of professionals working behind the scenes of vital systems. The concept of biopolitical security, as

outlined in Chapter 2, is further extended here: life is not secured directly, but through the training of those responsible for the systems that sustain it. Infrastructural actors are not merely agents of control, but practitioners and pioneers of what Anderson & Gordon (2017) call “non-events”, interventions that prevent escalation by ensuring continuity in the face of emergent threats.

Furthermore, the chapter contributes to debates on biopolitical governance by showing how the management of circulation (Foucault 2007) is mediated not only through algorithmic prediction or pre-emption relying on backcasting, but through repeated practices that cultivate the capacity to respond to what remains unknown. Training, in this context, is not a tool of total control but a biopolitical security technique aimed at navigating a world of systemic, multiple, and often inconceivable uncertainties (Dillon & Lobo-Guerrero 2008, Mason 2022). It reflects a shift from the logic of eliminating failure to one of managing its possibility, reinforcing a broader CSS interest in the anticipatory and affective dimensions of security work (Adey & Anderson 2012, Anderson 2010b, Dillon & Lobo-Guerrero 2008, Mason 2022).

In conclusion, this chapter has demonstrated that training is a vital yet underexamined security technique that sustains the everyday functioning of critical infrastructures. It enables actors to act not only when the grid functions as expected, but especially when it does not. In combination with standardisation and forecasting, training secures the power grid through a layered architecture of anticipation. Its contribution lies in extending the temporal and epistemological bandwidth of infrastructural security, from the routine to the uncertain, from the known to the emergent, and from the procedural to the improvisational. In doing so, it highlights that the endurance of vital systems depends not only on technical stability or predictive foresight, but on the capacities of those who are trained to live with uncertainty—and act despite it.

7. Conclusion

This thesis makes an original contribution to the field of Critical Security Studies (CSS) by demonstrating how life is secured in and through the everyday governance of critical infrastructure. Drawing on sustained ethnographic fieldwork, it traces how anticipatory techniques—standardisation, forecasting, and training—are deployed by transmission system operators (TSOs) and regional security coordinators (RSCs) to manage a multiplicity of uncertainties in the German transmission grid. In doing so, the thesis makes biopolitical approaches to security empirically tangible by tracing how life is sustained not through spectacular interventions or sovereign decisions, but through the mundane, recursive labour of securing a particular vital infrastructure and its circulations. It also contributes to interdisciplinary debates in human geography and infrastructure studies by revealing how security is enacted across networked infrastructures, interlinked operational spaces and regulatory scales. By foregrounding the figure of the "uncertainty manager" and the importance of routine technopolitical practices, the thesis offers new insight into how infrastructural life is governed under conditions of systemic complexity.

Overall, this thesis aimed to understand how the contemporary German power grid, as a complex infrastructure, is secured in the everyday. It aimed to understand how the security of a specific flow (electricity) relates to a broader concern for the security of the infrastructure (power grid) that enables it. The analysis of the German grid focused on the transmission scale and its actors, particularly the transmission system operators (TSOs) and the regional security coordinators (RSC) TSCNET. Behind the concern for the ensured flow of electricity lies the conceptualisation of the power grid as critical infrastructure. This criticality was shown to originate in the growing dependence of Western, and particularly German, "lives and lifestyles" (Graham 2010) on the constant flow of electricity since the early to mid-20th century (Hughes 1983). Ever since, electrical flow has been discussed as essential but inherently unstable, uncertain and in need of constant securing.

Electricity flow was presented as constantly at risk of blacking out or failing catastrophically if the balance of demand and generation, indicated by the grid frequency, is not carefully managed. The potential for catastrophic failure was attributed to the grid's complexity and its "tight coupling" (Perrow 1984). The grid, thus electrical flow, is at risk of small, embryonic events "escalating or cascading" (Little 2004) towards a blackout. The blackout was presented as a threat to grid security and a potential catastrophe if it were to become widespread and prolonged. It is distinct from 'normal incidents' (cf. Perrow 1984), regularly occurring local and usually short-lived power outages. The catastrophic blackout was briefly introduced as a low-probability, high-impact event, rarely happening and so far never unleashing its destructive potential. Yet, the blackout is a latent, uncertain potential lurking in the background that needs to be thwarted.

The uncertainties that threaten power grid security are multiple and intrinsic to the infrastructure's complexity. As discussed in the introduction and literature review, the transmission grid is a highly complex and tightly coupled socio-technical system. Its functioning depends on a vast array of interdependent components, whose interactions are non-linear and frequently opaque. Following Perrow (1984) and Pescaroli & Alexander (2015, 2016), this complexity introduces systemic uncertainty: events do not occur in isolation but can escalate or cascade unpredictably across spatial and temporal scales. The impossibility of full system knowledge in such a context makes comprehensive control illusory. Thus, the grid's complexity is the condition that renders it uncertain, and these uncertainties, in turn, become the object of security.

This thesis has demonstrated that infrastructural complexity not only generates the need for security but also influences the security techniques employed. The layered deployment of standards and standardisation, forecasting and training does not aim to eliminate uncertainty, but to make it governable within acceptable margins. These techniques are not redundant or interchangeable: each addresses a different dimension and temporality of uncertainty, from technical deviation to behavioural readiness. Together, they form a security amalgam that is both distributed and recursive, operating within and across infrastructural systems. By foregrounding complexity as a constitutive condition, this thesis also contributes to the interdisciplinary literature on infrastructure and security (Collier & Lakoff 2008, 2015, Perrow 1984, Pescaroli & Alexander 2015, Star 1999), demonstrating how the governance of vital systems depends on the practical management of uncertainties in different spacetimes.

In this thesis, I argue and examine security not as control, but as the management of uncertainties and uncertain potentials. The complexity of the infrastructure, the number of its components and potential (inter-) relationships, and the volatility of the medium, electricity, negate stability and full control. Power grid security was shown to be guaranteed primarily in the seemingly 'mundane' everyday. It is primarily in the everyday that the flow of electricity is secured and the ability to prevail and manage exceptional situations is incubated. In demonstrating how standards and standardisation, forecasting, and training 'work on uncertainty', 'relate to the future', and 'secure by' differently, this thesis provided a novel perspective on everyday power grid security (Figure 8).

The novelty of this thesis stems from discussing the combination of individual security techniques to work on and secure against a multiplicity of uncertainties (cf. Mason, 1993, 2019, 2022), as illustrated in Figure 2 (Chapter 2.2). Rather than relying on a centralised, exceptional intervention by the state or sovereign actor, this layered approach reflects how security is increasingly enacted through routine, anticipatory practices distributed across networked infrastructures (Adey et al. 2015, Anderson & Gordon 2017, Aradau & van Munster 2011, Collier & Lakoff 2015, Folkers 2017a). It is through the combination of these three security techniques that any deviation from acceptable parameters (frequency, voltage, over-loading) is kept in check, and the uncertain potential for escalation and cascading system failure is managed.

In engaging with power grid security as a mundane, everyday practice, this thesis followed Star's (1999) call to study seemingly boring things. In studying everyday power grid security and beyond the primary contribution to CSS, the thesis engaged in an interdisciplinary way to related literature on infrastructure (Amin 2014, Anand et al. 2018, Star 1999) and energy and electricity (Bridge et al. 2018, Bulkeley et al. 2014, Jenny et al. 2019, Luque 2014) and critical infrastructure security (Aradau 2010, Coaffee & Clarke 2016, Edwards 2014, Schulman et al. 2004). The thesis's interdisciplinary contribution lies in providing new empirical material on the power grid's criticality, operation and security as a specific (critical) infrastructure. It furthermore offers empirical insights into the transmission scale that, in debates on ('smart') power grid security, has been neglected (Folkers 2019b, Lovell 2018, Luque 2014). In doing so, it offers an opportunity for future debates on the power gird, its transition, and security to include the transmission scale.

At the same time, the thesis argues that critical infrastructure security relies on practices that are rarely recognised as security techniques. Standards, standardisation, and training are typically viewed as technical or administrative; however, this thesis has demonstrated how they function as vital anticipatory techniques for managing uncertainty and sustaining infrastructural life. By foregrounding

these hidden forms of securing, the thesis contributes to ongoing debates in Critical Security Studies about what constitutes security and how it is practised beyond sovereign decision or visible threat (Adey et al. 2015, Amoore 2013, Anderson & Gordon 2017, Nyman 2021, Collier & Lakoff 2015). This emphasis on mundane and backgrounded techniques supports recent calls within CSS for empirically grounded, ethnographic engagements with the dispersed practices of security (Mc Cluskey et al. 2022). The methodology adopted here reflects that concern and suggests that similar approaches may be fruitful in other domains of infrastructural governance.

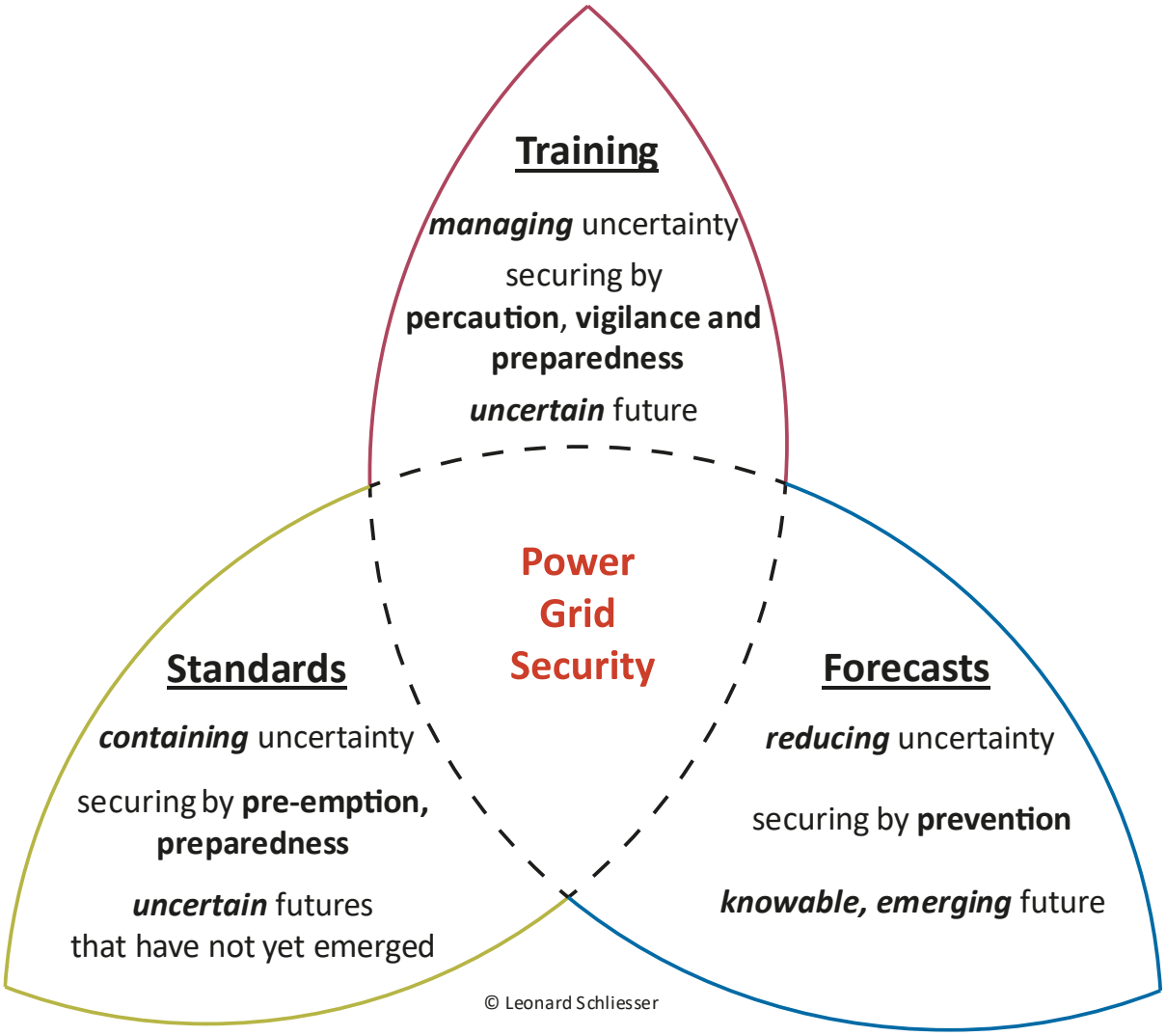


Figure 8 The Triad of Power Grid Security

7.1 Everyday Power Grid Security

With the uncertainties potentially threatening power grid security being multiple, various security techniques are required to protect the grid. Thus, this thesis argued that power grid security, in addition to formal and physical security measures, requires the integration of three independent security techniques. Standards and standardisation were discussed to contain, forecasts to reduce, and training to manage different uncertainties differently (Figure 8) and across varying bandwidths (Figure 9). While they individually secure a specific quadrant of uncertainty, it is through their combination that they can secure the power grid against a wide range of potential threats.

This thesis foregrounds the everyday as the primary space-time in which power grid security is enacted. Rather than treating the everyday as residual or unremarkable, it is here understood as the domain in which anticipatory practices are deployed, events are normalised, and catastrophic potentials are deferred. Following Anderson & Gordon (2017), Folkers (2017a) and Collier & Lakoff (2021), the everyday is the domain in which infrastructural security is primarily enacted, not through spectacle or sovereign decision, but through routines, monitoring, and preparedness. This thesis responds to calls within CSS and human geography for empirical research that makes visible the dispersed, often invisible techniques through which infrastructures are secured (Anderson & Adey 2011, Aradau et al. 2015, Collier & Lakoff 2021, Mc Cluskey et al. 2022). Power grid security is not secured through exceptional interventions but through ongoing, recursive work performed by transmission system operators (TSOs) and regional security coordinators (RSCs). Standards and standardisation pre-empt disruptions by embedding expectations; forecasts reduce uncertainty by calculating a future; and training cultivates vigilance, improvisation and the capacity to manage the unexpected. Their individual and collective goal is not to eradicate uncertainty and offer total (full) control, but to manage uncertainty to a point that is considered “safe” (cf. Mason 2022) or “safe enough” (cf. Wellock 2021). In doing so, they shape the conditions of infrastructural life and the thresholds at which exceptionality emerges.

Standards and standardisation, for example, define this level, at 3000 MW of frequency containment reserves in continental Europe (European Commission 2017a). They define the range of eventfulness and uncertainty that can be contained through pre-emption and preparedness in the event of a potential loss of power stations with around 3,000 MW of generation. A future to be desired or averted is imagined and informs present action through backcasting. By layering standards and standardisation for the everyday and the exceptional, they can cover a broader range of what might happen. Forecasts, on the other hand, aim to reveal an emerging future, thereby reducing the uncertainty of what might happen. Through preventive action, they aim to reduce what is happening within the range of standardised security techniques. Training encompasses both aspects, as it secures the correct application of standards and forecasts. It furthermore fosters experience as a distinct form of knowledge that prepares for continued operation should standards and forecasts fail to contain and reduce uncertainty. In fostering precaution and vigilance, this failure is anticipated, and its possibility is continually kept in mind.

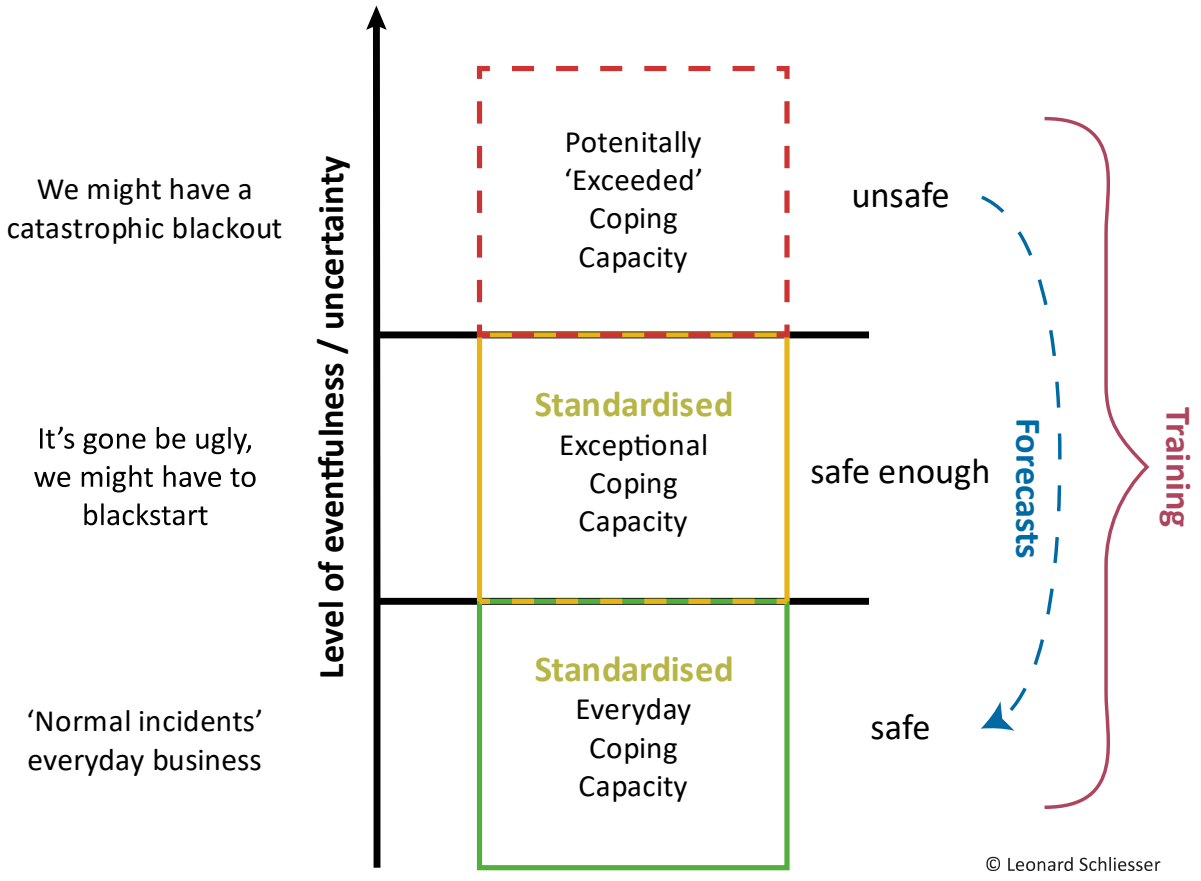


Figure 9 How Standards, Forecasts, and Training Secure

Standards and standardisation were positioned as essential security techniques for the power grid. They secure by pre-emption, by taking action in the present to avoid an imagined undesirable future through backcasting (Adam & Groves 2007). A technical component or a procedure in the present then is aligned with this to be avoided and pre-empts this future from occurring. When technical components and procedures operate within their standardised parameters, they are guaranteed (within a specified range of possible deviation) to function, creating a reliability of expectation. When standards are applied and adhered to, a future becomes known through this reliability of expectation. Uncertainty about what might happen or is to be done is contained beyond the standard.

As standards and standardisation regulate technical grid components and procedures, they promise to minimise the disruptiveness of emergent events through pre-emption. They do this by providing information about what can be expected to happen and possible responses. Through this, they coordinate and foster a unified understanding of a future. Information encoded within the standard does not need to be acquired anew each time, as what might happen has already been imagined. This then allows for the significant compression of the response interval between diagnosis and response (Anderson 2016).

This thesis argued that if standards are seen as infrastructures, what is to be expected is "learnt as part of membership" (Star 1999). For the power grid, standards are foundational. Especially technical standards and standardisation processes co-constitute the power grid and have shaped and are shaping it (Mohla 2017, Hughes 1983, Taylor 1941). The standardisation of procedures has been less explicit and primarily originates from "habituation" (Edwards 2019). Through the liberalisation of the electricity sector and correlating increasing volumes of inter-European energy exchange, the need for

and amount of procedural standardisation through European Union legislation has increased. The System Operational Guidelines (SO GL) that the European Commission (2017a) partly developed after the Emsland Case were one of the examples provided. Standards were said to be “politics by other means” (Latour 1988) and as a compromise between technocrats and a negotiated (minimal) level of security (Easterling 2016, Folkers 2017b). Their political dimension, however, was not the focus and only appeared on the sideline.

Stockpile like (cf. Folkers 2019a) standards and standardisation were discussed as pre-positioned to act both in the everyday and in the exceptional. By layering standards of different scopes, a wider bandwidth of potential events can be secured. While some standards perform in the everyday and in the exceptional, others lose or become applicable beyond the everyday. As forms of everyday securing, the European energy legislation and its actors were discussed, as well as the German standardised reserve power activation. Standards and standardisation, both technical and procedural, were shown to provide a framework through which the grid and its operation can be understood. In regulating the conduct between the transmission grid actors and the technical grid components, a reliability of expectation is formed that mitigates the risk of misunderstandings. The Emsland Case in the preface served as an example of uncoordination due to the lack of adherence to the standards at that time. Standards are only able to secure if they are applied and adhered to as intended. Nevertheless, any excessive standardisation was also discussed as a potentially limiting factor, as well as a threat to the standard's ability to secure (Hanseth et al. 2006).

Forecasts as a security technique contrasted the standard's imaginary mode of backcasting with the calculatory mode of forecasting. In the second empirical chapter, forecasts were discussed to open the possibility of preventing potential events through forecasting. Potential events become known through the forecast; the forecasts create them. Uncertainty about the likelihood of events can be lifted, and preventative action can be taken. To predict the forecast heavily relies on a past understanding of the grid and its functioning, as well as historical data that feeds models that calculate a future. The spatiotemporal horizons and the metrics forecasted are multiple. In the empirical chapters, forecasts engaging the problem of overloads from various angles were the main exemplary focus. Forecasts are stacked; they leverage different degrees of predictability to reduce the possibility of an event exceeding a standardised momentary level of ‘safe enough’. Specific long-range forecasts intend to predict, for example, where planned outages will occur and whether they have the potential to lead to overloads in the transmission grid. They are followed by medium and short-range forecasts, while their accuracy exponentially increases the closer they come to the present.

Both the German energy regulator (Bundesnetzagentur 2011, Folkers 2019b) and geographers (Bulkeley et al. 2016b, Luque 2014) assign the ‘real-time’ management/forecasting of (electrical) flows considerable importance, thus potentially questioning this thesis's focus on the forecast. To justify it, the thesis highlighted and demarcated its boundaries and the importance of forecasts, thus ‘real-time’ was first engaged. The forms of ‘real-time’ encountered in this thesis starkly differ from those attributed to ‘smart’ narratives. Firstly, I could not locate an inversion of the responsibility for the balancing of demand and generation to the individual household, which is usually attributed to ‘smart’ grids (Hodson 2023b, a, Bulkeley et al. 2014, Strengers 2013, 2012). Secondly, while the transmission grid is increasingly upgraded with digital sensors (like weather sensors on the powerline), ‘real-time’ is still primarily a legacy of highly standardised electromechanical automatisation. In providing three examples of substation protective mechanisms, reserve power activation and redispatch, ‘real-time’

was shown to be multiple. Furthermore, the border between perpetual present and future becomes conflated when including the close to' real-time'.

Three forecasts for the week ahead outage planning, the day ahead transmission capacity, and overloads were presented to highlight how forecasts work on uncertainties and secure differently. Each offered a unique temporal horizon and focused on different metrics. Yet, they were all deployed by the RSC, TSCNET, to work on and secure against potential overloads, a specific security concern in the grid. The forecasted values gained their epistemological meaning relating to the forecasted metrics and, by themselves, lacked it. Their contribution to the overall security of the grid was shown to be direct (Day Ahead Congestion Forecast) and indirect (Outage Planning Coordination/Inconsistencies and CORE Flow-Based Market-Coupling). While not a focus, the importance of the electricity market shined through in this chapter, as the forecasts partly calculated the availability of commodity (for CORE FB MC transmission capacity).

The last empirical chapter discussed training as a security technique. In contrast to standards, standardisation and forecasting, which secure by containing or reducing uncertainty about a future, training secures by managing uncertainty. It was positioned as a tool that secures in three different ways. It enables the operators and OMs to deploy pre-emption and prevention correctly. It fosters experience and, through it, experiential knowledge. The operator's expertise can provide guidance if standards and forecasts fail to contain and reduce uncertainty. The operators and OMs can switch and rely upon these different modes of knowing through their training. Lastly, training secures the power grid as it fosters precaution and vigilance. Even in the uneventful everyday, residual uncertainty remains, and training prepares the operators and OMs to stay alert and expect failure. If events and potentially catastrophic failures in embryonic form can be identified and addressed, they do not escalate or cascade into system failure, resulting in a blackout.

Through their initial and continued training, the TSO and RSC personnel are to become ‘uncertainty managers’. Their initial training builds on their formal knowledge while providing the operators and OMs with job-specific process knowledge. Furthermore, and apprenticeship-like they are to gain experience. To gain this experience securely and without endangering power grid operation, the novice OM at TSCNET had to first verbalise their intended action to their mentor. For continued training, the operators at TSOs could rely on a private simulation provider that allowed them to conduct their advanced training outside of the live power grid. In both cases, the experience gained through this trial-and-error learning provides a reference framework to fill the explanatory gaps in standardised processes should the standard's ability to contain uncertainty is exceeded. Experiential knowledge, thus, operates in both the everyday and exceptional situations.

Besides the TSO operators and TSCNET OMs, a second group of so-called contingency managers was introduced to train for the exceptional specifically. Their job focuses explicitly on fostering operational preparedness and continuity. They learn to navigate the legal requirements for their company's operational and cyber security or business continuity through training and preparing their company. However, the ability to train and build experience is limited for contingency managers, operators and OMs, as training is disruptive and resource intensive. In the triad of power grid security techniques, training is without alternative as it facilitates the grid operators and RSCs OMs encounter with and management of uncertainty.

7.2 Reflections and Limitations

This thesis has examined how power grid security is enacted through techniques that manage uncertainty in the everyday. While the empirical material offers a grounded account of how standards and standardisation, forecasting, and training operate within the German transmission grid, it is necessary to reflect on the methodological and conceptual limitations of this focus. The reflections below concern the scope of the research, the spatial assumptions it rests upon, and how these shape the thesis's contribution.

The research focused on the practices of transmission system operators (TSOs) and the regional security coordinators (RSCs). This decision reflects a deliberate focus on the organisations responsible for the everyday operation and stabilisation of the German transmission grid. The study did not include perspectives from generators, distribution system operators (DSOs), market actors, or policy bodies. While these are undoubtedly relevant, their exclusion was necessary to maintain the research's focus and empirical grounding. Exploring these other perspectives would likely have produced a more expansive but less detailed account of the specific security techniques investigated here.

To explore the question of how the power grid is secured and uncertainty is managed, an ethnographic approach was employed. The methodological choice to research power grid security primarily through a participatory and ethnographic approach allowed me to locate, visualise, and problematize its hidden everyday security techniques and practices. It enabled me to identify the key transmission grid actors involved in everyday power grid security. The operators at the transmission system operators (TSOs) and the operational managers at the regional security coordinator (RSC) are the everyday uncertainty managers who disproportionally contribute to power grid security. In conducting an ethnography at the RSC, TSCNET and participatory observation at the TSO TransnetBW, I could visualise, see and experience how they operate and secure the grid daily. The sustained ethnographic engagement with TSCNET and, to a lesser extent, the participatory observations at TransnetBW provided me with an understanding of how these actors perceive power grid security. It gave me an understanding of how and what they problematise as power grid security issues in the everyday.

This ethnographic methodology concentrated the focus of this thesis on a relatively small area and group of actors within the power system. It limited the perspective to two groups of actors, TSOs and the RSC, TSCNET and the transmission scale. It deliberately blacked out and excluded the electricity generators, distribution grid operators, con-/prosumers, and electricity markets to maintain a manageable size. The four German transmission grid operators are currently the only actors legally responsible for upholding the security of the electricity supply. Furthermore, their position within the electricity networks provided a systemic perspective that the first and second-tier distribution system operators could not have provided. Yet, the academic debates on power grid security and its transformation are primarily located at these scales (Bulkeley et al. 2014, Folkers 2019b, Lovell 2018). Focusing on the transmission scale added an overlooked perspective in the debate on power grid security. Exploring the connection between the scales and giving it space could have strengthened the research into power grid security.

At the same time, the thesis engages with how security practices operate across various spatial scales—from the national to the regional and supranational. The empirical material shows that while transmission system operators are embedded in national regulatory regimes, their operations are increasingly shaped by coordination at the European level, particularly through regional security

coordinators and regulatory bodies such as ENTSO-E and ACER. Standards and standardisation, forecasts and training function as techniques that can enable alignment across these scales. When working in a coordinated way, these security techniques can produce harmonised expectations and interoperable operational procedures across spatial scales. However, the scalar implications of these practices were not examined systematically. Although the thesis conceptually draws on biopolitics, which is often aligned with the governance of national populations, its findings suggest that what is secured is not just a nationally bounded population. Instead, what is indirectly secured are the lives that critically depend on a critical infrastructure embedded within a supranational governance framework. Future research could explore how different security imaginaries—national and supranational—interact or diverge, and how infrastructures mediate and materialise these layered forms of governance.

The methodological focus also narrowed the field of view on everyday power grid security. While deliberate, it initially complicated the research. It required a methodology sensitive enough to engage with a primarily transparent infrastructure and techniques not usually seen and discussed to secure the power grid. Furthermore, it foreclosed a deeper engagement with security against extremes, such as the blackout. While the discussed security techniques were said to secure against the uncertain but potentially catastrophic potential, the blackout in embryonic form would have required other tools and a different perspective. For example, when analysing grid restoration techniques.

The review of documents and audio-visual materials supported and prepared the ethnographic fieldwork. It provided the basic power grid (security) knowledge and the current debates within the industry. It helped narrow down possible actors to engage and provided a sense of direction in the research and the meaning of power grid security. While the review of documents and audio-visual materials was intended only as a supportive method, it could have been more structured and positioned as an independent research method. This would have opened the opportunity to use it beyond a supporting role.

The interviews provided first-hand accounts of power grid security and how uncertainty is managed. They particularly provided valuable insights into how system security is conceptualised and how the blackstart of the power grid is prepared in the everyday. Due to the Covid-19-related difficulties of acquiring interview partners they failed to be plentiful enough to provide much empirical material, as well as failed to be an entry tool and door opener to the transmission grid actors.

The literature review primarily engaged and drew out the analytical categories of ‘work on uncertainty’, ‘relates to a future’ and ‘securing by’ from a general and technical engagement with Foucauldian biopolitics. It further demarcated the general use of biopolitics from its possible mutations, i.e. necropolitics, vital system security or energopower. As Foucauldian biopolitics provided a general perspective, the engagement with the literature on uncertainty supplemented it. The illustration of the possible multiplicity of uncertainty and related security techniques was beneficial (Figure 2, Chapter 2.2) as it implied how the later security techniques were discussed to secure. Furthermore, the review of the literature is also spread out over the introduction and empirical chapters. Although this was a conscious decision due to the multiplicity of very different literature and addressed security techniques, this might have created confusion or a sense of seemingly disconnected ideas.

The thesis answered how the power grid is secured and through what security techniques. Future work on power grid security could more deeply engage with the politics behind each technique and their combination. On the one hand, this includes questions about the level of security aspired. In further developing the analysis of the empirical chapters, the question of what kind of security level is encoded in standards and standardisations, forecasting horizons and resolutions, as well as training curricula, may be raised. This might encourage further questions about who defines and deems a level of security 'secure enough'. Such an inquiry might require engaging with everyday security techniques and those for extremes, such as the blackout. On the other hand, the political dimensions of power grid security are important for current debates on the energy transition and energy system transformations. What implications does seeing grid security as the coming together of standards and standardisation, forecasting, and training have for these debates? Asking this question might suggest that the discussions of 'smart' and 'real-time' solutions for power grid security overestimate the ability to secure the grid by relying solely on flexible energy demand.

This thesis engaged with the question of how the contemporary German power grid, as a complex infrastructure and the electrical flow it enables, is secured in the everyday. It sought to understand how and through what techniques uncertainty is managed and secured in the power grid. The empirical chapters on standards and standardisation, forecasting, and training answer these questions and reflect the findings from my fieldwork. Each chapter provided examples of how the power grid is secured in the everyday. While they were addressed as individual security techniques, only in combination and being layered onto each other are sufficient to address a broad range of uncertainties and potential threats to power grid security. While the empirical depth was valuable, the narrow focus on each technique in isolation may obscure their interdependence and the broader architecture of power grid security. These reflections, however, do not undermine the empirical findings presented but clarify the specific terrain on which this thesis makes its contribution.

7.3 Outlook

In concluding this thesis, I hope it provides a foundation for further research on securing electricity infrastructures. The analysis presented here offers a situated account of transmission grid security, based on a specific set of actors, techniques, and operational settings. However, this is only a partial perspective. A more comprehensive understanding of power grid security practices would require a holistic engagement with the power infrastructure across its different scales. It would require engaging with both traditional and decentralised renewable generators, as well as prosumers, distribution grid operators, various power market participants, and national and multinational regulators to trace how security is configured, distributed, and contested across different scales and institutional sites. Such research becomes increasingly important as the electricity system is transformed by decarbonization, digitalisation, and decentralisation, and the question of what this means for power grid security remains largely unanswered.

Although this thesis initially set out to examine how security operates in the 'smart' grid, it instead encountered legacy techniques—standards and standardisation, forecasting, and training—anchored in the grid's technical and procedural domains. Whether this is a feature specific to the transmission scale or indicative of broader disjunctures between 'smart' grid imaginaries and operational realities remains an open question. Future work should critically examine how decentralised and digital infrastructures affect the rationalities, responsibilities, and techniques through which security is imagined and enacted.

This thesis has demonstrated that infrastructural security is not achieved through singular or exceptional acts of control, but through layered, distributed, and anticipatory practices that operate across the everyday. By focusing on the routines of transmission system operators and regional security coordinators, it shifts attention within Critical Security Studies from abstract threat discourses to the situated labour of securing circulations. Methodologically, it underscores the value of ethnography for revealing hidden or backgrounded practices and the practical knowledge required to govern infrastructural life. Conceptually, it introduces the figure of the "uncertainty manager" as a subject of biopolitical security, defined not by sovereign power, but by anticipatory competence, standardised responsiveness, and situated judgement. These insights open new avenues for researching how vital infrastructures are governed under conditions of systemic complexity and uncertain futures.

This thesis also foregrounds the importance of examining security as an everyday practice. While public and policy discourses often centre on catastrophic events—such as blackouts—the findings presented here show that security is enacted well before such events materialise. Security is incubated and emerges through the quiet work of pre-emption, prevention, and preparedness. Training plays a critical role in this configuration by preparing operators to navigate the different uncertainties that each of these techniques individually secures against but cannot fully resolve. These practices are anticipatory by designed to manage the multiple and often overlapping uncertainties that arise from the grid's systemic complexity. As a tightly coupled and interdependent infrastructure, the transmission system does not allow for isolated failures; even minor deviations can escalate or cascade if not appropriately addressed. The need for everyday security practices arises precisely from this complexity as they serve to contain volatility, prevent overloads, and keep grid parameters within acceptable bounds. Although these techniques lack the spectacle of emergency response, they are essential for maintaining infrastructural stability. As such, they deserve sustained critical attention, particularly when they are embedded in routines and rationalities that rarely attract public scrutiny, thus limiting democratic oversight.

This thesis contributes to Critical Security Studies by demonstrating how security is enacted through mundane, anticipatory practices embedded in the management of complex infrastructures. It shifts attention away from sovereign decisions and visible emergencies, foregrounding instead the dispersed, often overlooked techniques that govern infrastructural life on an everyday basis. These practices do not merely implement policy; they make security. Decisions about what standards define acceptable risk, which temporalities are modelled and prioritised, or how operators are trained to respond to exceptional scenarios, all carry political weight, even when framed as technical or procedural. From a biopolitical perspective, such practices matter not because they are exceptional, but because they organise how infrastructural life, and the circulations that sustain and emerge from it, are secured and made resilient through it. By making these routines visible, the thesis opens space for further CSS inquiry into how infrastructural security is produced, not through crisis response, but through the quiet calibration of what counts as normal, urgent, or actionable within systems increasingly governed by complexity and uncertainties.

Bibliography

Abram, S. 2014. The time it takes: temporalities of planning. *Journal of the Royal Anthropological Institute,* 20**,** 129-147.

Acemoglu, D. & Robinson, J. A. 2012. *Why nations fail the origins of power, prosperity and poverty,* London, Profile.

Acer 2019. Methodology for assessing the relevance of assets for outage coordination. online: Agency for the Cooperation of Energy Regulators.

Acer. n.d. *Operation Codes: Milestones* [Online]. online: Agency for the Cooperation of Energy Regulators. Available: https://www.acer.europa.eu/sites/default/files/documents/en/Electricity/OPERATION-CODES/Documents/timeline_operationcodes.pdf [Accessed 21.06.2022].

Adam, B. & Groves, C. 2007. *Future matters: action, knowledge, ethics,* Leiden, Leiden: Brill.

Adey, P. & Anderson, B. 2012. Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue,* 43**,** 99-117.

Adey, P., Anderson, B. & Graham, S. 2015. Introduction: Governing Emergencies: Beyond Exceptionality. *Theory, Culture & Society,* 32**,** 3-17.

Agamben, G. 1998. *Homo sacer. Sovereign power and bare life,* Stanford, Calif., Stanford University Press.

Agamben, G. 2005. *State of exception,* Chicago, Chicago : University of Chicago Press.

Alexandru, A., Vevera, V. & Ciupercă, E. M. 2019. National Security and Critical Infrastructure Protection. *International conference KNOWLEDGE-BASED ORGANIZATION,* 25**,** 8-13.

Altvater, E. 1994. Die Ordnung rationaler Weltbeherrschung oder: Ein Wettbewerb von Zauberlehrlingen. *PRIKLA Zeitschrift für kritische Sozialwissenschaft,* 95**,** 186-225.

Amin, A. 2013. Surviving the Turbulent Future. *Environment and Planning D: Society and Space,* 31**,** 140-156.

Amin, A. 2014. Lively Infrastructure. *Theory, Culture & Society,* 31**,** 137-161.

Amin, S. M. Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems. 2010 2010. IEEE, 1-5.

Amoore, L. 2009. Algorithmic War: Everyday Geographies of the War on Terror. *Antipode,* 41**,** 49-69.

Amoore, L. 2011. Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture & Society,* 28**,** 24-43.

Amoore, L. 2013. *The politics of possibility: risk and security beyond probability,* Durham, Duke University Press.

Amoore, L. 2014. Security and the incalculable. *Security dialogue*.

Amoore, L. & De Goede, M. 2008. *Risk and the war on terror,* London; New York, Routledge.

Amprion 2023. Schalt-und Umspannanlagen: Knotenpunkte unseres Stromnetzes. online.

Anand, N., Gupta, A. & Appel, H. 2018. *The promise of infrastructure,* Durham, Duke University Press.

Anderson, B. 2010a. Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography,* 34**,** 777-798.

Anderson, B. 2010b. Security and the Future: Anticipating the Event of Terror. *Geoforum,* 41**,** 227-235.

Anderson, B. 2016. Governing emergencies: The politics of delay and the logic of response. *Transactions of the Institute of British Geographers,* 41.

Anderson, B. 2017. Emergency futures: Exception, urgency, interval, hope. *The Sociological Review,* 65**,** 463-477.

Anderson, B. 2021. Scenes of emergency: Dis/re-assembling the promise of the UK emergency state. *Environment and Planning C: Politics and Space,* 39**,** 1356-1374.

Anderson, B. & Adey, P. 2011. Affect and Security: Exercising Emergency in 'UK Civil Contingencies'. *Environment and Planning D: Society and Space,* 29**,** 1092-1109.

Anderson, B. & Adey, P. 2012. Governing events and life: 'Emergency' in UK Civil Contingencies. *Political Geography,* 31**,** 24-33.

Anderson, B. & Gordon, R. 2017. Government and (non)event: the promise of control. *Social & Cultural Geography,* 18**,** 158-177.

Anderson, B., Grove, K., Rickards, L. & Kearnes, M. 2020. Slow emergencies: Temporality and the racialized biopolitics of emergency governance. *Progress in Human Geography,* 44**,** 621-639.

Anderson, B. & Harrison, P. 2011. *Taking-Place: Non-Representational Theories and Geography,* Farnham, Routledge.

Aradau, C. 2010. Security that matters: Critical infrastructure and objects of protection. *Security Dialogue,* 41**,** 491-514.

Aradau, C. & Blanke, T. 2010. Governing Circulation: A critique of the biopolitics of security. *In:* DE LARRINAGA, M. & DOUCET, M. G. (eds.) *Security and Global Governmentability: Globalization, Governance and the State.* Routledge.

Aradau, C., Huysmans, J., Neal, A. W. & Voelkner, N. 2015. *Critical security methods : new frameworks for analysis*, Abingdon, Oxon : Routledge.
Aradau, C. & Van Munster, R. 2007. Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future. *European Journal of International Relations,* 13**,** 89 - 115.
Aradau, C. & Van Munster, R. 2011. *Politics of catastrophe: genealogies of the unknown,* London, New York, Routledge.
Aradau, C. & Van Munster, R. 2012. The Time/Space of Preparedness. *Space and Culture,* 15**,** 109 - 98.
Attenberg, R. H. 2009. *Global energy security,* New York, Nova Science Publishers.
Atug, M. 2022. Datenschutzmanagement. online.
Barnett, J. 2001. *The meaning of environmental security: ecological politics and policy in the new security era,* London, Zed.
Barry, A. 2001. *Political machines: governing a technological society,* London, Athlone.
Barry, T. 2011. *Border wars,* Cambridge, Mass, MIT Press.
Beck, U. 1992. *Risk society towards a new modernity,* London, Sage Publications.
Bennetto, J. 1997. How IRA plotted to switch off London. *Independent*, 11.04.1997.
Berlant, L. G. 2016. The commons: Infrastructures for troubling times. *Environment and Planning D: Society and Space,* 34**,** 393-419.
Bernstein, P. L. 1998. *Against the gods: The remarkable story of risk,* New York, NY, Wiley.
Bierhoff, H.-W. & Rohmann, E. 2017. Diffusion von Verantwortung. *In:* HEIDBRINK, L., LANGBEHN, C. & LOH, J. (eds.) *Handbuch Verantwortung.* Wiesbaden: Springer Fachmedien Wiesbaden.
Bijker, W. E. 1995. *Of bicycles, bakelites, and bulbs: toward a theory of sociotechnical change,* Cambridge, Mass., MIT.
Bijker, W. E., Hughes, T. P. & Pinch, T. 1993. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, The MIT Press.
Boin, A. & Mcconnell, A. 2007. Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management,* 15**,** 50-59.
Bonß, W. 2013. Risk. Dealing with Uncertainty in Modern Times. *Social Change Review,* 11**,** 7-36.
Bowker, G. C., Elyachar, J., Kornberger, M., Mennicken, A., Miller, P., Nucho, J. R. & Pollock, N. 2019. Introduction to Thinking Infrastructures. *In:* KORNBERGER, M., BOWKER, G. C., ELYACHAR, J., MENNICKEN, A., MILLER, P., NUCHO, J. R. & POLLOCK, N. (eds.) *Thinking Infrastructures.* Emerald Publishing Limited.
Boyer, D. 2014. Energopower: An Introduction. *Anthropological Quarterly,* 87**,** 309-333.
Bridge, G., Barr, S., Bouzarovski, S., Bradshaw, M., Brown, E., Bulkeley, H. & Walker, G. 2018. *Energy and society a critical perspective,* Abingdon, Oxon, Routledge.
Brown, G., Carlyle, M., Salmerón, J. & Wood, R. 2006. Defending Critical Infrastructure. *Interfaces,* 36**,** 530-544.
Browne, S. 2010. Digital Epidermalization: Race, Identity and Biometrics. *Critical Sociology,* 36**,** 131-150.
Browne, S. 2015. *Dark matters: on the surveillance of blackness,* Durham Duke University Press.
Bruijne, M. & Eeten, M. 2007. Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingency and Crisis Management,* 15**,** 19–29.
Brunsson, N. & Jacobsson, B. 2002a. The Pros and Cons of Standardization — An Epilogue. *A World of Standards.* Oxford: Oxford University Press.
Brunsson, N. & Jacobsson, B. 2002b. *A World of Standards*, Oxford University Press.
Bulkeley, H., Mcguirk, P. M. & Dowling, R. 2016a. Making a smart city for the smart grid? The urban material politics of actualising smart electricity networks. *Environment and Planning A,* 48**,** 1709-1726.
Bulkeley, H., Powells, G. & Bell, S. 2014. Smart grids and the governing of energy use: reconfiguring practices? *Social practices, interventions and sustainability: beyond behaviour change.* London, New York: Routledge.
Bulkeley, H., Powells, G. & Bell, S. 2016b. Smart grids and the constitution of solar electricity conduct. *Environment and Planning A: Economy and Space,* 48**,** 7-23.
Bundesamt Für Bevölkerungsschutz Und Katastrophenhilfe (ed.) 2015. *Autarke Notstromversorgung der Bevölkerung unterhalb der KRITIS-Schwelle*: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).
Bundesamt Für Bevölkerungsschutz Und Katastrophenhilfe (ed.) 2019. *Notstromversorgung in Unternehmen und Behörden*: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).
Bundesamt Für Sicherheit in Der Informationstechnik 2009. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz). *BSIG.* online.

Bundesamt Für Sicherheit in Der Informationstechnik 2016. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV). online: Bundesministerium der Justiz.
Bundesanstalt Für Materialforung Und -Prüfung, B. 2006. Schadensanalzse an im Münsterland umgebrochenen Strommasten.
Bundesministerium Des Inneren 2005. Schutz Kritischer Infrastruktur - Basisschutzkonzept. online.
Bundesnetzagentur 2011. "Smart Grid" und "Smart Market": Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems online.
Bundesnetzagentur 2017. Flexibilität im Stromversorgungssystem. online.
Bundesnetzagentur. 2023. *Kennzahlen der Versorgungsunterbrechungen Strom* [Online]. online. Available: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/start.html [Accessed 10.07.2024].
Burger, B. 2024. Electricity generation in Germany in 2023. Fraunhofer ISE.
Campbell, D. 1998a. *Writing security United States foreign policy and the politics of identity,* Minneapolis, University of Minnesota Press.
Campbell, D. 1998b. *Writing Security: United States Foreign Policy and the Politics of Identity,* Minneapolis, University of Minnesota Press.
Carnes, W. E. 2011. Highly Reliable Governance of Complex Socio-Technical Systems. *Deepwater Horizon Study Group*.
Carse, A. 2016. Keyword Infrastructure: How a humble French engineering term shaped the modern world. *In:* HARVEY, P., JENSEN, C. B. & MORITA, A. (eds.) *Infrastructure and social complexity: A Companion.* London, New York: Routledge.
Chandler, D. 2014a. Beyond neoliberalism: resilience, the new art of governing complexity. *Resilience,* 2**,** 47-63.
Chandler, D. 2014b. *Resilience: the governance of complexity,* Oxfordshire, England, Routledge.
Chandrashekeran, S. 2022. Energopower, statecraft and political legitimacy. *Environment and Planning E: Nature and Space,* 5**,** 1788-1806.
Cisotto, G. & Badia, L. Cyber Security of Smart Grids Modeled Through Epidemic Models in Cellular Automata. 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 21-24 June 2016 2016 Coimbra, Portugal online: IEEE.
Clausewitz, C. V. 1976. *On war,* Princeton, N.J, Princeton, N.J: Princeton University Press.
Clinton, W. J. 1996. Executive Order EO 13010 Critical Infrastructure Protection. The White House.
Clinton, W. J. 1998. Presidential Decision Directive/NSC-63 Critical Infrastructure Protection. *In:* HOUSE, T. W. (ed.).
Coaffee, J. & Clarke, J. 2016. Critical infrastructure lifelines and the politics of anthropocentric resilience. *Resilience,* 5**,** 161-181.
Coaffee, J., Wood, D. M. & Rogers, P. 2009. *The everyday resilience of the city: How cities respond to terrorism and disaster,* New York, Palgrave Macmillan.
Cohendet, P. & Amin, A. 2004. *Architectures of Knowledge: Firms, Capabilities, and Communities,* Oxford, Oxford University Press.
Collier, S. J. 2008. Enacting catastrophe: preparedness, insurance, budgetary rationalization. *Economy and Society,* 37**,** 224-250.
Collier, S. J. & Lakoff, A. 2008. The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem. *In:* DUNN, M. & KRISTENSEN, S. (eds.) *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation.* Routledge.
Collier, S. J. & Lakoff, A. 2015. Vital Systems Security: Reflexive Biopolitics and the Government of Emergency. *Theory, Culture & Society,* 32**,** 19-51.
Collier, S. J. & Lakoff, A. 2021. *The Government of Emergency: Vital Systems, Expertise, and the Politics of Security*, Princeton University Press.
Colvile, R. 2006. Decade that dimmed - the strike- hit Seventies. *The Thelegraph*, 2006.
Conner, S. The Good News About Nuclear Destructions. Doctors for Disaster Preparedness 2020 Conference, 2020.
Consentec 2022. Beschreibung von Konzepten des Szstemausgleichs und der Regelreservemärkte in Deutschland. *In:* ÜBERTRAGUNGSNETZBETREIBER, D. (ed.). online.
Cooper, M. 2006. Preempting Emergence: The Biological Turn in the War on Terror. *THEORY CULTURE AND SOCIETY,* 23**,** 1-24.
Cooper, M. 2008. *Life as surplus: biotechnology and capitalism in the neoliberal era,* Seattle, Wash., University of Washington Press.

Coreso. 2024. *Outage Planning Coordination* [Online]. Available: https://www.coreso.eu/services/opc/ [Accessed 14.08.2024].
Coward, M. 2009. Network-Centric Violence, Critical Infrastructure and the Urbanization of Security. *Security Dialogue,* 40**,** 399-418.
Cowen, D. 2010. A Geography of Logistics: Market Authority and the Security of Supply Chains. *Annals of the Association of American Geographers,* 100**,** 600-620.
Cross, J. 2017. Off the grid: Infrastructure and energy beyond the mains. *In:* HARVEY, P., JENSEN, C. & MORITA, A. (eds.) *Infrastructures and Social Complexity: A Companion.* London: Routledge.
Cutter, S. L. 2016. Resilience to What? Resilience for Whom? *Geographical Journal,* 182**,** 110-113.
Dalby, S. 2002. *Environmental security,* Minneapolis, Minn, University of Minnesota Press.
Dalby, S. 2022. *Rethinking Environmental Security,* Cheltenham, UK, Edward Elgar Publishing.
De Goede, M. & Randalls, S. 2009. Precaution, Preemption: Arts and Technologies of the Actionable Future. *Environment and Planning D: Society and Space,* 27**,** 859-878.
De Goede, M., Simon, S. & Hoijtink, M. 2014. Performing preemption. *Security Dialogue,* 45**,** 411-422.
De Lange, M. 2018a. From real-time city to asynchronicity: exploring the real-time smart city dashboard. *In:* LAMMES, S., PERKINS, C., GEKKER, A., HIND, S., WILMOTT, C. & EVANS, D. (eds.) *Time for Mapping: Cartographic Temporalities.* Manchester University Press.
De Lange, M. 2018b. From real-time city to asynchronicity: Exploring the real-time smart city dashboard. *In:* HIND, S., PERKINS, C., GEKKER, A., EVANS, D., LAMMES, S. & WILMOTT, C. (eds.) *Time for mapping.* Manchester, England: Manchester University Press.
Debruler, D. 2018. *High-Strength bolts replaced rivets during the 1960s and 70s* [Online]. online,: Industrial History, Blogspot. Available: https://industrialscenery.blogspot.com/2018/05/high-strength-bolts-replaced-rivets.html [Accessed 25.05.2022 2022].
Department of Homeland Security 2002. Natiolal Strategy for Homeland Security. online.
Department of Homeland Security 2007. Natioal Strategy for Homeland Security. online.
Department of Homeland Security 2010. DHS Risk Lexicon. Washington, DC: US Department of Homeland Security.
Der Derian, J. 1992. *Anti Diplomacy,* Oxford, Blackwell.
Der Derian, J. 2009. *Virtuous War,* 2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN, Routledge.
Deutscher Bundestag 2005. Energiewirtschaftsgesetz.
Deutsches Institut Für Normung 2011. DIN EN 60034-1 Rotating electrical machines. VDE Verlag.
Dewalt, K. M. & Dewalt, B. R. 2011. *Participant observation a guide for fieldworkers,* Lanham, Md, Rowman & Littlefield.
Dillon, M. 2007. Governing through contingency: The security of biopolitical governance. *Political Geography,* 26**,** 41-47.
Dillon, M. 2008. Underwriting security. *Security Dialogue,* 39**,** 309-332.
Dillon, M. & Lobo-Guerrero, L. 2008. Biopolitics of security in the 21st century: an introduction. *Rev. Int. Stud.,* 34**,** 265-292.
Dillon, M. & Reid, J. 2009. *The liberal way of war killing to make life live,* London, Routledge.
Dunning, D. 2011. Chapter five - The Dunning–Kruger Effect: On Being Ignorant of One's Own Ignorance. *In:* OLSON, J. M. & ZANNA, M. P. (eds.) *Advances in Experimental Social Psychology.* Academic Press.
Dutrain. 2022. *Independent Training & Service Centre for Power System Control* [Online]. online. Available: www.dutrain.de [Accessed 04.04.2022].
Easterling, K. 2016. *Extrastatecraft: The Power of Infrastructure Space*, London: Verso.
Ebrahimy, R. & Pourmirza, Z. Cyber-interdependency in Smart Energy Systems. Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 2017. SCITEPRESS - Science and Technology Publications, 529–537.
Edwards, M. 2014. *Critical infrastructure protection,* Amsterdam, IOS Press.
Edwards, P. N. 2003. Infrastructure and modernity: force, time, and social organization in the history of sociotechnical systems. *In:* MISA, T. & BREY, P. (eds.) *Modernity and Technology.* Cambridge, MA: MIT Press.
Edwards, P. N. 2019. Infrastructuration: On Habits, Norms and Routines as Elements of Infrastructure. *In:* KORNBERGER, M., BOWKER, G. C., ELYACHAR, J., MENNICKEN, A., MILLER, P., NUCHO, J. R. & POLLOCK, N. (eds.) *Thinking Infrastructures.* Emerald Publishing Limited.
Edwards, P. N., Jackson, S. J., Chalmers, M. K., Bowker, G. C., Borgman, C. L., Ribes, D., Burton, M. & Calcert, S. 2012. Knowledge Infrastructures: Intellectual Frameworks and Research Challenges. University of Michigan School of Information.

Elnaga, A. & Imran, A. 2013. The Effect of Training on Employee Performance. *European Journal of Business and Management,* 5**,** 11.
Elsberg, M. 2012. *Blackout: Morgen ist es zu spät*, Blanvalet Verlag.
Enbw. 2024. *Umspannerk - die Knoten in unseren Stromnetzen* [Online]. online. Available: https://www.enbw.com/unternehmen/themen/netze/umspannwerke.html [Accessed 23.04.2025].
Endsley, M. R. 2006. Expertise and Situation Awareness. *In:* ERICSSON, K. A., CHARNESS, N., FELTOVICH, P. J. & HOFFMAN, R. R. (eds.) *The Cambridge Handbook of Expertise and Expert Performance.* Cambridge: Cambridge University Press.
Engeström, Y. 1990. *Learning, Working, and Imagining: Twelve studies in active theory,* Helsinki.
Entso-E 2012. Special Protection Schemes. online.
Entso-E 2015. Quality of datasets and calculations for system operations third edition. online: European Network of Transmission System Operators for Electricity.
Entso-E 2017. Explanatory note DA FB CC methodology for CORE CCR. online: European Network of Transmission System Operations for Electricity.
Entso-E 2019. Explainer services by RSCs and ENTSO-E *Playlist.* YouTube.
Entso-E 2021a. 1 Core Consultative Group Meeting 22 04 2021 Conference call. YouTube.
Entso-E 2021b. Continental Europe Synchronous Area Separation on 08 January 2021. online.
Entso-E 2021c. Continental Europe Synchronous Area Separation on 08 January 2021 ICS Investigation Expert Panel » Final Report » 15 July 2021 Main Report. online: European Network of Transmission System Operations for Electricity.
Entso-E 2021d. European Resource Adequacy Assessment: 2021 Edition. online.
Entso-E 2021e. European Resource Adequacy Assessment: 2021 Edition Annex 3: Methodology. online.
Entso-E 2022a. System Defence Plan. online: European Network of Transmission System Operators for Electricity.
Entso-E. 2022b. *Website of ENTSO-E* [Online]. Available: https://www.entsoe.eu/ [Accessed 21.02.2022].
Entso-E. 2023. *ENTSO-E Map* online: European Network of Transmission System Operators.
Entso-E. 2024a. *Capacity Calculation Regions* [Online]. online: European Network of Transmission System Operations for Electricity. Available: https://www.entsoe.eu/network_codes/ccr-regions/ [Accessed 15.08.2024].
Entso-E. 2024b. *Manually Activated Reserves Initiative (MARI)* [Online]. online. Available: https://www.entsoe.eu/network_codes/eb/mari/ [Accessed 09.08.2024].
Entso-E. 2024c. *PICASSO* [Online]. online. Available: https://www.entsoe.eu/network_codes/eb/picasso/ [Accessed 09.08.2024].
Entso-E. 2024d. *Single Day-Ahead Coupling (SDAC)* [Online]. online: European Network of Transmission System Operations for Electricity. Available: https://www.entsoe.eu/network_codes/cacm/implementation/sdac/ [Accessed 15.08.2024].
Erkens, H. 2018. Staat extrem: Der Ausweichsitz als Anschauungsobjekt rechtlicher Resilienz im Ausnahmezustand. *In:* JÄGER, T., DAUN, A. & FREUDENBERG, D. (eds.) *Politisches Krisenmanagement: Band 2: Reaktion – Partizipation – Resilienz.* Wiesbaden: Springer Fachmedien Wiesbaden.
Esposito, R. 2011. *Immunitas: the protection and negation of life*.
European Commission 2006a. Communication from the Commission on a European Programme for Critical Infrastructure Protection. *COM(2006) 786.* online: EURLEX.
European Commission 2006b. The European Programme for Critical Infrastructure Protection (EPCIP). online.
European Commission 2008. Green Paper on Territorial Cohesion. Turning Territorial Diversity into Strength. Brussels: Commission of the European Union,.
European Commission 2015. Energy Union Package. *COM(2015) 80 final.* online: EUR-Lex.
European Commission 2016a. Clean Energy For All Europeans. *COM(2016) 860.* online EUR-Lex.
European Commission 2016b. Commission Regulation (EU) 2016/631 of 14 April 2016 establishing a network code on requirements for grid connection of generators. online: EUR-Lex.
European Commission 2017a. Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation. *EU 2017/1485.* online: EUR-Lex.
European Commission 2017b. Commission Regulation (EU) 2017/2195 of 23 November 2017 establishing a guideline on electricity balancing. *(EU) 2017/2195.* online: EUR-Lex.
European Commission 2017c. Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration. *2017/2196.* online: EUR-Lex.
European Commission 2017d. Commission Staff Working Document Impact Assessment, accompanying the docoument ... establishing a Guideline on Electricity Balancing *SWD/2017/0383 final.* EURLex.

European Commission 2019. *Clean energy for all Europeans,* Luxembourg, Publication Office of the European Union.
European Commission 2023. State of the Energy Union Report 2023. *COM(2023) 650 final.* EURLex.
European Parliament & Council of the European Union 2009a. Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC. *32009L0073.* online.
European Parliament & Council of the European Union 2009b. Regulation (EC) No 713/2009 Of the European Parliament and of the Council of 13 July 2009 establishing an Agency for the Cooperation of Energy Regulators. Official Journal of the European Union.
European Parliament & Council of the European Union 2009c. Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003. online: EUR-LEX.
European Parliament & Council of the European Union 2009d. Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003 (1). online: EUR-Lex.
European Parliament & Council of the European Union 2016. Directive (EU) 2016/1148 Concertning measures for a high common level of security of network and information systems across the Union. online: Official Journal of the European Union.
European Parliament & Council of the European Union 2019a. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast) *2019/944.* online: EUR-Lex.
European Parliament & Council of the European Union 2019b. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. *2019/941* online: EUR-Lex.
European Parliament & Council of the European Union 2019c. Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulators. *2019/942.* online: EUR-Lex.
European Parliament & Council of the European Union 2019d. Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity. *2019/943.* online: EUR-Lex.
Ewald, F. 1991. Insurance and Risk. *In:* BURCHELL, G. & FOUCAULT, M. (eds.) *The Foucault effect.* [Nachdr.] ed. Chicago, Ill.: Univ. of Chicago Press.
Ewald, F. 1993. Two Infinities of Risk. *In:* MASSUMI, B. (ed.) *The Politics of Everyday Fear.* Minneapolis, London: University of Minnesota Press.
Folkers, A. 2017a. Continuity and catastrophe: business continuity management and the security of financial operations. *Economy and Society,* 46**,** 103-127.
Folkers, A. 2017b. Existential provisions: The technopolitics of public infrastructure. *Environment and Planning D: Society and Space,* 35**,** 855-874.
Folkers, A. 2018. *Das Sicherheitsdispositiv der Resilienz : Katastrophische Risiken und die Biopolitik vitaler Systeme*, Frankfurt am Main : Campus Verlag.
Folkers, A. 2019a. Freezing time, preparing for the future: The stockpile as a temporal matter of security. *Security Dialogue,* 50**,** 493-511.
Folkers, A. 2019b. Smart Grids and Smart Markets: the Promises and Politics of Intelligent Infrastructures.
Forman, P. J. 2017. *Securing Natural Gas: Entity-Attentive Security Research.* PhD, Durham University.
Forman, P. J. 2018. Circulations beyond nodes: (in)securities along the pipeline. *Mobilities,* 13**,** 231-245.
Forman, P. J. 2020. Security and the Subsurface: Natural Gas and the Visualisation of Possibility Spaces. *Geopolitics: Subterranean Geopolitics,* 25**,** 143-166.
Forsthoff, E. 1938. *Die Verwaltungs als Leistungsträger,* Stuttgart, Berlin, Kohlhammer.
Foster, J. S., Gjelde, E., Graham, W., Hermann, R., Kluepfel, H., Lawson, R., Soper, G., Wood, L. & Woodard, J. 2004. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume 1: Executive Report.
Foucault, M. 1978. *The History of Sexuality: Volume 1 An Introduction,* New York, Pantheon Books.
Foucault, M. 1984. *The Foucault reader,* New York, New York: Pantheon Books.
Foucault, M. 1991. *Discipline and punish : the birth of the prison,* Harmondsworth, Penguin.
Foucault, M. 2003. *Society must be defended: Lectures at the Collège de France, 1975 - 76,* New York, Picador.
Foucault, M. 2005. *The Hermeneutics of the Subject: Lectures at the College de France 1981-1982,* New York, Palgrave Macmillan.

Foucault, M. 2007. *Security, territory, population: lectures at the Collège de France: 1977-78,* Basingstoke, Basingstoke: Palgrave Macmillan.
Foucault, M. 2008. *The Birth of Biopolitics: Lectures at the Collège de France, 1978-1979,* London, Palgrave Macmillan UK.
Franke, U. 2019. It is time for Germans to talk about Sicherheitspolitik. *War on the Rocks*.
Franke, U. 2021. A Millennial considers the new German problem after 30 years of peace. *War on the Rocks*.
Fukuyama, F. 1989. The End of History? *The National Interest*, 3-18.
Galloway, A. & Thacker, E. 2004. Protocol, Control, and Networks. *Grey Room*, 6-29.
Galloway, A. R. 2004. *Protocol: how control exists after decentralization,* Cambridge, Massachusetts, London, England, MIT Press.
Gandy, M. 2005. Cyborg Urbanization: Complexity and Monstrosity in the Contemporary City. *International Journal of Urban and Regional Research,* 29, 26-49.
Geist, E. M. 2019. *Armageddon Insurance: Civil Defense in the United States and Soviet Union, 1945-1991,* Chapel Hill, The University of North Carolina Press.
Gekker, A. & Hind, S. 2019. Infrastructural surveillance. *New Media & Society*, 1461444819879426.
Ghamari-Tabrizi, S. 2005. *The worlds of Herman Kahn : the intuitive science of thermonuclear war,* Cambridge, MA, Harvard University Press.
Giddens, A. 1990. *The consequences of modernity,* Stanford, Stanford University Press.
Goode, E. 2014. Labeling Theory. *In:* BRUINSMA, G. & WEISBURD, D. (eds.) *Encyclopedia of Criminology and Criminal Justice.* New York, NY: Springer New York.
Graham, S. 2005. Switching cities off. *City,* 9, 169-194.
Graham, S. 2010. *Disrupted cities: When infrastructure fails,* New York, New York: Routledge.
Graham, S. & Marvin, S. 2001. *Splintering urbanism: networked infrastructures, technological mobilities and the urban condition,* London, New York, Routledge.
Gridradar.Net. 2020. *Influence of football on mains frequency* [Online]. online. Available: https://gridradar.net/en/blog/2 [Accessed 21.10.2022].
Gridradar.Net. 2021. *Analysis: the periodic patterns of the network frequency* [Online]. online. Available: https://gridradar.net/en/blog/1 [Accessed 21.10.2022].
Griffith, T. E. J. 1994. *Strategic Attack of National Electrical Systems.* Air University Press.
Grosz, E. 2004. *The Nick of Time: Politics, Evolution and the Untimely*, Duke University Press.
Grove, K. 2013. On Resilience Politics: From Transformation to Subversion. *Resilience,* 1, 146-153.
Grove, K. 2018. *Resilience,* London; New York, Routledge Taylor & Francis Group.
Hacking, I. 1990. *The taming of chance,* Cambridge, Cambridge Univ. Press.
Hagen, J. J. 2016. Queering women, peace and security. *International Affairs (Royal Institute of International Affairs 1944-),* 92, 313-332.
Hahn, R. 2017. The origin of Schuko. Available: https://www.plugsocketmuseum.nl/Schuko-Origin_v2.pdf [Accessed 15.06.2022].
Hans, J. 2021. Offenbar gezielter Brandanschlag auf Infrastruktur. *Süddeutsche Zeitung*.
Hanseth, O. 2001. Gateways—just as important as standards: How the internet won the "religious war" over standards in Scandinavia. *Knowledge, Technology & Policy,* 14, 71-89.
Hanseth, O., Jacucci, E., Grisot, M. & Aanestad, M. 2006. Reflexive standardization: Side effects and complexity in standard making. *MIS Quarterly: Management Information Systems,* 30, 563-581.
Haraway, D. J. 2016. A Cyborg Manifesto: Science, Technology and Socialist-Feminism in the Late Twentieth Century. University of Minnesota Press.
Harvey, D. 1990. *The condition of postmodernity: an enquiry into the origins of cultural change,* Oxford, Basil Blackwell.
Harvey, P. & Knox, H. 2012. The Enchantments of Infrastructure. *Mobilities: Roads & Anthropology,* 7, 521-536.
Haupt, F. 2024. Das Ziel war ein Blackout bei Tesla. *Frankfurter Allgemeine*, 05.03.2024.
Heinzen, B. 2004. Surviving uncertainty. *Development,* 47, 4.
Herz, J. H. 1950. Idealist Internationalism and the Security Dilemma. *World Politics,* 2, 157-180.
Hiermaier, S., Gebbeken, N., Klaus, M. & Stolz, A. (eds.) 2017. *Gefährdung, dynamische Analyse und Schutzkonzepte für bauliche Strukturen* Fraunhofer Verlag.
Hinchliffe, S. 2000. Performance and Experimental Knowledge: Outdoor Management Training and the End of Epistemology. *Environment and Planning D: Society and Space,* 18, 575-595.
Hinchliffe, S. & Lavau, S. 2013. Differentiated Circuits: The Ecologies of Knowing and Securing Life. *Environment and Planning D: Society and Space,* 31, 259-274.
Hodson, H. 2023a. The electricity grid is about to be transformed. *The Economist*.

Hodson, H. 2023b. The physics of rotating masses can no longer define the electric grid. *The Economist*.
Hofinger, G. & Heimann, R. (eds.) 2016. *Handbuch Stabsarbeit: Führungs- und Krisenstäbe in Einsatzorganisationen, Behörden und Unternehmen,* Berlin, Heidelberg: Springer.
Holmberg, J. & Robert, K. H. 2000. Backcasting — a framework for strategic planning. *International Journal of Sustainable Development & World Ecology,* 7**,** 291-308.
Howe, C., Lockrem, J., Appel, H., Hackett, E., Boyer, D., Hall, R., Schneider-Mayerson, M., Pope, A., Gupta, A., Rodwell, E., Ballestero, A., Durbin, T., El-Dahdah, F., Long, E. & Mody, C. 2015. Paradoxical Infrastructures: Ruins, Retrofit, and Risk. *Science, Technology, & Human Values,* 41**,** 547-565.
Hughes, T. P. 1983. *Networks of power: Electrification in Western society, 1880 - 1930,* Baltimore, Md., John Hopkins Univ. Press.
Ieee 2021. IEEE Draft Guide for Physical Security of Electric Power Substations. *IEEE P1402/D11, June 2021***,** 1-40.
International Electrotechnical Commission 2022. Uninterruptible power system (UPS) online: International Electrotechnical Commission.
International Grid Controle Cooperation 2019. IGCC Regular Report on Social Welfare Q1 2019. online.
Jacobsson, B. 2002. 3 Standardization and Expert Knowledge. *In:* BRUNSSON, N. & JACOBSSON, B. (eds.) *A World of Standards.* Oxford: Oxford University Press.
Jasanoff, S. 2010. Beyond Calculation: A Democratic Response to Risk. *In:* LAKOFF, A. (ed.) *Disaster and the politics of intervention.* New York: Columbia University Press.
Jenny, R., Elizabeth, S. & Jacopo, T. 2019. *Energy Fables: Challenging Ideas in the Energy Sector*, Taylor and Francis.
Jonas, H. 1984. *The imperative of responsibility: in search of an ethics for the technological age,* Chicago, University of Chicago Press.
Karimi, S., Musilek, P. & Knight, A. M. 2018. Dynamic thermal rating of transmission lines: A review. *Renewable and Sustainable Energy Reviews,* 91**,** 600-612.
Kavalski, E. 2009. Timescapes of Security: Clocks, Clouds, and the Complexity of Security Governance. *World Futures,* 65**,** 527-551.
Kearny, C. H. 1987. *Nuclear War Survival Skills,* Cave Junction, Oregon, Oregon Institute of Science and Medicine.
Kellert, S. H. 1993. *In the wake of chaos unpredictable order in dynamical systems,* Chicago, University of Chicago Press.
Kemmer, L., Kühn, A., Otto, B. & Weber, V. 2021. Standby: Organizing modes of in|activity. *Ephemera,* 21**,** 1-20.
Keohane, R. O. & Nye, J. S. 2000. Globalization: What's New? What's Not? (And So What?). *Foreign Policy***,** 104-119.
Kissinger, H. A. 1977. *American Foreign Policy*.
Kitchin, R. 2014. The real-time city? Big data and smart urbanism. *GeoJournal,* 79**,** 1-14.
Kitchin, R. 2019. The Timescape of Smart Cities. *Annals of the American Association of Geographers,* 109**,** 775-790.
Klinger, C., Mehdianpour, M., Klingbeil, D., Bettge, D., Häcker, R. & Baer, W. 2011. Failure analysis on collapsed towers of overhead electrical lines in the region Münsterland (Germany) 2005. *Engineering failure analysis,* 18**,** 1873-1883.
Knox, H. 2017. Affective infrastructures and the political imagination. *Public Culture,* 29**,** 363-384.
Kraiger, K. 2003. Perspectives on Training and Development. *Handbook of Psychology.*
Kühn, A. 2021. Infrastructural standby: Caring for loose relations. *Ephemera,* 21**,** 121-139.
Lakoff, A. 2007. Preparing for the next emergency. *Public Culture,* 19**,** 247.
Lakoff, A. 2008. The Generic Biothreat, or how we became Unprepared. *Cultural anthropology,* 23**,** 399-428.
Lakoff, A. 2017. *Unprepared*

Global Health in a Time of Emergency, University of California Press.
Lakoff, A. 2020. "The Supply Chain Must Continue": Becoming Essential in the Pandemic Emergency.
Lakoff, A. & Klinenberg, E. 2010. Of risk and pork: urban security and the politics of objectivity. *Renewal and Critique in Social Theory,* 39**,** 503-525.
Lampland, M. & Star, S. L. 2009. *Standards and their stories: how quantifying, classifying, and formalizing practices shape everyday life,* Ithaca, Cornell University Press.
Land Baden-Württemberg 2017. Verwaltungsvorschrift Technische Baubestimmungen − VwV TB. *In:* WIRTSCHAFTSMINISTERIUM, L.-U.-U. (ed.). online.
Land Baden-Württemberg 2019. Landesbauordnung für Baden-Württemberg (LBO). online.

Laporte, T. R. 2007. Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise. *Journal of Contingencies and Crisis Management,* 15**,** 60-64.
Laporte, T. R. & Consolini, P. M. 1991. Working in practice but not in theory: Theoretical challenges of "high-reliability organizations". *Journal of Public Administration Research and Theory,* 1**,** 19-48.
Larkin, B. 2013. The Politics and Poetics of Infrastructure. *Annual Review of Anthropology,* 42**,** 327-343.
Latour, B. 1987. *Science in action: how to follow scientists and engineers through society,* Milton Keynes, Open University Press.
Latour, B. 1988. How to Write 'The Prince' for Machines as well as for Machination. *In:* ELLIOTT, B. (ed.) *Technology and Social Change.* Edinburgh University Press.
Lawhon, M., Nilsson, D., Silver, J., Ernstson, H. & Lwasa, S. 2018. Thinking through heterogeneous infrastructure configurations. *Urban Studies,* 55**,** 720-732.
Le Coze, J.-C. 2020. *Post Normal Accident : Revisiting Perrow's Classic,* Milton, UNITED KINGDOM, Taylor & Francis Group.
Lecompte, M. D. & Schensul, J. J. 2010. *Designing and Conducting Ethnographic Research: An Introduction,* California, AltaMira Press.
Lehtonen, M. & Nye, S. 2009. History of electricity network control and distributed generation in the UK and Western Denmark. *Energy Policy,* 37**,** 2338-2345.
Lessig, L. 2006. *Code: And Other Laws of Cyberspace,* New York, New York: Basic Books.
Little, R. G. 2002. Toward more robust infrastructure: Observations on improving the resilience and reliability of critical systems. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences.* IEEE.
Little, R. G. 2004. Holistic Strategy for Urban Security. *Journal for Infrastructure Systems (ASCE),* 10.
Lobo-Guerrero, L. 2012. *Insuring security: biopolitics, security, and risk,* London, London: Routledge.
Lobo-Guerrero, L. 2013. *Insuring Life: Value, Security and Risk*, Routledge.
Longhurst, R. 2016. Semi-structured Interviews and Focus Groups. *In:* CLIFFORD, N. J., COPE, M., GILLESPIE, T. W. & FRENCH, S. (eds.) *Key Methods in Geography.* London: SAGE.
Lorenz, E. N. 1972. Predictability: Does the Flap of a Butterfly's Wings in Brazil Set Off a Tornado in Texas? *American Association for the Advancement of Science*.
Lovell, H. 2018. The promise of smart grids. *Local Environment,* 24**,** 580-594.
Luhmann, N. 2014. *A sociological theory of law,* Abingdon, Oxon UK, Routledge.
Lundborg, T. & Vaughan-Williams, N. 2011. Resilience, Critical Infrastructure, and Molecular Security: The Excess of "Life" in Biopolitics. *International political sociology,* 5**,** 367-383.
Luque-Ayala, A. & Marvin, S. 2016. The maintenance of urban circulation: An operational logic of infrastructural control. *Environment and Planning D: Society and Space,* 34**,** 191-208.
Luque-Ayala, A. & Marvin, S. 2020. Urban Operating Systems: Producing the Computational City. The MIT Press.
Luque, A. 2014. The smart grid and the interface between energy, ICT, and the city: retrofitting and integrating urban infrastructures. *In:* DIXON, T., EAMES, M., HUNT, M. & LANNON, S. (eds.) *Urban Retrofitting for Sustainability: Mapping the transition to 2050.* London & New York: Routledge.
Marquardt, N. 2017. Zonen infrastruktureller Entkopplung. Urbane Prekarität und soziotechnische Verknüpfungen im öffentlichen Raum. *In:* FLITNER, M., LOSSAU, J. & MÜLLER, A.-L. (eds.) *Infrastrukturen der Stadt.* Wiesbaden: Springer Fachmedien Wiesbaden.
Martin, R. 2007. *An empire of indifference: American war and the flnancial logic of risk management,* Durham, Duke University Press.
Marx, K. 1993. *Grundrisse*, Penguin Classics.
Mason, B. 1993. Towards Position if Safe Uncertainty. *The Journal of Systemic Consultation & Management,* 4**,** 189-200.
Mason, B. 2019. Re-visiting safe uncertainty: six perspectives for clinical practice and the assessment of risk. *Journal of Family Therapy,* 41**,** 343-356.
Mason, B. 2022. Towards positions of safe uncertainty. *Human Systems,* 2**,** 54-63.
Massey, D. B. 1994. *Space, place and gender,* Cambridge, Polity Press.
Massumi, B. 2007. Potential Politics and the Primacy of Preemption. *Theory & event,* 10**,** 0-0.
Massumi, B. 2009. National Enterprise Emergency: Steps Toward an Ecology of Powers. *Theory, Culture & Society,* 26**,** 153-185.
Mbembe, A. 2003. Necropolitics. *Public Culture,* 15**,** 11.
Mc Cluskey, E., Charalambous, C., Mccluskey, E. & Charalambous, C. 2022. *Security, Ethnography and Discourse : Transdisciplinary Encounters,* Place of publication not identified, Routledge.

Mcfarlane, C. & Rutherford, J. 2008. Political Infrastructures: Governing and Experiencing the Fabric of the City. *International Journal of Urban and Regional Research,* 32**,** 363-374.
Mcfarlane, C. & Silver, J. 2017. Navigating the city: dialectics of everyday urbanism. *Transactions of the Institute of British Geographers,* 42**,** 458-471.
Millerand, F. & Bowker, G. C. 2007. Metadata Standards: Trajectories and Enactment in the Life of an Ontology. *In:* LAMPLAND, M. & STAR, S. L. (eds.) *Standards and their Stories.* Ithaca & London: Cornell University Press.
Mitteldeutscher Rundfunk 2015. Die DDR versinkt im Schnee: Fernsehjahr 1978/79. YouTube.
Moeran, B. 2013. From Participant Observation to Observant Participation. *In:* YBEMA, S., YANOW, D., WELS, H. & KAMSTEEG, F. (eds.) *Organizational Ethnography: Studying the Complexities of Everyday Life.* London: Sage.
Mohla, D. 2017. The History and Benefits of Standardization in Power Distribution Systems [Standards News]. *IEEE Industry Applications Magazine,* 23**,** 70-80.
Montuori, A. 2003. The Complexity of Improvisation and the Improvisation of Complexity: Social Science, Art and Creativity. *Human Relations,* 56**,** 237-255.
Morehouse, C. 2023. Extremists keep trying to trigger mass blackouts - and that's not even the scariest part. *Politico*, 09.10.2023.
Morgenthau, H. J. 1950. The Mainsprings of American Foreign Policy: The National Interest vs. Moral Abstractions. *The American Political Science Review,* 44**,** 833-854.
Murphy, J. F. & Conner, J. 2012. Beware of the black swan: The limitations of risk analysis for predicting the extreme impact of rare process safety incidents. *Process Safety Progress,* 31**,** 330-333.
Neal, A. W. 2019. *Security as Politics Beyond the State of Exception*, Edinburgh University Press.
Neyrat, F. 2016. The biopolitics of catastrophe, or how to avert the past and regulate the future. *The South Atlantic Quarterly,* 115**,** 247-265.
Nolte, A. 2022. Ordering Movement and Mobilizing Security. *In:* HEIN-KIRCHER, H. & DISTLER, W. (eds.) *The Mobility-Security Nexus and the Making of Order: An Interdisciplinary and Historicizing Intervention.* London: Routledge.
Nolte, A. & Westermeier, C. 2020. Between Public and Private: The Co-production of Infrastructural Security. *Politikon,* 47**,** 62-80.
Nye, D. E. 1999. *Consuming power: A social history of American energies,* Cambridge, Mass, MIT Press.
Nye, D. E. 2010. *When the lights went out: A history of blackouts in America,* Cambridge, MA, MIT Press.
Nyman, J. 2021. The Everyday Life of Security: Capturing Space, Practice, and Affect. *International Political Sociology,* 15**,** 313-337.
O'grady, N. & Shaw, D. 2023. Resilience, responsibility and state abandon: The changing role of the government in emergencies. *Political Geography,* 100**,** 102796.
Ofgem 2019. Technical Report on the events of 9 August 2019. online: Office of Gas and Electricity Markets.
Ophir, A. 2007. The two-state solution: Providence and catastrophe (Reprinted from Theoretical Inquiries in Law). *J. Homel. Secur. Emerg. Manag.,* 4.
Opitz, S. & Tellmann, U. 2015. Europe as Infrastructure: Networking the Operative Community. *The South Atlantic quarterly,* 114**,** 171-190.
Otter, C. 2007. Making Liberal Objects: British techno-social relations 1800-1900. *Cultural Studies: Liberalisms, government, culture,* 21**,** 570-590.
Oud, O. 2009. Digital Museum of Plugs and Sockets. online.
Palme, J. 2006. Can Computers Decide what is Right and Wrong? Available: https://people.dsv.su.se/~jpalme/reports/right-wrong.html [Accessed 17.06.2022].
Pargman, D. & Palme, J. 2009. ASCII Imperialism. *In:* LAMPLAND, M. & STAR, S. (eds.) *Standards and Their Stories: How quantifying, classifying and formalizing pratices shape everyday life.* Ithaca & London: Cornell University Press.
Perrow, C. 1984. *Normal accidents: Living with high-risk technologies,* New York, NY, Basic Books.
Perrow, C. 1994. The Limits of Safety: The Enhancement of a Theory of Accidents. *Journal of Contingencies and Crisis Management,* 2**,** 212-220.
Pescaroli, G. & Alexander, D. 2015. A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor. *Planet@ risk,* 3**,** 58-67.
Pescaroli, G. & Alexander, D. 2016. Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards,* 82**,** 175-192.
Pescaroli, G. & Alexander, D. 2018. Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework. *Risk Analysis,* 38.

Pescaroli, G., Turner, S., Gould, T., Alexander, D. E. & Wicks, R. T. 2017. *Cascading Effects and Escalations in Wide Area Power Failures: A Summary for Emergency Planners*, University College London.
Petermann, T., Bradke, H., Lüllmann, A., Paetzsch, M. & Riehm, U. 2011a. *Was bei einem Blackout geschieht: Folgen eines langandauernden und großflächigen Stromausfalls* Deutschen Nationalbibliothek
Petermann, T., Bradke, H., Lüllmann, A., Poetzsch, M. & Riehm, U. 2011b. *What happens during a blackout: Consequences of a prolonged and wide-ranging power outage,* online, Office of Technology Assessment at the German Bundestag.
Porter, T. M. 1986. *The rise of statistical thinking,* Princeton, Princeton University Press.
Porter, T. M. 2020. *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*, Princeton University Press.
Powells, G., Bulkeley, H., Bell, S. & Judson, E. 2014. Peak electricity demand and the flexibility of everyday life. *Geoforum,* 55**,** 43-52.
Powsybl. 2022. *UCTE-DEF* [Online]. Available: https://www.powsybl.org/pages/documentation/grid/formats/ucte-def.html [Accessed 28.06.2022].
Puar, J. K. 2017. *Terrorist Assemblages: Homonationalism in Queer Times,* Durham, UNITED STATES, Duke University Press.
Quarantelli, E. L. 2006. *Catastrophes Are Different from Disasters: Some Implications for Crisis Planning and Managing Drawn from Katrina* [Online]. online. Available: https://items.ssrc.org/understanding-katrina/catastrophes-are-different-from-disasters-some-implications-for-crisis-planning-and-managing-drawn-from-katrina/ [Accessed 05.11.2020 2020].
Queiro, F. 2021. Entrepreneurial Human Capital and Firm Dynamics. *Review of Economic Studies***,** 51.
Raich, T. 2021. Das Erbe der Feuernacht. *Die Zeit*, 11.06.2021.
Reason, J. 1990. *Human Error,* Cambridge, Cambridge University Press.
Reed, C. & Reed, M. 2023. *Enough of Experts : Expert Authority in Crisis,* Berlin/Boston, Walter de Gruyter GmbH.
Rerin, C. 2006. *Shouldering Risk: The Culture of Control in the Nuclear Power Industry*, Princeton University Press.
Rittel, H. W. J. & Webber, M. M. 1973. Dilemmas in a General Theory of Planning. *Policy Sciences,* 4**,** 155-169.
Rochlin, G. I. 1989. Informal organizational networking as a crisis-avoidance strategy: US naval flight operations as a case study. *Industrial Crisis Quarterly,* 3**,** 159-176.
Rochlin, G. I., La Porte, T. M. & Roberts, K. H. 1987. The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea. *Naval War College Review,* 40**,** 76-92.
Roe, E. & Schulman, P. R. 2008. *High Reliability Management: Operating on the Edge,* Standford, California, Stanford Business Books.
Roitman, J. L. 2014. *Anti-crisis,* Durham, Duke University Press.
Rose, G. 1997. Situating knowledges: positionality, reflexivities and other tactics. *Progress in Human Geography,* 21**,** 305-320.
Rumsfeld, D. 2002. DoD News Briefing - Secretary Rumsfeld and Gen. Myers.
Rutherford, J. & Marvin, S. 2022. Urban smart microgrids: a political technology of emergency-normalcy. *Urban Geography***,** 1-22.
Rybczynski, W. 2000. *One good turn: a natural history of the screwdriver and the screw,* London, Simon & Schuster.
Sagan, S. D. 1993. *The limits of safety: organizations, accidents, and nuclear weapons,* Princeton, N.J., Princeton University Press.
Salas, E., Tannenbaum, S. I., Kraiger, K. & Smith-Jentsch, K. A. 2012. The Science of Training and Development in Organizations: What Matters in Practice. *Psychological Science in the Public Interest,* 13**,** 74-101.
Salter, M. B. & Zureik, E. 2005. *Global surveillance and policing: borders, security, identity,* Cullompton [England], Willan.
Sánchez, A., Aragón, M. & Sanz Valle, R. 2003. Effect of training on business results. *International Journal of Human Resource Management - INT J HUM RESOUR MANAG,* 14**,** 956-980.
Schechter, B., Schneider, J. & Shaffer, R. 2021. Wargaming as a Methodology: The International Crisis Wargame and Experimental Wargaming. *Simulation & gaming,* 52**,** 513-526.
Schönheit, D., Kenis, M., Lorenz, L., Möst, D., Delarue, E. & Bruninx, K. 2021. Toward a fundamental understanding of flow-based market coupling for cross-border electricity trading. *Advances in Applied Energy,* 2**,** 100027.
Eingeschneit: Schneechaos im Münsterland, 2015. Directed by Schröder, L. & Klaue, C. Germany: WDR.
Schulman, P. 2004. General attributes of safe organisations. *Quality and Safety in Health Care,* 13**,** 39-44.

Schulman, P., Roe, E., Eeten, M. V. & Bruijne, M. D. 2004. High Reliability and the Management of Critical Infrastructures. *Journal of Contingencies and Crisis Management,* 12**,** 14-28.
Schwenkel, C. 2015. Spectacular infrastructure and its breakdown in socialist Vietnam. *American Ethnologist,* 42**,** 520-534.
Serrano, R. A. & Halper, E. 2014. Sophisticated but low-tech power grid attack baffles authorities. *Los Angeles Times*, 11.02.2014.
Star, S. L. 1999. The Ethnography of Infrastructure. *American Behavioral Scientist,* 43**,** 377-391.
Star, S. L. & Ruhleder, K. 1996. Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information systems research,* 7**,** 111-134.
Steele, W., Hussey, K. & Dovers, S. 2017. What's Critical about Critical Infrastructure? *Urban Policy and Research,* 35**,** 74-86.
Stern, M. 2006. 'We' the Subject: The Power and Failure of (In)Security. *Security Dialogue,* 37**,** 187-205.
Strengers, Y. 2012. Peak electricity demand and social practice theories: Reframing the role of change agents in the energy sector. *Energy Policy,* 44**,** 226-234.
Strengers, Y. 2013. *Smart energy technologies in everyday life: smart utopia?,* Houndmills, Basingstoke, Hampshire, Palgrave Macmillan.
Szeman, I. 2014. Conclusion: On Energopolitics. *Anthropological quarterly,* 87**,** 453-464.
Taylor, H. G. 1941. Standardization in the Electrical Industry. *Nature,* 148**,** 747 - 748.
Thrift, N. 1996. Spatial Formations. London.
Thrift, N. 2007. *Non-representational theory space, politics, affect,* New York ;, Routledge.
Tscnet. 2022. *Webpage TSCNET* [Online]. Available: www.tscnet.eu [Accessed 21.02.2022].
Übertragungsnetzbetreiber. 2022. *Regelleistungen.net* [Online]. online. Available: www.regelleistung.net [Accessed 19.08.2022 2022].
Übertragungsnetzbetreiber. 2024. *Netztransparenz.de* [Online]. online: German Transmission System Operators. Available: https://www.netztransparenz.de/de-de/ [Accessed 12.08.2024].
Ucte 2006. Final Report: System Disturbance on 4 November 2006. online: ENTSO-E.
Ucte n.d. UCTE data exchange fomat for load flow and three phase short circuit studies (UCTE-DEF). online: Union for the Coordination of the Transmission of Electricity
Us Cybersecurity and Infrastructure Security Agency (Cisa). 2024. *Critical Infrastructure Sectors* [Online]. online. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors [Accessed 22.04.2024].
Van Der Woerd, J. D., Wagner, M., Pietzsch, A., Andrae, M. & Gebbeken, N. 2022. Design methods of blast resistant façades, windows, and doors in Germany: a review. *Glass Structures & Engineering,* 7**,** 693-710.
Vde. Sicherheit und Verfügbarkeit von Netzleitstellen. VDE-Kongress 2006 - Innovations for Europe, 2006 Aachen, Germany. Verband der Elektrotechnik, Elektronik Informationstechnik e.V.
Vde Fnn. 2020. *Ressourcenregister für Krisenfälle* [Online]. online. Available: https://www.vde.com/de/fnn/themen/risiko-krisenmanagement/fnn-ressourcenregister [Accessed 01.07.2024].
Wakefield, S. 2018. Infrastructures of liberal life: From modernity and progress to resilience and ruins. *Geography Compass,* 12**,** n/a-n/a.
Wakefield, S. 2020. Urban resilience as critique: Problematizing infrastructure in post-Sandy New York City. *Political Geography,* 79**,** 102148.
Walters, K. & Rodriguez, J. 2017. The Importance of Training and Development in Employee Performance and Evaluation. *World Wide Journal of Multidisciplinary Research and Development*.
Walz, K. N. 1979. *Theory of International Politics,* Reading, Massachusetts

Menlo Park, California

London, Amsterdam, Sydney, Addison-Wesley Publishing Company.
Weick, K. E. 1987. Organizational Culture as a Source of High Reliability. *California Management Review,* 29**,** 112-127.
Weick, K. E. & Sutcliffe, K. M. 2007. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, John Wiley & Sons.
Weick, K. E. & Sutcliffe, K. M. 2015. *Managing the unexpected: sustained performance in a complex world,* Hoboken, New Jersey, Wiley.

Wellock, T. R. 2021. *Safe enough? A history of nuclear power and accident risk,* Oakland, California, University of California Press.
Welsh, M. 2014. Resilience and responsibility: governing uncertainty in a complex world. *The Geographical Journal,* 180**,** 15-26.
West, E. 2000. Organisational sources of safety and danger: sociological contributions to the study of adverse events. *Qual Health Care,* 9**,** 120.
Wilbur, W. R. 1905. *History of the Bolt and Nut Industry of America*, Ward & Shaw.
Wilcox, R. H. & Garrity, P. J. 1894. America's Hidden Vulnerabilities: Crisis Management in a Society of Networks. *A Report of the Panel on Crisis Management of the CSIS Science and Technology Committee.* Georgetown, Washington DC: Center for Strategic and International Studies.
Winzer, C. 2011. Conceptualizing Energy Security. *EPRG Working Paper 1123, Cambridge Working Paper in Economics 1151.*
Zimmerman, R. 2001. Social Implications of Infrastructure Network Interactions. *The Journal of urban technology,* 8**,** 97-119.
Zuboff, S. 2019. Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum,* 28**,** 10-29.