Secrecy and Society

ISSN: 2377-6188

Volume 3
Number 1 *Special Issue on Secrecy and Technologies*

Article 5

July 2023

(Not) Accessing the Castle: Grappling with Secrecy in Research on Security Practices

Lilly P. Muller
Cornell university, lilly.muller@kcl.ac.uk

Natalie Welfens
Hertie school, welfens@hertie-school.org

Recommended Citation
Muller, Lilly P. and Natalie Welfens. 2023. "(Not) Accessing the Castle: Grappling with Secrecy in Research on Security Practices." *Secrecy and Society* 3(1). DOI: https://doi.org/10.55917/2377-6188.1073
https://scholarworks.sjsu.edu/secrecyandsociety/vol3/iss1/5

(Not) Accessing the Castle: Grappling with Secrecy in Research on Security Practices

Abstract

This article discusses how to deal with secrecy and limited access in ethnographically inspired research of security fields. Drawing inspiration from recent debates about secrecy in Critical Security Research and from Franz Kafka's *The Castle*, we propose to treat access limitations and the secrecy we encounter as methodological tools that provide insights into social relations and power structures of security fields. We develop the argument in two steps. First, we argue for a more fine-grained taxonomy of secrecy, that allows to distinguish between mystery, concealment and the relational dimension of secrecy. Second, we apply the taxonomy to our respective fieldwork experiences in the fields of cybersecurity and refugee governance, to show how attending to different forms of secrecy produces empirical insights into the fields of study. Setting out how to work *with* rather than *against* secrecy, the article contributes to methodological debates in Critical Security Studies and Secrecy Studies, and ultimately to further cross-fertilize these fields.

Keywords

critical security studies, fieldwork, Franz Kafka, methodology, secrecy

(Not) Accessing the Castle: Grappling with Secrecy in Research on Security Practices

Lilly Pijnenburg Muller[1] and Natalie Welfens[2]

Abstract

This article discusses how to deal with secrecy and limited access in ethnographically inspired research of security fields. Drawing inspiration from recent debates about secrecy in Critical Security Research and from Franz Kafka's *The Castle*, we propose to treat access limitations and the secrecy we encounter as methodological tools that provide insights into social relations and power structures of security fields. We develop the argument in two steps. First, we argue for a more fine-grained taxonomy of secrecy, that allows to distinguish between mystery, concealment and the relational dimension of secrecy. Second, we apply the taxonomy to our respective fieldwork experiences in the fields of cybersecurity and refugee governance, to show how attending to different forms of secrecy produces empirical insights into the fields of study. Setting out how to work *with* rather than *against* secrecy, the article contributes to methodological debates in Critical Security Studies and Secrecy Studies, and ultimately to further cross-fertilize these fields.

Keywords: access, critical security studies, fieldwork, Franz Kafka, methodology, secrecy, secrecy studies

1 Lilly Pijnenburg Muller is a Postdoctoral Fellow in the Department of Science & Technology Studies and in the Judith Reppy Institute for Peace and Conflict at Cornell University. Previously Lilly worked as a Research Fellow at the Norwegian Institute of International Affairs (NUPI) and as a James Martin Fellow the Global Cyber Security Capacity Building Centre (GCSCC) at the University of Oxford. She holds her PhD from War Studies Kings' College London.

2 Natalie Welfens is a postdoctoral researcher working on the project "Refugees are Migrants: Refugee Mobility, Recognition and Rights." Natalie's research focuses on inequalities in refugee mobility and protection and combines insights from interdisciplinary Migration Studies, Security Studies and feminist scholarship.

In Franz Kafka's *The Castle* (2009 [1926]) the protagonist K. is summoned by the authorities of a village far away to measure a piece of land. From the moment of his arrival to the end of the book, K. never gains access to the authorities - the only ones who know the details of the task he has been summoned to conduct. Going through endless hurdles and attempts to reach the authorities, K. is often distracted on the way by the local villagers who all work for the authorities but appear to never have met them. Through K.'s quest and distractions on his path to reach the castle, Kafka paints a picture of a bizarre, outlandish village and its mysterious rulers. While K. never reaches the inside of the castle or meets the authorities, an image of the castle and K.'s task become visible for the reader through K.'s many attempts and interactions with the villagers.

Research on security practices often resembles K.'s attempts to access the castle and authorities. In Critical Security Studies (CSS) gaining insights through first-hand observations of security practices and "following the actors" count as the gold standard. There is a common sense that security researchers need to immerse themselves in the daily experts' practice, learn "the daily language, plotting the struggles" (Salter 2013, 105). However, like K., as security researchers, we are regularly confronted with complex security assemblages and "the secret" in our efforts to gain access to our subject (Bosma et al 2019). This struggle makes security research commonly understood as a "difficult terrain" (Schwell 2019). Challenges in researching security fields that are

presented as secret by those working with and in them can vary from access being endlessly postponed, contract delays, negotiations, the process of gaining and losing access, regulations, the role of trust vs. legality, ethical considerations, confidentiality, obscured data, and so on. As Walters (2014: 105) puts it, this then poses the question of how to follow the actors when they operate under and use secrecy to avoid insights?

In this article, we rephrase this question and ask which insights do we gain *through* secrecy and limited access in research on security practices? Drawing on and contributing to the vibrant literatures in secrecy studies (e.g. Birchall 2011, 2014; Maret 2016) and in Critical Security Studies (e.g. de Goede, Bosma and Pallister-Wilkins 2020; Walters 2014, 2021), we propose to think about secrecy as a methodological tool and thus as "more than a barrier to overcome" (Bosma et al 2019). Drawing on how we encounter and work with secrecy in our respective field research, we follow calls in secrecy studies to "stay with the secret" (Birchall 2014) and in Critical Security Studies to write "with secrecy" (Rappert 2010; De Goede 2020). We argue that instead of striving to open up the "black box" or removing a veil (Sommerer 2022), entering the Castle, or lamenting what at first can seem to be *failed attempts* of accomplishing what one originally sets out to find, it is precisely the messiness of access that provides important empirical and theoretical puzzle pieces. In particular, we contend that secrecy and limited access provide insights into a field's situated power and social

dynamics and ultimately allow us to draft a richer empirical picture of security practices.

To illustrate this argument, in this article we draw on Kafka's *The Castle* and K.'s seemingly endless attempts to access the authorities, akin to the ways we as researchers try to gain access to security practitioners. Like scholars in Critical Migration and Border Studies, we found Kafka to be fruitful to think about the diffuse and opaque ways in which power operates, structures asymmetric access to information and social relations (Sutton and Vigneswaran 2011; Eule et al 2019). In line with the tropes in Kafka's novels, we show how secrecy and the power relations it produces can be there because of unreadability and complexity of regulations and processes (see also Eule et al 2019), and how state practices can be secretive and "Kafkaesque'" despite the ideal of a Weberian bureaucracy (Sutton and Vigneswaran 2011).

The article is structured as follows. First, we situate the article within the current debates in Critical Security Studies and secrecy studies. Subsequently, drawing on Horn (2011) we propose a taxonomy of three forms of secrecy: mystery, concealment, and relational secrecy. In the second section we provide a brief description of our respective research approaches before we, with Kafka's *The Castle* and our taxonomy in mind, illustrate the secrecy dynamics in the security fields we researched, namely cybersecurity and refugee governance. Through three "secrecy vignettes" (de Goede 2020) from our ethnographically inspired fieldwork we show how limited access and secrecy can, rather than being barriers

to overcome, provide insights into the field's social relations, power dynamics and dysfunctions.

Secrecy Effects and Security Research

In Kafka's *The Castle* the reader follows K. on his quest to access the mysterious authorities and K.'s surreal efforts to understand the job he has been summoned to execute (De Jong and Rizvi, 2008). K.'s experience in the village has parallels to the fieldwork of social science academics in security fields: their attempts to gain access to sites and practices that are, seemingly and de-facto, hidden from the public eye, or to business or state practices that are often considered secrets. For instance, warzones are tough and dangerous to access; military practices and operations are classified or kept under "information management" (Campbell 2003), police and border guards work in often secretive environments (Dijstelbloem and Pelizza 2019; Glouftsios 2023), while security technologies and infrastructures are covered in technification and require technoliteracy (Valdivia et al. 2022; Aradau and Canzutti 2022; de Goede and Wesseling 2017).

Accounts of researching these contexts and security practices are often depicted as covered in a haze of secrecy that gets "especially thick the closer we get to the heartland of national security issues" (Best and Walters 2013, 346). At the same time, as Bosma, de Goede, and Pallister-Wilkins (2019, 5) point out, "doing qualitative and ethnographic fieldwork in the security domain (…) encounters very specific challenges of secrecy and confidentiality that largely remain under-theorized."

Acknowledging the specific challenges that research in security domains entails, research at the intersection of Critical Security Studies and secrecy studies has started to produce methodological tools to "grapple with" secrecy in research practice: accessing the field, collecting and generating data in secretive settings, or writing *with* secrecy (de Goede 2020; Rappert 2010). For instance, in their edited collection *Secrecy and Methods in Security Research,* de Goede, Bosma and Pallister-Wilkins (2020) provide a rich set of analyses of the challenges of secrecy in security research and set out practical ways to circumnavigate, encompass and work with secrecy. Moving beyond binary understandings of secrecy, this collective work sets out to embrace the "messiness" of fieldwork (Bosma et al 2020).

Crucially, this recent strand in Critical Security Studies builds on and advances insights developed in secrecy studies and/or longstanding methodological debates about ethnographically inspired fieldwork. For example, building on Brain Balmer's (2012:116) earlier work that shows how secrecy is not simply an obstacle to overcome but is an "active tool" that allows for the exercise of power, Belcher and Martin (2020) highlight how secrecies can operate through bureaucratic obfuscation, silences and delays in replying to research requests (see also Belcher and Martin 2013). Ultimately, they argue that secrecy offers insights into the (dis)functioning of the state (see also Dijstelbloem and Pelizza 2020). Likewise, Schwell (2020) reminds us how the "arrival story," i.e. narratives about how researchers sought and got access to particular

sites, is a classic trope in ethnographic scholarship. Yet, as anthropologists (e.g. Fassin 2013, 19) and interpretive methodologists (Yanow and Schwartz-Shea 2006) highlight, fieldwork access is not so much a clear-cut moment, but an iterative process, precariously negotiated through ongoing "critical dialogue" (Fassin, 2013, 19). Too often however the arrival story remains an anecdotal prelude to the "real" research analysis; gaining access is reduced to an initial barrier to overcome before the research process can commence (Schwell, 2020). Such a perspective dismisses how the very process of getting access and the secrecies we encounter reflect back on our research questions and can provide data in their own right.

We argue that to methodologically utilize the secrecy we encounter when accessing the field, a more fine-grained understanding of secrecy is essential, which we tease out in the following section. Subsequently, thinking with Kafka's *The Castle*, we apply the taxonomy of secrecy to our respective experiences of accessing and analyzing security practices to illuminate the power and social relations that structure the fields of study.

A Taxonomy of Secrecy

In our engagement with secrecy, we draw on Horn's (2011) three-fold categorization of secrecy, each of which foregrounds a different understanding or aspect of secrecy: *mysterium*, *arcanum* and *secretum*. As we find the Latin words to create a layer of opacity of their own, we

propose to simply speak of mystery, concealment, and relational secrecy instead.

In this taxonomy, mystery relates to something that is "unknowable" and denotes that something is puzzling or strange and impossible to explain or identify. Concealment in contrast, relates to deliberate techniques and practices of silence and seclusion. As a state practice, Luhmann (cited in Horn 2011) has linked this form of secrecy to political tactics of time management (e.g. to excess power without interference) and the preservation of the status quo. As such, concealment "is an essential tool of security, protecting sensitive forms of information from abuse – today most prominently in the form of classification" (Horn 2011, 108). Relational secrecy foregrounds the relational dimension of secrecy: the way "it structures social and political relations of exclusion and inclusion; by separating those who know from those who do not (but who may know, at one point, or who doubt or suppose that there is a secret), it constitutes their relation" (Horn 2011, 109). Importantly, in this particular understanding of secrecy, it is less about the actual content of the secret (or the very question of whether there is a secret or not), but the "secrecy effect": the ways in which the belief, suspicion or rumor that there is a secret can itself structure social and power relations (Derrida 1994).

Relational secrecy invites researchers to turn away from the "hermeneutics of the secret", which sees the secret as a problem to be solved through revelation. Instead researchers should attend to the

"aesthetics of the secret" (Birchall 2014, 26) and ask how secrecy constitutes social relations and the field. These social relations shape definitions of self and other, insider and outsider, collectivities and subjectivities (Birchall 2014). Focusing more squarely on the context of organizations, Costas and Grey (2016, 1423-1424) for instance note:

> secrecy can fundamentally shape behavior and interactions in organizations, regulating what is said and not said by whom and to whom. Such regulations not only are a result of and a source of control, but also shapes particular identity constructions, that is how individuals, groups and organizations define "who they are."

Thus, disentangling secrecy by means of the taxonomy, researchers can identify, for instance, when and where (non) access to knowledge shapes social and power relations between actors in the security fields we research. Consequently, the object of study is not the "black box" or "the secret," but '"secrecy effects" that structure social and political relations between "those who are supposed to know and those excluded from this knowledge" (Derrida 1994).

In research practice, an emphasis on secrecy effects as structuring social relations guides researchers away from chasing what is behind closed doors. Focusing on secrecy effects enables the analysis to highlight what or who locks these doors, with what reason and what effects, and to question what is black-boxed out of national security or business interests, and what is *perceived* to be secret or mysterious due to technological illiteracy, confusion or overly complex bureaucracy. Thus, rather than revealing the secret, we propose to map which aspects are

known and unknown, and what this can tell us about our broader object of analysis. Similar to a jigsaw puzzle, we suggest to start with the edges and work our way inwards. As such we create a clearer sense of what pieces are lacking and for the whole picture to become visible by proxy. Placing focus on what is often perceived as secret in security practices and including the "unknowns" and barriers, the encounters with classification, confidentiality and bureaucracy – staying with the secret – can provide researchers with a deepened ability to research security fields and ultimately, to conduct research on the seemingly unobtainable or secret (see also de Goede, Bosma and Pallister-Wilkins 2020).

In the remainder of this article, with K.'s story of trying to reach the castle in mind, we utilize the taxonomy of secrecy and discuss how to methodologically grapple with secrecy throughout the process of gaining access to and then being "in the field." We look at secrecy dynamics in the process of (1) getting access; (2) turning towards secrecy effects, i.e. how secrecy structures social and power relations; and (3) piecing this information together to craft a more comprehensive empirical puzzle.

(Not) Accessing Castles: Security Communities and Practices

In the next section of this article, we draw on our research in security settings, namely cybersecurity and refugee governance. Author 1's primary research objective was to explore the role that digital security technologies play in the sociotechnical making of cybersecurity. With a focus on cybersecurity, ethnographic research was conducted with the aim

to uncover the practices of technical experts building and maintaining the construction that upholds cyberspace. Author 2's project sought to understand how policy categories and their enactment in everyday bordering practices include and exclude refugees in transnational resettlement programs.

Both research projects dealt with complex, transnational security assemblages, connected through digital tools and infrastructures. Cybersecurity's international nature crosses both national borders and involves international cooperation, ranging from the technical every day to the international (Shires 2019; Stevens 2019). Cybersecurity is discussed as an international security concern and is on top of the security agenda of states internationally. Yet, a large part of its everyday maintenance and upkeeping is conducted by private firms that build and develop the codes and systems that keep the internet afloat. Similarly, refugee resettlement programs bring together a heterogeneous, transnational community of practice, dispersed across political scales: state and non-state actors, international organizations, service providers and refugees themselves. To identify, process and select refugees for resettlement, different state and non-state actors compile digital dossiers through everyday practices such as interviews and frontline assessments and transfer information transnationally to ultimately decide which refugees to prioritize, include or exclude.

To tackle the multifaceted actor constellations in the two security settings, both projects drew inspiration from ethnographically inspired

security research (e.g. Salter 2006; Schouten 2014; Hoijtink 2014; Anwar 2020) and opted for a multi-sited ethnographic approach (Marcus 1995). We deployed interpretivist methods to produce insights "through systematic observations in the "field" by interviewing and carefully recording what [we] see, hear and observe people doing while also learning the meanings that people attribute to what they do and things they make" (LeCompte and Schensul 2010, 16). More concretely, both of us relied on the collection and reading of different forms of texts, semi-structured interviews with key informants, and observations of security actors' daily practices and practitioner events.

In researching security fields, we often encounter multiple layers of secrecy: something can be secret due to its securitized nature, and practices within it can also be secretive. Secrecy is encountered to some degree in nearly all ethnographic pursuits, but in security fields there is often an additional layer of secrecy connected to security. Utilizing the taxonomy of secrecy - mystery, concealment, and relational - we unpack the differences between secrecy effects on the one hand, and what are deemed necessary secrets due to the security contexts. Ethnography can lead the researchers through different paths, wanderings, and distractions. In security fields the taxonomy of secrecy is especially useful to identify what is genuinely secret and what is covered under secrecy for power, security or both.

The following account of our research experiences draws on a close reading of our respective fieldwork material. Our reading and analysis

thematically focused on negotiations of access (experiences of what we variously initially understood as "failures," limitations, as well as secrecy) and how we interpreted these instances. Methodologically, we follow de Goede's proposition to use vignettes as a "way to give secrecy a place in academic writing" (2020, 262). Such "secrecy vignettes" can be useful to make explicit "ethical dilemmas and ongoing fieldwork negotiations", and of "rendering visible that which normally remains invisible in research" (2020, 262). In the following section, we deploy secrecy vignettes to make secrecy and limitations in our fieldwork visible, and through the lens of the secrecy taxonomy identify social relations and power structures in security fields.

Encountering Different Shapes and Shades of Secrecy: Researching Security Practices

Using Kafka's *The Castle* as an allegory, the following section illustrates how we grappled with different types of secrecy and utilized them for our analysis of security practices. We highlight how we shifted from (1) trying to access "the castle", i.e. a particular site or actor, to (2) studying the village, i.e. what surrounds the secret parts and how secrecy produces social relations. Ultimately, we argue, this shift in focus (3) provides a more comprehensive empirical picture of security practices and power struggles.

Searching for the Castle: Demystifying the Field, Disentangling Secrecy

Like K.'s attempts to get to the castle and meet the authorities, fieldwork on security practices often starts with the idea that we have to get access to a specific site or a particular actor (Belcher and Martin 2020). When trying to gain access, our initial encounters with the field frequently focus on what we assumed to be (intentionally) veiled or blocked off and our hermeneutic efforts to get hold of "the secret" security practice.

Moreover, similar to K., we often start off as strangers in the field when conducting research in security settings. More often than not we need a permit or some kind of clearance which entail effort, uncertainty and waiting, and the official permit or discretionary research access may or may not be given in the end. How and with whom to negotiate access, the power dynamics in the field, are often difficult to grasp and may even feel diffuse and mysterious. However, rather than seeing these encounters as malfunctions, our initial encounters with the field, including encounters with its secrecies and what feels like defeat, provide key insights into the power structures that uphold the security field.

Cybersecurity

Having worked on the development of cybersecurity policy for NATO, the UN, and national cybersecurity strategy building, I had for years heard what by now had become some sort of mantra in the policy world; "I'm not a technical person," as a response to questions and discussions on cybersecurity in international politics. This symptom

seemed to have spread to the academic environment of the social sciences that I called my home. While acknowledging that technology plays an important role in cybersecurity production (Stevens 2016), the numerous articles and books in the social sciences that work to define cybersecurity (Valeriano et al 2018; Shires and Smeets 2017; Singer and Freidman 2014), often exclude the technical aspect of cybersecurity (DeNardis, 2014; Gartzke and Lindsay, 2015), or acknowledge it but engaged at a minimum level (Dunn Cavelty and Wenger 2020). The technical elements and technicality of cybersecurity are treated as a "black box" in the social sciences – an element that does not need critical engagement to enable an understanding of cybersecurity. Yet, cybersecurity's sociotechnical construction (Dwyer et al 2022) meant the technology used impacts the security produced, and vice versa, so it was a black box I felt I had to open.

When a call came out for a joint social and computer science research position, which allowed for cooperation with a cybersecurity firm and gave access to their threat intelligence data set, I jumped on the application. Explaining my motivation and interests in the data and practice of the firm the excitement was overwhelming when I was offered the position. I was going to be inside the "black box" of cybersecurity. Making a longwinded story short, from the point of my arrival, it took six months of contract negotiations to even receive an access card to the firm. This process, full of uncertainty and confusion surrounding if I would even get the promised access, and what this would give me, was full of

frustration and disillusionment. I was in the dark regarding *if* I would ever get access and, even more alarming, access to what. Yet, the show had to go on. I decided to write drafts of my theory and methods based on the calls and conversations with the representatives in the firm during negotiations, to prepare myself for how to work with the data once I was granted access. As the research position originally was for a computer science student, I thought it was reasonable to expect that I was going to be exposed to some degree of technical data within the firm. Yet, when the big day finally came six months later, the surprise was underwhelming when I was presented with the facts.

In the company there was little to no interests in sharing information. Upon arrival I was given a desk in a landscape with the administration and secretaries. The partners in the firm had a habit of being too busy to discuss matters or would cancel meetings last minute, if they had agreed to schedule one with me in the first place. As such, they remained mysterious rulers due to their busy schedules and inability to meet with me. The need for clients to not share their vulnerabilities and possible attacks due to fear of leaked information, led to most meetings being held behind closed doors. Even with my granted "formal" access, the research site remained secretive, obscure, and difficult to access. Yet, I refused to give up, and followed the "field work handbook" spending the following four months trying to gain trust, by joining as many events as possible, drink coffees, and "hang around," yet little came out of it my time spent there.

I slowly realized in the few conversations I did manage to have with the people there that they neither had access to nor extended knowledge of the technical aspect of cybersecurity I thought I was trying to find. What they wanted from me, the researcher, was to teach *them* about cybersecurity. What seemed to be mysterious from the outside remained equally mysterious from within. The promised threat data in the project description turned out to be an unorganized Excel sheet composed by various interns. The data had been added over time when they had had the time to add cases ad hoc as they were being solved, made without any methodology for classifying threat actors or any indicator of what should be placed where in the categorization of importance, degree, ramifications. Everything had been categorized based on the various interns' personal judgment. Thus, the security practices that looked mysterious and complex from outside where, from up close, actually rather simplistic and highly discretionary practices. After six months of struggling to gain access, and another four months spent to build trust, it felt like what I was searching for was falling through my hands like sand. Another dead end? Had the struggle to get "in" led me to an empty box?

Refugee Governance

In my research, access to the wider community of practice centrally hinged on accessing German migration authorities, in particular the Ministry of the Interior and the Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge, BAMF). Within the broader

process of refugee admission, it was ultimately these actors' sovereign and discretionary decision to set up resettlement programs in the first place, to define selection criteria and to decide who gets on an airplane to Germany and who stays put in countries of refuge. Therefore, I thought, uncovering state officials' frontline decision making would be key to answering my research question – the equivalent to accessing the castle in K.'s journey.

While a first interview request with a ministerial bureaucrat was successful, any attempts to get access to first-hand observations of selection practices or access to material evidence about selection practices failed. My inquiry to do a research internship with the German Ministry of the Interior was turned down without further explanation so that the internal workings of the state apparatus remained opaque and somewhat mysterious to me. As an alternative I was offered an interview with the head of the department, which turned out to be a conversation of thirty minutes, infused with technical and legal explanations of the process. Similarly, state bureaucrats at the BAMF were only available for a non-taped interview with rather press-like statements about their selection practice. Although devoid of anything insightful I had hoped to learn about the logics of refugee selection, the emphasis on bureaucratic technicalities and logistics in these interviews also demystified what from outside had appeared to be a deliberately opaque state practice of concealment.

Despite their limitations, these interviews were key to partly demystify the field; to disentangle what was kept secret and which information did simply not exist. Asking about dossiers and the paper trail from previous selection missions, I learned that in admissions from Lebanon (2013-2015) individual selection criteria were not assessed in detail or weighted, but that frontline workers only needed to write a few lines in an open textbox to justify their decision over inclusion or exclusion. While these files were for internal use only, I had to realize that the data I expected to be key to answering my research question simply did not exist in the form I had imagined. One of my interlocutors explained to me, that there were also no internal statistics about how many people are selected per priority category, and claimed that the information did not exist, because it is not of interest to the state. Thus, what initially seemed like deliberate concealment, turned out to be ignorance, whether strategic (McGoey 2012) or not. This lack of knowledge about how many refugees Germany admitted primarily as "particularly vulnerable" and how many due to "family ties" or their "integration prospect" could indeed be a strategic choice of "knowing what not to know" (Taussig 1999) to limit scrutiny and accountability. Just like it could be the result of lacking resources, skills and technological infrastructures in public administration.

Observing frontline practices of ongoing selection missions then seemed a promising if not better alternative to records of past missions. My first request was declined after two months of waiting for a reply.

Another attempt to get access to a selection mission – this time via the Ministry of the Interior did not lead to fruition. After repeated inquiries via email, I finally got to talk to a BAMF bureaucrat via phone, who explained to me that shadowing a mission would not be possible because the space at the visa counters, where interviews take place, was too small. Whether it was deliberate concealment or real infrastructural limitation which created the appearance of secrecy is hard to tell. Either way, it kept me as a researcher at arms-length and thereby impeded detailed scrutiny of state selection practices.

Gaining Access as a Method

The first and initial efforts to access our fields both illustrate how gaining access to the site, initially assumed to be core to a research question, can be lengthy and uncertain, full of waiting and partly denied access (Belcher and Martin 2020). Once the site that at first seemed central to unravel the core is (partly) accessed, the data one expects to find either does not exist, is not in the form imagined, or does not contain the value first assumed. Like K's experience in *The Castle*, in this initial phase of entering the field a researcher's foreignness and questions regarding intentions, the potential benefits and risks an outsider's presence can bring about can make the research process and data collection daunting and disillusioning.

Yet, these initial encounters with the field do not just present barriers to what at first is assumed to need uncovering. These

experiences of delays, hindrances and disappointments are research outcomes that help to disentangle the initial cloak of secrecy we often encounter in researching security practices. First, initial failures of getting access or particular types of data can *demystify* our research object and the security field. What from the outside appears to be secretive in a mysterious sense of the word – how data sets and classifications are being made and decisions taken – might be a question of technicalities or, seen from up close, rather unsophisticated practices, as both of our cases illustrate. Moreover, real gatekeeping and gatekeepers lack of knowledge or ignorance – both creating the appearance of secrecy – can be difficult to distinguish.

Second, our first ("failed") attempts of getting access offer insights into how we as researchers may engage with and potentially impact the field's secrecy. In cybersecurity we see how practices are both mysterious and opaque from the outside *and* the inside. The fact that external researchers can be considered as experts with skills to demystify practitioners' practices exemplifies this point. In refugee governance, in contrast, deliberate practices of concealment are more identifiable and secrecy, real or perceived, is what keeps the researcher at a distance and limits scrutiny. Third, as we will unfold in more detail below, initial encounters with the field, including failures and disappointments provide insights into the social relations and power dynamics.

Turning Towards the Village: Studying Secrecy Effects

In Kafka's *The Castle* instead of getting to know the specifics of K.'s task, we as readers get to know the inner workings of the village around the castle. Through the tales the inhabitants tell we slowly gain a picture of the authorities and the way in which secrecy, in terms of (non-)access of information, shapes social interactions. Where the villagers do not have full information, they still have hunches and ideas about what motivates the castle's actions. These understandings of the castle shape social relations and power dynamics among the villagers and between the villagers and the authorities.

As security researchers, too, we start off with a specific task or research question – in our case the socio-technical co-production of cybersecurity and selection of refugees for resettlement – which may initially seem nowhere to be found. Just like K. who never meets the authorities but gains insights about the castle and its mysterious rulers through encounters with the villagers, we can turn the gaze from what we initially identified as the place where the secret is stored to its surroundings. Instead of entering the castle, we can opt for an approach that "stays with the secret" (Birchall 2014) and takes an interest in "secrecy effects" (Derrida 1994). That way, how secrecy – assumed or real – is productive of social relations and power asymmetries is made visible.

Cybersecurity

Every door I knocked on, was either closed or empty. Like K., I was desperate to meet the authority. I felt left at a crossroad, was I going to have to alter my research question based on the access I ended up getting? Or could I stay with the research question and continue?

If I based my research output on the data that was provided from the firm I would have to let the role of digital technologies in the threat construction take a back seat. As many researchers do in this situation, this meant altering my question to work with the data. In this approach my findings would describe the firm's perspective on cybersecurity. It would however not answer the questions I set out to answer, namely to understand the sociotechnical construction of cybersecurity. The research would as such be another discourse analysis description of cybersecurity. I could contribute with a new perspective to an already known point - that cybersecurity is complex and messy, with no one core to it (Stevens 2021, 10). As Smeets and Shires (2017, 17) remind us, "the complexity of cyberspace - who considers it complex, and for what reasons – is (…) a key means of contest." Cybersecurity signifies a complex and emergent series of interactions and processes, meaning different things to different stakeholders at different times and places depending on their focus and orientation (Shires 2019). These definitional differences represent the coexistence of multiple and competing understandings of security (Stevens 2021, 10). Describing how this firm understood cybersecurity I would contribute with a new perspective on cybersecurity, but not the sociotechnical one I had set out to find.

A Latourian approach of staying with and tracing the actors in the firm would tell me about the construction of the legal covering up of cybersecurity incidents, the protection of customers, the importance of keeping secrecy around who is attacked and protecting their name out of economic interests, and the sprint to catch up with new legislation. While this is also a part of the cybersecurity assemblage, the technical and the international aspect that I wanted to include would continue to largely be left out. My goal was to tear down this leviathan and examine the role of the complex digital technology therein.

What was I to do after endlessly awaiting access, and the realization that the access was different than what was promised? These moments of (dis)continuity in the research - denied access, messy and contingent practices – are not failures but part of the analyses. Rather than thinking about the "secret" or seemingly "excluded" technology as something to be uncovered I started to unpack the dynamics of power within the cybersecurity practice. I changed my perspective from understanding the socio-technical making of cybersecurity as a simple binary (information is *either* secret *or* public), towards focusing on the complex trajectories and contestations (Bosma et al 2020). In my research this meant analyzing the play of power and authority I encountered, while *resisting* the "magical reification" of the secret or the holder of secrets.

Changing my approach, I rather asked who decides what data is shared? How is data made? What effect does this practice have on how

cybersecurity is understood? In seeking answers to these questions, it became increasingly clear that secrecy structures social relations. Few authorities or practitioners hold an understanding of the full picture and what constitutes cybersecurity. Cybersecurity is continuously made throughout the whole process of its becoming (Bousquet, Grove and Shah, 2020). There is not one place or "funnel" where the technical and social meet as I had thought when setting out to research its socio-technical making. The technology and the social impact each other continuously in the making of knowledge of threat actors. What technology is used where is a socially determined, but the knowledge produced is made through and with the technology. This knowledge again impacts what further technology is used and so forth.

The taxonomy of secrecy allowed the research to go beyond a binary approach to methods that seeks to *either* establish laws for research validity or question the very possibility of such an aim. Categorizing the secrecy met I helped reorient towards what was mysterious, what was being concealed intentionally or unintentionally, and what was secret out of necessity. Shifting my perspective meant the power structures within the organization became visible. Staying true to a research question I moved from trying to identify a binary to mapping the layers of secrecy, the truly secret, what was secret through knowledge being distributed and what was secret by concealment. I shifted from understanding the secrecy encountered as *a mystery* to uncover, to working with secrecy to identify the power structures and asymmetries.

Refugee Governance

After my initial attempts of getting firsthand observations of the German state's selection practices failed, also interviews seemed to not bring me closer to getting the information I was looking for. In an interview with a BAMF frontline worker, my interlocutor replied that she was not allowed to tell me details about frontline selection, and that what she had told me until then was already a lot. After a rather empty remainder of the interview, when already walking to the door, it was a brief small-talk sequence that left me wondering whether my longing to uncover the German state practices was actually blocking my view. Apologizing for not being able to tell me more, the frontline worker suggested not too focus too much on the state's selection, as it was - according to them - only a small part of the process.

What if I put the initial imperative of pushing further to make practices of border governance more transparent to the side for a moment and focused on the workings of secrecy in refugee resettlement? What if, like K. in Kafka's novel, I would explore the village and ask about the authorities, instead of desperately trying to meet with them?

Hence, I started to explore the practices and institutional sites which proceeded German state actors' selection and the 'secrecy effects' of (non)knowledge on other actors: NGOs and offices of the United Nations High Commissioner for Refugees (UNHCR) in Turkey and Lebanon, which identified and processed the dossiers of 'resettlement candidates'

before a number of select files reached the frontline of admission countries, such as Germany. During my fieldwork in Lebanon and Turkey, I interviewed these different actors not only about their respective practices of categorizing and prioritizing refugees but also inquired what they knew, or thought to know, about Germany's or other states' selection practices.

To my surprise, I learned that neither NGOs identifying people in "need of resettlement" nor UNHCR staff who processes these files further knew in detail about all admission states' selection practices. UNHCR Turkey reported that it was left in the dark about what exactly classified as "severe medical needs" for German authorities, or how exactly they assessed "integration potential" and "security risks." As a consequence of their limited knowledge, UNCHR would sometimes not submit cases of vulnerable refugees whose chances to be resettled it deemed "too low". Thus, while unable to find out "the truth" about Germany's selection practices, I could render visible how secrecy – in terms of (non)-access to particular kinds of knowledge – had important effects on practices and resulting boundaries of inclusion exclusion for refugees: in a spirit of anticipatory obedience, UNHCR was "deprioritizing" dossiers, which it assumed to not make it past the frontline of admission states.

Shifting the focus towards the relational dimension of secrecy – who has access to certain knowledges, why and with what effects – also provided insights into power relations within the field. Questions about

why other actors did not push for more information about resettlement countries' practices, highlighted for instance UNHCR's financial dependence on resettlement states' contributions and the relative power of states in a fully discretionary policy process. Secrecy within the field was thus reflective and productive of power relations between different actors.

This also included the relations between state and non-state refugee-selecting actors and refugees themselves. While for me as a researcher – white, middle class, German-native, equipped with a generous research budget and a four-year PhD contract – mainly German state bureaucrats' practices appeared obscured. However, for refugees themselves much larger parts of the process remained opaque – from the initial vulnerability assessments of NGOs, via UNHCR's complex multi-step assessment of "resettlement candidates," to the final interview with resettlement states' migration and security authorities. As scholarly work confirms, limited access to official information about selection practices is productive of rumors and informal information sharing among refugees, which become essential to navigate the resettlement process (Menetrier 2021; Ozkul and Jarrous 2021). Yet, these works have also shown that "deliberate or not, the opacity inherent to the bureaucracy of the resettlement selection process initiates refugees' confusion and actions which, in many cases, work to their detriment" (Menetrier 2021, 8). As such, secrecy around resettlement selection practices and state practices more broadly, crucially structures the power asymmetry between the

state and refugees: *concealment* here indeed served" to protect and stabilize the state" (Horn 2011, 106). It secures the state's sovereign power over outsiders, while limiting the agency and subjecthood of refugees – an insight which, without having shifted the focus from "the secret" to its surroundings, I would have missed.

Towards Relational Secrecy

Both of our accounts illustrate a shift from understanding our original "failures" of getting access towards understanding secrecy and limited access as producing data in its own right. This approach foregrounds secrecy as a factor that shapes social relations and power asymmetries between security actors as well as their self-understandings within the field. Through using the taxonomy of secrecy as a methodological approach, we steered away from hunting particular pieces of information and actors, supposedly making up the "core" of the practices we studied. Instead, we focused on how access to information is distributed and governed among security practitioners, what is kept secret, by whom and to what end. Studying the "secrecy effects" (Derrida, 1994) in the field allows research to disentangle *who* creates secrecy – e.g., through limiting access to information. Making this shift, we as researchers can identify who holds power in the field and thus shapes the knowledge produced. In cybersecurity we see that knowledge is distributed as a security measure, where secrecy is used functionally to keep the field secure, as well as instrumentally to obtain and maintain

power. In contrast, the case of refugee governance shows that especially the state's practices of concealment are more intentional and work to secure the state's sovereign power and limit public scrutiny. In line with secrecy studies' theorization, one may further inquire into how power holders are legitimated or challenged, how secrecy is productive in such processes and the effect this has on the field as a whole (Horn 2011).

Piecing Together the Bigger Picture

Like Kafka's protagonist, security researchers' sense of getting or already having access fluctuates throughout the process of conducting research. Sometimes, what we wanted to get at seems to be out of reach, other times it can feel like we are getting fairly close to the information we are looking for, but there is *just one more* barrier to overcome, or one more interview that will give us the last missing piece. Fieldwork can bring about new connections to gatekeepers or "fixers," who can provide access. Or just like in K.'s experience, there might a moment of realizing that even with some parts remaining blocked, we actually *do* have access, immersed ourselves into the field. With a relational view to secrecy, as outlined above, we can then piece together the data we have as well as instances of "failed access" and start to see the bigger picture.

Cybersecurity

In my fieldwork I struggled to find the complex and advanced machine learning algorithmic models in making cybersecurity that I expected to encounter. Instead of seeing the seemingly simple technological use encountered as "failure" and as my inability to encounter and "find" the complex machine learning algorithms and artificial intelligence, the encounters suggest instead that there is no "one" type of "complex digital technology" that is *the* technology in the making of cybersecurity, just as there is no "one" social process within cybersecurity companies. My "mistakes" or what felt like "wrong paths" in my aim to gain access to the technical core of machine learning and artificial intelligence I wanted to find show that the technology plays a more convoluted role than I had expected in the larger cybersecurity assemblage, but a no less important one. There is power in distributed secrets. The hindrances I met on the way, rather than being interpreted as obstacles, clarify what is secret, what is covered under the illusion of secrecy to keep it secure, and what is complex - minimizing the perceived complexity of cybersecurity.

The experience of gaining access is as much an account of socio-technical relations and secrecy as any other, but it does not uncover digital technologies' role in threat production. The actors that continuously take part in building up the mystery surrounding the technology in use in cybersecurity practices gain from being the few that know, keeping cybersecurity secure, vital, necessary, and unattainable. For the security practitioners the most sensitive information to share is who is attacked,

how, where, through and by whom, how they know this, and the algorithms and techniques used to find and hinder these actors. These details can reveal their customers' (both private sector, individuals', and states') weaknesses, the very weaknesses they are paid to protect. The technology they use, the models that shape how these codes and data are collected and built is less sensitive and less detrimental for them. How they find these threats and politicize them is kept secret – these practices are their business model. The everyday practices by individual security practitioners are however less sensitive.

Thus, when we cannot access the larger picture, or it is hard to see, mapping the everyday practices and connecting the dots between them we can put together the outer pieces of the puzzle to make a frame of the picture emerge. As such we can start to see the outline and begin to understand what is needed in the center for the picture to emerge. Mapping the everyday practices helps minimize what is secret for security reasons versus what is seemingly secret due to concealment, mystery, or relational practice. Acknowledging the different forms of secrecy at play gives a clearer vision of the missing pieces and which pieces just seemed secret due to secrecy effects.

Refugee Governance

The continuous process of getting access confronted me with the cloak of secrecy around particular parts of the refugee resettlement process but also opened up new ways of approaching and learning about

my research object: selection practices in refugee governance. Through analyzing secrecy in its different shapes and shades, I better understood the processual character of selection practices and how power over inclusion and exclusion was dispersed along the transnational policy process. Decisions which I had thought to be taken by the BAMF were actually taken by other actors; some dossiers were sorted out long before they would even reach admission countries' frontline bureaucrats. Rather than the decision-making power being concentrated in one place and in the hands of state authorities only, it was the many micro-decisions by a multiplicity of actors that shaped the boundaries of inclusion and exclusion in refugee admission programs. To a large degree it was this very process of many hands, with state and non-state actors involved, that made refugee selection opaque and seemingly secretive, also for all actors involved. Thus, examining instead of challenging the secrecy in refugee admissions.

Moreover, while states' discretionary and deliberately secretive selection practices clearly casted a shadow over other actors' selection, as described above, I also understood that it was not always secrecy that was at play. NGOs limited knowledge about admission states practices related more to the complexity of the overall process and limited capacities (or interest) to push for more information. Likewise, UNHCR reported that missing information in a dossier – even in internal processes - was often the result of untidy practices, lack of resources or translating bureaucratic categories from one actor to the next along the policy chain.

Taken together, grappling with secrecy and disentangling its different forms allowed me to craft a richer and further ranging story of selection practices in resettlement.

The Sum of Secrecy is Greater Than the Parts of the Individual Holders: Crafting a Multi-faceted Account

Our accounts illustrate that, in the end, our initial "failures" to gain access to what we understood to be "the secret" of our respective fields did not only allow us to better understand how secrecy structures social interactions, but to also make this a central part of our analyses. Piecing together the insights generated, not despite but through secrecy, we arrive at a comprehensive picture of what we initially set out to find – in our cases, the making of cybersecurity and refugee selection. In both of our cases, engaging with secrecy teaches us – in sharp contrast to our initial understanding of the field – that power is not concentrated and contained at a particular site, in distinct objects or held by specific people. Analyzing power with a focus on access to information and impact on decision-making, both of our cases exemplify that power is dissipated, and there is no one all-knowing actor. To stay with *The Castle* as an allegory, an essential part of what "failed access" and secrecy in fieldwork may teach us is that there might not be a castle to access, and no authorities to find. Yet, as we show, analytically engaging with secrecy allows to show not only that knowledge and power are distributed but *how* and with what effects.

Moreover, our respective experiences illustrate how disentangling the different shapes and shades of secrecy, by means of the taxonomy deployed here, can produce more multi-faceted accounts of security fields and practices. Centrally, it enables us to distinguish "the secret", i.e. hermeneutic approaches to secrecy as acts of intentional concealment, from other forms of secrecy and related phenomena which may only appear as secrecy at first sight. For instance, in cybersecurity, access to information can be distributed as part of a deliberate security strategy, serving to secure digital infrastructures and keeping intruders out. In refugee governance, admission states' selection practices are deliberately obscure to prevent "risky" individuals to abuse the procedure and enter state territory. This, however, is different from what makes these fields *appear* secretive – a lack of technical literacy in cybersecurity and overly complex bureaucracy in refugee governance - and the relational effects this secrecy has.

Unpacking the layers of mystery, concealment and relational secrecy opens up how secrecy is used by the actors for security reasons and power, and how this impacts the field studied. While security fields are often understood to be particularly difficult to study due to their secret nature, the taxonomy of secrecy presented here can assist researchers in approaching their fieldwork reflexively and inductively. We might not always be invited in by the authorities through the front door, but we can learn from the system around it.

Conclusion: The Castle, the Secret, the Complex, and the Power In-Between

The point of departure for this article was the observation that secrecy is often believed to cloud critical engagement with security fields. In this article, we have rephrased questions of access and instead asked which insights we can gain *through* secrecy and limited access in research on security practices. Taking Kafka's *The Castle* as an allegory, we have illustrated how to harvest limited access and secrecy in fieldwork as data in its own right. More concretely, we have proposed to disentangle different types of secrecy and scrutinize how secrecy shapes practices, social relations and the power dynamics: what is secretive to whom and why, and how differential access to information is reflective and productive of power relations within the field. Providing "secrecy vignettes" (De Goede 2019) from our own research in cybersecurity and refugee governance, we have drawn attention to the processual character of getting access and dealing with secrecy throughout the fieldwork process.

Theoretically, we combined recent debates in Critical Security Studies with insights from secrecy studies, that have called attention to the different forms of secrecy and the "aesthetics of the secret" (Birchall 2014, 26). Concretely, drawing on Horn (2011), we proposed to distinguish between mystery, concealment and relational secrecy, as a taxonomy that can help us utilize experiences of limited access. This taxonomy, we argued, provides researchers with a tool to analytically

disentangle the various types of secrecy and their effects in security fields. It clarifies what is secret out of necessity due to the security field itself, and what is complex, fragmented, mysterious or concealed even for experts and practitioners.

Drawing on our respective fieldwork experiences, we have shown how this taxonomy provides insights into how secrecy works and how it structures social relations and power dynamics in cybersecurity and refugee governance. Proclaimed experts and elites can use secrecy in an effort to cover up their own ignorance of bureaucratic or technical complexity, use secrecy to make their field more important or lucrative, to limit scrutiny of sensitive practices or to exercise power over other actors. The day-to-day technical aspects of a field might not be what needs to be kept secret due to security matters yet making it secret gives power to certain practitioners. At the same time, practitioners tend to refer to secrecy, where in fact illiteracy of technologies or processes may actually be at play.

Through a focus on secrecy then we better understand the very security practices we initially set out to research. Disentangling what is secretive and what *appears* secretive, what is bureaucratic opacity and what is strategic intention, as well as how these two poles interact, allows for a better understanding of how security is practiced and to what effect. Rather than being hindrances in the way to trace an object or secret, the inability and struggles to gain access can be used to understand the security practices themselves.

Including these interactions allows research to move beyond tracing the object (Latour 2005), towards tracing how these interactions themselves show how the object comes about or does not exist as preconceived. In cybersecurity, secrecy is both used to keep systems secure by not letting enemies and competition know how a system works and by people working in the field that do not want to admit to not knowing something in an exercise of power. Knowledge is spread out to keep a system secure, but also leads to secrecy in the form of mystery or concealment. The power struggles intrinsic to many security practices become visible through tracing the outlines of the secrecy built around and into it. In refugee admissions too, engaging with secrecy brings power dynamics built into the sharper relief to the researcher. Admission states deliberately conceal their practices for security reasons, which secures their sovereign power vis-à-vis refugees and other actors involved. At the same time, what makes refugee selection as a whole appear secretive and opaque – for refugees, researchers and policy actors alike - is the complex, bureaucratic process of many hands and dissipated decision-making power.

Crucially then, engaging with secrecy alters our very understanding of security fields and practices. Where we initially set out to access the castle and the authorities, the one actor and specific site, we might come to understand that it is actually the village that holds the relevant information; that in fact, there might not be a castle and its mysterious ruler to uncover. More concretely, mapping who has information to what,

what is secret for security reasons and what is secret to instill power or protect it - disentangling the secret - shows that few people in security practices actually hold "access" to or "extended knowledge" of the research object at hand. Rather, individual actors often hold only knowledge of smaller pieces within it. The sum of secrecy is greater than the parts of the individual holders. The "secret veil" is not the result of a single move, or a single act of intention, but an accretion of often insignificant, mundane but powerful everyday moves. Ultimately, piecing the different edges of the jigsaw puzzle together means the researcher often ends up becoming the expert the practitioners rely on to understand their own broader practice.

In sum, working from the assumption that there is no one "core" or "right answer" and rather clarifying what is secret and what is complex, shows that secrecy is not necessarily something to overcome. The struggles and obstacles met on the way can be used to gain insights into the (dis)function of the field. Consequently, the secret is not necessarily something that has to be unveiled. As in in *The Castle*, it is not K.'s access to the Castle and the seemingly non-existent authorities, but the quest and the dead ends that together paint a picture of the village, the authorities, and K.'s task.

References

Anwar, Tasniem. 2020. "Unfolding the Past, Proving the Present: Social Media Evidence in Terrorism Finance Court Cases." *International*

Political Sociology 14, no. 4: 382–98. https://doi.org/10.1093/ips/olaa006

Aradau, Claudia, and Lucrezia Canzutti. 2022. "Asylum, Borders, and the Politics of Violence: From Suspicion to Cruelty." *Global Studies Quarterly* 2, no. 2: 1-11. https://doi.org/10.1093/isagsq/ksab041

Balmer, Brian. 2012. *Secrecy and Science: A Historical Sociology of Biological and Chemical Warfare*. London: Routledge.

Belcher, Oliver and Lauran L. Martin. 2013. "Ethnographies of Closed Doors: Conceptualising Openness and Closure in US Immigration and Military Institutions." *AREA* 45, no. 4: 403-410. https://doi.org/10.1111/area.12048

Best, Jacqueline, and William Walters. 2013. "Translating the Sociology of Translation." *International Political Sociology* 7, no. 3: 345–349.

Birchall, Clare. 2011. "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness." *Theory, Culture & Society* 28, no. 7–8: 7–25.

Birchall, Clare. 2014. "Aesthetics of the Secret." *New Formations* 83: 25-46.

Bosma, Esmé. 2020. "Multi-sited Ethnography of Digital Security Technologies." In *Secrecy and Methods in Security Research. A Guide to Qualitative Fieldwork*, edited by Marieke de Goede, Esmé Bosma, and Polly Pallister-Wilkins, 193-212. London/New York: Routledge.

Bosma, Esmé, Marieke de Goede, and Polly Pallister-Wilkins. 2020. "Introduction: Navigating Secrecy in Security Research." In *Secrecy and Methods in Security Research. A Guide to Qualitative Fieldwork*, edited by Marieke de Goede, Esmé Bosma, and Polly Pallister-Wilkins, 1-27. New York: Routledge.

Bousquet, Antoine, Jairus Grove, and Nisha Shah. 2020. "Becoming War: Towards a Martial Empiricism." *Security Dialogue* 51, no. 2-3: 99-118. https://journals.sagepub.com/doi/epub/10.1177/0967010619895660

Campbell, David. 2003. "Cultural Governance and Pictorial Resistance: Reflections on the Imaging of War." *Review of International Studies* 29, no. 1: 57–73.

Dijstelbloem, Huub, and Annalisa Pelizza. 2020. "The State Is the Secret: For a Relational Approach to the Study of Border and Mobility

Control in Europe." In *Secrecy and Methods in Security Research. A Guide to Qualitative Fieldwork*, edited by Marieke de Goede, Esmé Bosma, and Polly Pallister-Wilkins, 48–62. New York: Routledge.

De Goede, Marieke. 2020. "Secrecy Vignettes." In *Secrecy and Methods in Security Research. A Guide to Qualitative Fieldwork*, edited by Marieke de Goede, Esmé Bosma and Polly Pallister-Wilkins, 175-192. London/New York: Routledge.

De Goede, Marieke, Esmé Bosma, and Polly Pallister-Wilkins. 2020. *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. New York: Routledge.

De Goede, Marieke, and Mara Wesseling. 2017. "Secrecy and Security in Transatlantic Terrorism Finance Tracking." *Journal of European Integration* 39, no. 3: 253–69. https://doi.org/10.1080/07036337.2016.1263624

De Jong, Jorrit, and Gowher Rizvi, eds. 2008. *The State of Access: Success and Failure of Democracies to Create Equal Opportunities*. Washington DC: Brookings Institution Press.

DeNardis, Laura. 2014. *The Global War for Internet Governance.* New Haven: Yale University Press.

Derrida, Jacques. 1994. "To Do Justice to Freud: A History of Madness in the Age of Psychoanalysis." *Critical Inquiry* 20, no. 2: 227-266. https://doi.org/10.1086/448710

Dunn Cavelty, Myriam, and Andreas Wenger. 2020. "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41, no 1: 5-32. https://doi.org/10.1080/13523260.2019.1678855

Dwyer, Andrew C., Clare Stevens, Lilly Pijnenburg Muller, Myriam Dunn Cavelty, Lizzie Coles-Kemp, and Pip Thornton. "What Can a Critical Cybersecurity Do?" *International Political Sociology* 16, no. 3.

Eule, Tobias, Lisa Marie Borrelli, Annika Lindberg, and Anna Wyss. 2019. *Migrants Before the Law. Contested Migration Control in Europe*. Cham: Palgrave.

Fassin, Didier. 2013. *Enforcing Order: An Ethnography of Urban Policing*. London: Polity.

Gartzke, Erik, and Jon R. Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace." *Security Studies* 24, no. 2: 316-348. https://doi.org/10.1080/09636412.2015.1038188

Glouftsios, Georgios. 2023. "Performing Secrecy: Hiding and Obfuscation in Frontex's Pushbacks Scandal." *Journal of Ethnic and Migration Studies*: 1-21.

Hoijtink, Marijn. 2014. "Capitalizing on Emergence: The 'New' Civil Security Market in Europe." *Security Dialogue* 45, no. 5: 458–75.

Horn, Eva. 2011. "Logics of Political Secrecy." *Theory, Culture & Society* 28, no. 7-8: 103-122.

Kafka, Franz. 2009 [1926]. *The Castle.* London: Penguin Modern Classics.

LeCompte, Margaret D., and Jean J. Schensul. 2010. *Designing and Conducting Ethnographic Research*. Lanham, MD: AltaMira Press.

Marcus, George E. 1995. "Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography." *Annual Review of Anthropology* 24: 95–117.

Maret, Susan. 2016. "The Charm of Secrecy: Secrecy and Society as Secrecy Studies." *Secrecy and Society* 1, no. 1. https://scholarworks.sjsu.edu/secrecyandsociety/vol1/iss1/1

McGoey, Linsey. 2012. "The Logic of Strategic Ignorance." *British Journal of Sociology* 63, no. 3: 553-576. https://doi.org/10.1111/j.1468-4446.2012.01424.x

Menetrier, Agathe. 2021. "Implementing and Interpreting Refugee Resettlement Through the Veil of Secrecy. A Case of LGBT Resettlement from Africa." *Frontiers of Human Dynamics* 3. https://doi.org/10.3389/fhumd.2021.594214

Ozkul, Derya, and Rita Jarrous. 2021. "How do Refugees Navigate UNHCR's Bureaucracy? The Role of Rumours in Accessing Humanitarian Aid and Resettlement." *Third World Quarterly* 42, no. 10: 2247-2264. https://doi.org/10.1080/01436597.2021.1928487

Rappert, Brian. 2010. "Revealing and Concealing Secrets in Research. The Potential for the Absent." *Qualitative Research* 10, no. 5: 571-587.

Salter, Mark B. 2006. "The Global Visa Regime and the Political Technologies of the International Self: Borders, Bodies, Biopolitics." *Alternatives: Global, Local, Political* 31, no. 2: 167–89.

_____. 2007. "Governmentalities of an Airport: Heterotopia and Confession." *International Political Sociology* 1, no. 1: 49–66.

_____. 2013. "Expertise in the Aviation Security Field." In *Research Methods in Critical Security Studies. An Introduction*, edited by Mark B. Salter and Can E. Mutlu, 105-108. New York: Routledge.

Schwell, Alexandra. 2019. "Navigating Difficult Terrain." In *Secrecy and Methods in Security Research. A Guide to Qualitative Fieldwork*, edited by Marieke de Goede, Esmé Bosma, and Polly Pallister-Wilkins, 80–96. New York: Routledge.

Shires, James. 2019. "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." *Journal of Cyber Policy* 4, no. 2: 235-256.

Shires, James, and Max Smeets. 2017. *Contesting Cyber*. December 13. Cybersecurity Initiative, New America. https://www.newamerica.org/cybersecurity-initiative/policy-papers/contesting-cyber/

Singer, Peter W., and Allan Freidman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.

Sommerer, Lucia. 2022. *From Black Box to Algorithmic Veil: Why the Image of the Black Box is Harmful to the Regulation of AI.* Nomos/Hart Blog. February 1. https://blog.betterimagesofai.org/from-black-box-to-algorithmic-veil-why-the-image-of-the-black-box-is-harmful-to-the-regulation-of-ai/

Stevens, Tim. 2016. *Cyber Security and the Politics of Time*. Cambridge University Press.

Stevens, Clare. 2021. "*Bounding" US Cybersecurity: Negotiating a Symbolic and Organisational Thing of Boundaries* (Doctoral dissertation, University of Bristol).

Stevens, Clare. 2019. "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet." *Contemporary Security Police* 41, no. 1: 129-152. https://doi.org/10.1080/13523260.2019.1675258

Sutton, Rebecca and Darsha Vigneswaran. 2011. "A Kafkaesque State: Deportation and Detention in South Africa." *Citizenship Studies* 15, no. 5: 627-642.

Taussig, Michael. 1999. *Defacement: Public Secrecy and the Labour of the Negative*. Stanford, CA: Stanford University Press.

Valdivia, Ana, Claudia Aradau, Tobias Blanke and Susan Perret. 2022. "Neither Opaque nor Transparent: A Transdisciplinary Methodology to Investigate Datafication at the EU Borders." *Big Data & Society* 9, no. 2. https://doi.org/10.1177/20539517221124586

Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press.

Walters, William. 2014. "Drone Strikes, Dingpolitik and Beyond: Furthering the Debate on Materiality and Security." *Security Dialogue* 45, no. 2: 101-118.

_____. 2015. "Secrecy, Publicity and the Milieu of Security." *Dialogues in Human Geography* 5, no. 3: 287–90.

Walters, William, and Alex Luscombe. 2016. "Hannah Arendt and the Art of Secrecy; Or, the Fog of Cobra Mist." *International Political Sociology* 11, no. 1: 5-20. https://doi.org/10.1093/ips/olw027

Wesseling, Mara, Marieke de Goede and Louise Amoore. 2012. Data Wars Beyond Surveillance. *Journal of Cultural Economy* 5, no. 1: 49-66.

Yanow, Dvora and Peregrine Schwartz-Shea. 2006. *Interpretation and Method. Empirical Research Methods and the Empirical Turn*. Armonk/London: M. E. Sharpe.