The technopolitics of cybersecurity

Sociotechnical configurations, epistemic devices, and the production of knowledge

Aanonsen, C.E.

Publication date
2025

2

Chapter two: Research design

2.1 Introduction

The journey of writing this thesis has been one of "making sense of making sense" (Jackson, 2014). This chapter shows how the research has methodologically embraced an interpretive and reflexive approach, and how methodological choices play into the questions posed and the forms of knowledge that can be produced. While I explore cybersecurity knowledge production in sociotechnical configurations, it zooms in on the *effects* of these: How danger, hereunder categories of 'vulnerability', 'threat', and 'risk' are rendered intelligible and actionable, and how this plays out in the technopolitics of security governance and order. Rather than treating them as pre-existing objects awaiting discovery, danger is constituted through specific technologies, institutional arrangements, and epistemic logics. In this sense, the trajectory of this research does not get comfortable with any ontological assumptions. It is operationalised show that there are ways of exploring sociotechnical configurations empirically by looking at the underlying assumptions about *security* in contrast to *insecurity*, and how dichotomies inform the basis for technological design and engineering, discourse, and practices. As illustrated in Chapter 4, automation and machine learning utilised to amplify the detection sensors within networks do not deliver the seamless oversight or predictive control often promised through envisioned 'total security' augmented by artificial intelligence. Interpretation and engagement with these technologies reveal instead a clear understanding of human responsibility, alongside a strong commitment to the militarised logic of 'knowing the unknown' enemy (Aradau and Blanke, 2018).

While this thesis is dedicated to a "configurational analysis of social action" (Jackson, 2014, p. 269), it also encompasses material-discursive practices (Aradau, 2010),

where the amalgamation of practice, discourse, and technologies are studied as constitutive of the political enactment of knowledge. Hence this thesis is organised in chapters based on independent research articles that each contribute with empirical studies on distinct configurations. In its entirety, it contributes to studies of technopolitics across disciplines by reconceptualising cybersecurity not as a bounded domain or object but as *knowledges*, and how different knowledges are configured. This sociotechnical world is explored, and can be understood, through *how* knowledge is produced. This perspective challenges dualisms between the human and non-human, or the social and technical (McCarthy, 2017). Importantly, it also avoids the limitations of operating at levels of analysis relying on dichotomies between the local, national, and international (Edwards, 2002).

This methodological orientation, however, does not embrace a 'flat ontology' where agency is equally distributed among *actants*, including humans, non-humans, and concepts (Latour, 2005), but instead reimagines concepts such as power, structure, and system in light of the inextricable relations among social beings and technologies. By rejecting both representationalism and dualisms, I emphasise the co-production of ways of knowing (epistemology) and ways of being (ontology). By adopting an *onto-epistemological* stance (Barad, 2007; Massumi, 2015), I situate the research with a lens that considers knowledge production in a social world as it is experienced and how security and technology inhabit these environments. The world is not a collection of static entities, such as 'threat', to be observed, but a dynamic field of *becoming* in which perception and participation co-produce what is, and what is known (Massumi, 2015). From there, the underpinning of sociotechnical configurations in making threat something certain, intelligible, and actionable within environments is a space that can be explored empirically. As machine learning increasingly subsumes everyday practices of security, by which algorithms are trained on mass collections of data, for instance, this only calls for deeper inquiry into the situated contexts in which machines operate, producing notions of (un)certainty and outcomes that portray the world as a calculable place of politics and inherent insecurity.

With an onto-epistemological lens I show how diverse, uncertain, and open-ended ecosystems not only make danger intelligible but *operational* by meaningfully articulating (in)security and (un)certainty also in the engineering of technical systems. Yet, as the next Section 2.2 on methodology further details, any analytical intervention is necessarily partial and reflexive. Methodological choices foreground some realities while obscuring others –

both in settings of security and politics as well as by conducting research in search of *meaning*. The methodological lens of this thesis thus adopts a multi-scalar, multi-perspectival approach to empirical inquiry, using varied methods – interviews and textual analysis – to illuminate the logics underpinning sociotechnical configurations. The following section sets out to illustrate the epistemological and methodological commitments underpinning the research. In Section 2.3, I then show how data collection and analysis has been guided and has informed the study, while remaining interpretive and reflexive, particularly through interviews and textual analysis. Finally, in Section 2.4, I reflect upon research ethics and the practice of 'navigating secrecy' and spell out the inherent limitations of the research design and its article-based format.

2.2 Methodology

Research itself is a knowledge-making practice. Since methodology refers to the overarching rationale guiding research, it is essential to draw out the guiding principles and philosophical orientation that informs how knowledge is acquired and interpreted. The interpretive orientation of the research is grounded in a reflexivist ethos that acknowledges the co-production of the researcher, research settings, and method. Reflexivity as a methodological underpinning preserves the interpretive agency of myself as a researcher and the objects of study (Jackson, 2014). Since interpretations are always situated and historically contingent, they do not yield epistemic neutrality. Social actors produce meaning, which is, in turn, interpreted by scholars, but also embedded and co-produced by the tools that social actors engage with. Meaning, then, is not assumed to reside in texts or technologies, but emerges through contextually situated practices of interpretation. Cybersecurity is treated as an area of study in which various actors, institutions, technologies, and epistemic cultures generate, contest, and stabilise knowledge claims. These claims are embedded in, and configured by, epistemic devices such as intrusion detection systems, certification protocols, or standardisation schemes – material *dispositifs* that, drawing on Foucault (1977) and later feminist technoscience scholars (Barad, 2007; Suchman, 2007), may be (re)conceptualised as sociotechnical configurations of practices, technologies, and discourses.

In short, the methodology guides how I respond to my question of how knowledge about cybersecurity is produced, and the tools I use to do so. With the interpretive approach

I explore subjective and sociotechnically produced onto-epistemologies in the context of cybersecurity. Rooted in traditions of hermeneutics and phenomenology, interpretive approaches challenge normative and positivist assumptions of objective knowledge (Yanow and Schwartz-Shea, 2014). Along these lines, I focus on uncovering the depth and complexity of sociotechnical phenomena, aiming not for generalisation but for rich, contextualised insights. Methods are thus not neutral containers but are themselves productive of particular experienced realities. They shape the kinds of questions that can be asked and the forms of knowledge that can be produced. In this sense, the methodology operates performatively and participates in the world-making practices it seeks to study.

Interviews can be interpretive (Soss, 2014). As further detailed in Section 2.3, my open-ended and informal interviews have not been a task to uncover objective facts but to explore epistemic encounters as sites of co-production in which the discursive and affective dimensions of cybersecurity knowledge come into view. In the same way, textual artefacts, or documents, have served the same purpose: I have sought to understand how texts are situated within particular technical environments and social, cultural, and historical contexts (Yanow and Schwartz-Shea, 2014). As I extract *meaning* from texts, this meaning is not fixed but co-constructed by the document itself, its context, and the reader (Suchman, 2000). Through this lens, I seek to understand how social, political, and technical possibilities are conditioned by their relationality through which 'danger' and its remedies are rendered visible, intelligible, and actionable.

With this methodological context, I can study the interplay between knowledge production and technology as processes of meaning-making and sense-making (see Section 5.5). Cybersecurity, as an empirically situated research site, is, inevitably, onto-epistemological (Barad, 2007). What I mean is that technical means (materiality) are manifested through devices. This is exemplified as the categorical quantification of variables for 'danger', such as 'vulnerability' in protocols for standardisation (Chapter 3), sensor-based surveillance systems (Chapter 4), and risk assessments (Chapter 5) that play into the imaginaries and possibilities for political action. Stringent taxonomies for risk and vulnerability materialise and force systems of alignment across institutions, government, and corporations. What then becomes noteworthy is how technologies for knowing danger come into being as they shape, and are shaped by, the meaning they are ascribed, and how they subsequently render the world into a calculable place where reality – or danger/risk – can be 'perceived'. This ontological assumption and how it is enacted is explored in detail

in Chapter 4, where military ideals of achieving 'situational awareness' are appropriated for cybersecurity technologies, subsequently producing meaningful interactions with data outputs as accurate and objective knowledge.

Rather than treating cybersecurity as a bounded technical field, interpretive and open-ended study on knowledge production foregrounds how onto-epistemologies come to light within specific sociotechnical configurations for cybersecurity. Put simply, it is a methodological commitment that enables a study of situated knowledges and practices that activate a particular way of presenting the world to us, thus giving us a way to uncover the dominant views and priorities that prevail, irrespective of ostensible good will or intent. Understanding cybersecurity this way demands focusing on the ways in which technologies are *invested* with meaning, agency, and political significance. Technologies are not passive instruments but are active participants in shaping and stabilising epistemic claims. Indeed, this thesis treats knowledge production not simply as methodological tools but as sites of inquiry in their own right – asking not just what is known about threat, but how and *through which sociotechnical means* such knowledge is made and politically actionable.

Bricolage

The 'bricoleur' of the thesis as well as its individual chapters are informed by the methodological sensibility of *bricolage* (Latour, 1981, p. 62), understood not merely as a pragmatic assemblage of diverse methods, but importantly as *method-as-experimentation* (Aradau et al., 2014). Experimentation here refers not to experiments in the 'laboratory' but to *experience*. As has been suggested with the analytical concept of 'tinkering' (van der Kist, 2024), it refers to an improvised, iterative, and adaptive mode of engaging with problems, tools, or situations using what is readily available, rather than following a fixed plan or standardised method (see also Bellanova and de Goede, 2022). As a scientific practise and methodological lens, it allowed for emphasis on investigation, responsiveness, and context-specific adjustments. Importantly, this is the premise for operationalising a study of multiple knowledges, and how these knowledges mobilise across various research sites. Bricolage is a material and relational practice in itself through which knowledge, technologies, and solutions are co-produced in contingent and situated ways. Rather than aiming for perfection, 'ideal types', or universality, bricolage, or tinkering, allows for challenging universalisms in cybersecurity, through studying partiality, flexibility, and the

capacity to work with uncertainty and complexity without risking oversimplifications (as discussed in Section 1.4).

Following the methodology of bricolage, I resist rigidly prescribed frameworks in favour of methodological creativity, adaptability, and reflexivity. It is particularly suited to research questions that traverse scale (Basaran, et al., 2016). The complex, heterogeneous terrain of the security, technology, and politics of cybersecurity can be understood without reverting to the state or the international as a fixed analytical unit. As Aradau et. al. (2014, p. 85) articulate, bricolage enables researchers to "experiment with methods to open up different ways of knowing and experiencing the political". This ethos resonates with the thesis's broader commitment to uncovering the contingent, multiple, and unstable ecosystem of devices and infrastructures of cybersecurity knowledges. For instance, as shown in Chapters 4 and 5, automation and machine learning for cybersecurity practices and technologies (specifically anomaly detection) reconfigure knowledge: By shifting the focus from identifying previously known patterns of malicious activity to detecting irregular behaviour, I show how meaning/sensing (Chapter 5) and, specifically, 'situational awareness' (Chapter 4) for cybersecurity emerge not as a product of automation alone but as a reflexive sociotechnical accomplishment that relies on the practical interplay of probabilistic machine signals and situated human-machine interpretation. With a commitment to bricolage, it can be understood as a *situated* awareness, which is not merely about how data is perceived, but rather a recursive feedback loop where individuals in a system remain ostensibly critical and aware of how technologies and their own perceptions, biases, and interpretative frameworks shape renderings of 'the situation'.

Furthermore, the idiom of co-production (Jasanoff, 2004) is central to my methodological commitment to bricolage. Co-production emphasises the reciprocal shaping of science, technology, and social order, allowing for an examination of how scientific and technological objects – far from being merely instrumental – are implicated in the governance of security, the distribution of authority, and the delineation of what counts as credible knowledge. When studying risk assessments, such as detailed in Chapter 5, a comparison of systems and practices in counterterrorism and cybersecurity shows how ideas and classifications of 'risk' are highly contingent on the mechanisms put to use irrespective of their intent. In contexts where automation and machine learning are increasingly embraced for intrusion detection systems for cybersecurity, 'risk' becomes a way of 'sense-making' without a reconceived idea of the potential harm to be prevented.

The threat is 'unknown' and empirically produced. Risk assessments in the UK's Prevent programme, on the other hand, operate with clear and calculable indicators of risk leading to harm, with embedded assumptions of causality. The point is to show how despite having an identical ambition – preventing harm from occurring – different tools, mechanisms, and logics to assess 'best practices' for doing so result in diverting conceptualisations of risk with implications for the production of threat and (in)security. Rather than being fixed, risk and (in)security are perpetually co-produced with the tools used for assessment.

By extension, Sheila Jasanoff and Sang-Hyun Kim's (2015, see p. 3) concept of 'sociotechnical imaginaries' shows how visions of the future shape and are shaped by technological development. For instance, they show nonfictional accounts too often overlook the imaginative labour involved in technological development. Take, for instance, science fiction. Works such as Frank Herbert's *Dune* or Isaac Asimov's *Foundation*, published in the 1950s and 60s respectively, are only a couple of examples of a longstanding tradition in fiction that has experimented with imaginaries of omniscience in the entanglement of humans, technology, and social order. While often relegated to the literary genre of fantasy, these cultural artefacts play a powerful role in shaping imaginaries of technological possibility and political inevitability (Jasanoff and Kim, 2015, p. 337). In the words of one of the most celebrated science fiction authors Ursula le Guin,

> Science fiction is not predictive; it is descriptive… But our society, being troubled and bewildered, seeking guidance, sometimes puts an entirely mistaken trust in its artists, using them as prophets and futurologists… science fiction isn't about the future… Science fiction is metaphor. What sets it apart from older forms of fiction seems to be its use of new metaphors, drawn from certain great dominants of our contemporary life—science, all the sciences, and technology, and the relativistic and the historical outlook… *the truth is a matter of the imagination*. (le Guin, 1976, foreword*, italics added*).

Albeit not collective (nor the 'truth'), multiple, or better yet, *infinite*, imaginaries are performative in shaping visions of the future and inform, and are informed by, machine design and engineering, as well as institutional cultures, norms, and practices (Mager and Katzenbach, 2021). Sociotechnical imaginaries are not epiphenomenal. The omniscient dream to achieve 'total security' is expressed in the perpetual trust in accuracy – 'more' data will naturally yield 'better' security (discussed in detail in Chapter 4, Section 4.4-5). Imaginaries are by no means apolitical or without consequence. In the example of Stuxnet, Chapter 6 critically examines what happened after its discovery, which brought on doomsday scenarios of futurisms of 'cyber war'. Multiple, contested, and commodified

threat narratives were embraced, translating into concrete governance practices and technological innovations. These configurations are precisely what forms the basis for the empirical inquiry of this very thesis. By exploring how speculative futures inform present policy and design, it draws attention to the anticipatory logics embedded in cybersecurity governance and the ways these imaginaries are enacted through discourses, devices, infrastructures, and institutional as well as cultural practices.

Finally, central to the 'bricoleur' of the thesis is the operationalisation of the concept of epistemic devices – the instruments, protocols, systems, routines – through which knowledge claims are generated, stabilised, and rendered actionable across various sites with different effects. As drawn out in Section 1.4, and analysed in Chapters 3 and 4, they include not only algorithms, platforms, and detection protocols, but also standards, metrics, and classificatory schemes that co-produce security onto-epistemologies. Rather than treating such artefacts as neutral tools or passive backdrops, this thesis draws especially on Lucy Suchman's human-machine (re)configurations (2006; see also 2012) to conceptualise them as active participants in sociotechnical configurations that shape the very conditions of knowing and acting in security contexts. Chapters 3 and 4 in this thesis show how devices participate in enacting authority, delimiting what 'counts' as credible knowledge. A methodological sensitivity to bricolage – *method-as-experimentation* (or 'tinkering') – allows for using epistemic devices as a tool that combines reflexivity, attentiveness to situatedness, and openness to methodological invention. It does not merely examine what is known, but interrogates *how knowing is done*, with the analytical tool of epistemic devices to uncover underlying assumptions and to what political effects. Across the next chapters, this approach sustains a critical engagement with the co-production of knowledge, technology, and security, revealing the heterogeneous and contested processes through which cybersecurity is open-ended and continuously (re)made.

Case selection

The cases explored in the analytical Chapters 3, 4, 5, and 6 are better understood as research sites because they are contextually situated. I operationalise the methodological logic of bricolage, as described in Section 2.2 – understood as *method-as-experimentation* (experience) (Aradau et al., 2014) – by reflexively engaging with the situated contexts which are, empirically, sociotechnical configurations unique to their environment. Since

there is no single, unified definition of cybersecurity and, by implication, insecurity, technologies, operators, politicians, and strategists will inevitably have widely different ideas about what cybersecurity is. The empirical sites in this thesis explore how cybersecurity is contingent on its operationalisation and how it is organised around the design, maintenance and use of technical mechanisms and organisational routines, and political objectives. Rather than following a uniform logic of case selection, I chose the different empirical research sites because of their capacity to show spaces where meaning and matter come into being (Barad, 2007). To be more specific, each of the cases are political arenas that explicitly enact cybersecurity, thus suitable sociotechnical sites to explore where authority and political order emerge or are transformed. Therefore, the analytical heterogeneity is a strength, rather than a weakness: Each empirical site allows for interpretive theoretical engagement that would not be possible from a rigid or representative design.

The first empirical site found in Chapter 3 is the EU Cybersecurity Certification Scheme based on Common Criteria (EUCC). The EUCC is compiled of technical evaluation protocols, formalised criteria, and conformity assessments, designed with the goal to regulate the development and distribution of cybersecurity technologies across the European Single Market. This site was chosen to foreground how seemingly technical instruments enact political authority and organise regimes of trust, accountability, and risk. Through exploring the dense textual protocols for testing conformity (such as rigorous scoring of a given products' AP) as epistemic devices, I find that standards are by no means mere technical artefacts but a mode of governance. The standards are developed from protocols that quantify and calculate simulated situations ('attacks') where the threshold for 'vulnerability' of the given product is negotiated among 'expert groups'.

The second empirical site is a distinct intrusion detection system (IDS) in Chapter 4. Norway's National Warning System for Digital Infrastructure was chosen because of an announcement made in 2023 that the system was 'upgraded' to incorporate automation and machine learning to improve the 'situational awareness' of the Norwegian Armed Forces. It invoked my curiosity toward what 'the situation' might entail (Hentschel, Krasmann, and Zebrowski, 2025). Through interviews with operators directly or indirectly involved with the warning system and all official documents referring to it within a distinct timeframe, I was able to interpretively explore how human *experiences* with automation and machine learning for cybersecurity is part of a (re)configuring threat epistemologies. The warning

system was not chosen as a representative technology, but as an empirical site through which the performativity of automated security could be investigated. Bricolage allowed a layered inquiry into sociotechnical practices, enabling analytical engagement with a 'situated' awareness and interpretive labour within cybersecurity practices and technologies.

The third empirical site is explored in Chapter 5, namely specific risk assessments: The U.S. government IDS entitled EINSTEIN and parts of the UK counterterrorism programme Prevent. While I approach risk assessments with a comparative sensibility, the aim is not to create a binary or typological contrast, but to 'experiment' with how different sociotechnical configurations co-produce conceptions of 'vulnerability', 'risk', and 'threat' in different ways. This difference is not interesting in and of itself but allowed for empirical reflection on the technologies and temporalities embedded in security governance. Thus, the comparison served as a ground for empirically showing how risk is not simply 'assessed' but actively constructed through the very tools of assessment.

The final empirical site, explored in Chapter 6, examines the infamous Stuxnet malware – not primarily as a cyber incident, but as a pivotal event when 'cyber' became treated as a strategic and intelligible concept within academic, governmental, and media discourse. This was the first study undertaken for the thesis and, in retrospect, it revealed key limitations in treating the event solely as a discursive object. While discourse analysis provides valuable insights into how language shapes security imaginaries, it overlooks the material dimensions through which knowledge is produced and stabilised. Technopolitics encompass not only discourse but also technical artefacts, institutional routines, and epistemic logics that co-produce authoritative knowledge. Focusing solely on the discursive representations of Stuxnet meant I did not fully account for the infrastructures and practices that enable such knowledge to circulate and sustain. The shortcomings of this study highlight my journey of "making sense of making sense" (Jackson, 2014). This realisation marked a significant turning point in my research, prompting a shift toward sociotechnically attuned analyses in the other chapters. Despite these limitations, the Stuxnet case remains a historically situated event that continues to inscribe meaning into cybersecurity practices and technical system design, sustaining imaginaries of future digital threats. It provided a critical entry point for reflecting on how strategic knowledge is discursively and temporally produced and helped reshape my approach to later empirical sites in a different manner.

2.3 Data collection and analysis

Texts and documents

Textual analysis, as an interpretive method, involves the close examination and interpretation of texts. In this thesis texts include government documents (draft resolutions, bills, whitepapers, budgets, reports, letters, and policy papers), acts and regulations, media statements, and technical manuals, protocols, and guidelines – to uncover the meanings, values, and assumptions embedded within them. Interpretive textual analysis is not only about identifying patterns or themes. It is a reflexive process that seeks to understand how texts are situated within particular social, cultural, and historical contexts. It acknowledges that meaning is not fixed but is co-produced by the text, its context, and the reader. Thus, textual analysis is inherently hermeneutic, emphasising the multiplicity of interpretations and the role of my own positionality in shaping meaning (Yanow and Schwartz-Shea, 2014). Human actions are not wholly determined by abstract plans but are instead contingent, context-dependent, and shaped by emergent interactions within specific environments. They are, in other words, *situated* (Haraway, 2016; Suchman, 2006, 2000). I view texts not as neutral containers of information, but as active participants in the production of social realities, shaped by and shaping the conditions in which they are read. Textual analysis, as I use it interpretively, similarly attends to how meaning is produced through contingent, contextual engagements with texts, rather than assuming static or universal interpretations or 'truths'.

In this sense, I treat texts as epistemic devices – interrogating how knowledge is made *with* the instruments, such as documents, that compute and represent information in particular ways. Texts are not simply translators or mediators. They are part of the microdynamics that make up the infrastructures that operationalise managerial, regulatory, and technical processes. Hence, in line with an infrastructuring approach to sociotechnical configurations, I do not treat the texts as passive conduits of information but as embedded in dynamic configurations that enact, stabilise, and contest the very notions through which cybersecurity (hereunder conceptions of vulnerability, risk and threat) becomes known, operationalised, and legitimised. They are heterogeneous and performative entities – vectors through which managerial, regulatory, and technical processes are enacted, translated, and maintained.

With the backdrop of methodological sensitivities presented above (Aradau et al., 2014), textual analysis here is conducted as a form of bricolage – a mode of experimental, situated inquiry that assembles diverse fragments of empirical and conceptual material to 'map' the contingent arrangements of knowledge and power. By mapping I do not refer to Latour's 'follow the actors' as a way of tracing actants and their relations to create complete map of a given research site as a preconfigured 'network' (Latour, 1987). Instead, mapping here signifies the effort to understand the processes through which knowledge is produced (Aradau et al., 2014). This necessitates a degree of abstraction, enabling methodological reflexivity that captures relationality as a logic. Such an approach aims to accommodate the empirical heterogeneity of imaginaries, practices, and material devices. For instance, in Chapter 3, the protocols for certifying digital products (ensuring standard compliance), is examined not as fixed guidelines, but practices and systems that are *designed* to enclose the world and stabilise a vision of (in)security predicated on total visibility, anticipatory control, and the privileging of particular security logics such as might benefit profit seeking corporations.

The standards themselves are neither developed nor examined as objective truths but how these 'best practices' reply on some sort of representation 'secure' (versus 'insecure') products. Standards are not arbitrary, nor invisible, but examined through their construction. Their construction and organisation – analysed in depth through the EU's standardisation project for cybersecurity – is a textual affair. Multiple so-called stakeholders and experts are assembled for the purpose of negotiating common 'best practices' for the assessment and certification of products and services. The scoring system for evaluating a product's attack potential (AP) or, in other words, the vulnerability of a given digital object, is not a set of objective indicators that determine the possibility of harm. The scoring system is developed and maintained through a highly contingent, instrumentalised, social and political process, informed by multiple and commodified imaginaries of the future, rather linear, static, and collective ambitions. Thus, while indeed being a textual process, through which it is analysed in Chapter 3, the text is not simply developed as a materialisation of managerial or technical routines, but produced in interplay with economic and political interests, institutional cultures, anticipatory rationalities, and the pursuit of omniscience by ostensibly producing calculable futures. Particularly in Section 3.5, the text (instructions for certifying product safety) is conceptualised as an epistemic device to highlight the dense ecosystem of multifaceted and

heterogeneous processes that underpin the complexity of the enactment of regulatory (and otherwise) intent for cybersecurity with highly political outcomes.

Conducted through bricolage, epistemic devices (in this example, the texts and documents) are not merely about what they *say* but about what they *do*, and how they might reflect and reinforce dominant ideological commitments to rationalism, objectivity, and centralised authority. I have thus been attentive to this in the analyses of government documents (the draft resolutions, bills, whitepapers, budgets, reports, letters, and policy papers) assembled in Chapter 4 and 5. With the multilayer reading as offered with a methodological sensitivity to bricolage, the texts provided both an important historical backdrop to the empirical sites, but the texts also served as sites themselves, where discourses across temporal and spatial environments could be understood through how they are used *in situ*. Rather than reducing complex phenomena to simplified categories, as routinely done in laboratory studies of ANT, I explore theoretical frameworks, conceptual tools, and empirical data as they come together as coherent logics. It is a way of attuning to the unexpected. It enables the articulation of complexity through a dynamic synthesis of theory and empirics (see an example of this in studies on warfare in Reichborn-Kjennerud, 2025). The bricolage is not merely an eclectic synthesis, but a methodological stance for exploding the obscure, complex, incomplete, and situated performativity of documents as both artefacts and actives in the co-production of cybersecurity.

As Lucy Suchman (e.g., 2000, 2023) reminds us, documents participate in the constitution of professional knowledge, projecting an image of comprehensive control while obscuring the contingent and often contested processes through which knowledge is enacted in practice. In this vein, Chapters 4 and 5 explore this performative dimension which becomes especially visible when turning to algorithms and machine learning. With claims that these technologies will optimise 'situational awareness' to detect threat and calculate risk, the templates upon which risk is assessed, the strategic documents and media statements that justify intervention, and the fiscal budgets allocating resources are all materials that articulate idealised workflows and rational procedures. Instead, institutional constraints, improvisation, and human judgment remain central and reveal the multiple and contested ways in which cybersecurity threat is made intelligible and actionable through means that legitimise, streamline, and rationalise structures. Texts as epistemic devices are generative: They make certain knowledges visible and actionable, while marginalising others. The production of 'vulnerability', 'risk', and 'threat' in these contexts is not only

anticipatory but involves the (re)calibration of what counts as 'normal' or 'anomalous', who decides, and on what basis. Interpretive textual analysis is a way of keeping open the multiplicity of imaginaries, devices, and epistemologies without collapsing or flattening them into totalising accounts. This requires methodological abstraction – not as detachment, but as a critical resource for theorising complexity without redundancy and reductionism. In this sense, textual analysis becomes a site for exploring how power, authority, and legitimacy are not merely represented but enacted through situated textual practices.

Interviews

In the studies presented in this thesis, interviews are not treated as neutral instruments for accessing objective facts but explored interpretively (Soss, 2014). They are explored as epistemic encounters – sites of co-production in which the discursive and affective dimensions of cybersecurity knowledge come into view. Between August 2022 and March 2024, I conducted 14 open-ended and informal interviews with security professionals, engineers, public officials, and other stakeholders directly or indirectly involved in the operation, governance, or strategic articulation of cybersecurity (see Annex A). The interviews enabled a 'mapping' of how threat is not only known but experienced, how practices of anticipation and mitigation are situated within organisational cultures, and how epistemic authority is enacted. In short, the interviews were themselves performative sites where cybersecurity was made thinkable, discussable, and governable. Specifically, in Chapter 4, on the Norwegian National Warning System for Digital Infrastructure, ten interviews were conducted with key individuals involved in its design, deployment, or strategic oversight. These included four computer engineers: two working on IDS development and data processing within the system, and two representing private sector entities bound by the Norwegian Security Act (2019) and therefore formal subscribers to the warning system. Additional interviews were held with one deputy from the Norwegian National Security Authority (NSM), one cybersecurity officer from the Norwegian Armed Forces, and four civil servants involved in drafting or implementing national cybersecurity strategy. Importantly, interviews with operators indirectly or directly involved with the warning system took place after the announcement of the upgraded system in 2023, providing temporal insight into how infrastructural transitions and institutional commitments were being interpreted and narrated in real time.

Methodologically, the interview process unfolded iteratively. Questions were adapted and recontextualised to suit the informal setting. The format allowed room for unexpected detours – revealing, for instance, how technical operators reflect on 'normal' versus 'anomalous' network behaviour and what automated intrusion detection systems powered by machine learning do for human labour and interaction between operators and the algorithmic systems for detecting threat. Notably, as detailed in Chapter 4, Section 4.4, none of the operators interviewed experienced automation as lessening nor simplifying the necessity for human labour in rendering system or network threats known. Rather, they were all attuned to a reflexive relationship to data outputs. This allowed for new perspectives on the promises of machine learning for anomaly detection, perspectives often overshadowed by the dominant ethos that 'more' data naturally yields 'better' security.

While the interviews offered access to individual perspectives and experiences with technologies, it also offered insight into institutional rationalities and epistemic cultures, perhaps unsurprisingly leveraged by private vendors who demand distinct tasks, consequently shaping the evaluative framework upon which operators enact. Thus, the accounts provided by interviewees illuminated the assumptions, temporal logics, and classificatory thresholds that animate daily practice but often remain invisible in official policy or technical documentation. In this way, interviews contributed to the study's broader aim of mapping the sociotechnical configurations of cybersecurity, not through direct revelation, but by rendering visible the tensions, normative commitments, and operational frictions that constitute the everyday operationalisation of onto-epistemologies that render the world knowable in a specific way.

By treating interviews as both methodological instruments and sites of situated knowledge production, they complement rather than merely corroborate the textual analyses by foregrounding the experienced epistemologies of cybersecurity, namely, embodied orientations, professional jargon, and institutional cultures through which (in)security is made intelligible and actionable. In other words, the interviews enabled a granular, reflexive account of how cybersecurity is experienced and negotiated, not just as a technical field, but as they are configured. They offered not access to hidden truths (Bosma, de Goede and Pallister-Wilkins, 2019) but invitations to explore how threat becomes known, contested, and operationalised across a fragmented landscape of actors, technologies, and the practice of managing uncertainty and anticipation.

2.4 Ethical considerations, navigating secrecy and limitations

Research ethics

Prior to any collection of data for this study, the research underwent ethical scrutiny and was formally approved by the Ethics Committee at the Amsterdam Institute for Humanities Research (AIHR).[6] This clearance process required careful reflection on a number of key ethical dimensions, including the potential for harm, respect for autonomy, informed consent, anonymity, and the vulnerability of participants. As part of this process, I also undertook a formal course in Research Data Management (RDM) organised by AIHR. This training deepened my understanding of best practices in data handling, storage, and protection in line with institutional and national standards. Importantly, the research also adheres to the ethical requirements of the Norwegian Centre for Research Data (NSD), now known as SIKT. This compliance was necessary due to the thesis' funding by the Norwegian Research Council under the CYKNOW project (grant no. 325297). The NSD/SIKT framework provided further guidelines concerning data minimisation, participant confidentiality, and long-term data archiving, thereby reinforcing the thesis' ethical foundations in accordance with international standards.

Ethical considerations were integral to the design, implementation, and authorship of this research project. Given the sensitivity oftentimes associated with cybersecurity as a field central to national security, where secrecy, confidentiality, and data protection are paramount, particular care was taken to ensure interviewees were clearly informed that they were under no obligation to reveal proprietary, classified, or otherwise restricted information. The focus of the study remained oriented towards their *ways of knowing* and communicating the strategic, technical, and institutional routines and practices, rather than concrete security vulnerabilities. This was intended not only to preserve the integrity of the research but also to safeguard participants and their organisations from unintended disclosure or reputational risk.

---

[6] The EC FGW project title is "2022-FGW_MED-15380 – PhD project Claudia Aanonsen".

Participants in this study were not drawn from vulnerable populations. All interviewees held senior roles within public institutions, organisations, or private corporations involved in cybersecurity policy and practice. Their professional standing and experience indicated that they were fully capable of providing informed consent and engaging in reflective dialogue about their work without exposure to personal risk. Nonetheless, careful ethical protocols were followed to protect the integrity and confidentiality of the information shared. Informed consent was obtained verbally, after participants were clearly informed about the aims of the research, the procedures for data storage and use, and their right to withdraw at any time without consequence. Anonymity was guaranteed to all participants, not only as an ethical safeguard but also as a methodological precondition for encouraging open discussion amid the 'grey zones' surrounding classified, operational, or politically sensitive topics. Several subjects – such as the precise technical configuration of IDS or protocols for organisational vulnerability assessments, as discussed in Chapter 4 – were explicitly deemed out of bounds due to their confidential nature. However, these constraints did not limit the analytical scope of the research. Instead, they were approached reflexively, following Bosma, de Goede and Pallister-Wilkins (2019), as productive limitations that foreground how secrecy is navigated, enacted, and justified in everyday practice. The interview process thus served as a site for exploring how actors articulate and negotiate their relationships with cybersecurity technologies within institutional, legal, and epistemic regimes of (non-)knowledge (Aradau and Perret, 2022).

All data collected during interviews were anonymised (see Annex A) and stored securely in accordance with both AIHR and NSD/SIKT data protection guidelines. Electronic files were encrypted and password-protected, and access to all interview materials was strictly limited to me. Data were retained only for as long as necessary to complete the analysis and write-up, after which appropriate data archiving procedures were followed in line with institutional data management policies. Beyond the data collection phase, ethical reflection also informed the authorship and collaborative aspects of this thesis. Chapter 5 of the thesis is co-authored (see 'Acknowledgement of co-authored chapter'). In line with the ethical standards articulated by the Norwegian National Research Ethics Committees for the Social Sciences and Humanities, as well as the Co-Author Declaration developed by the Ethics Committee at the Norwegian Institute of International Affairs (NUPI), the distribution of work and authorship responsibility was conducted

transparently and equitably. We jointly adhered to the principles outlined in the Vancouver Declaration, which requires substantive intellectual contribution, mutual accountability, and agreement on the final version of the co-authored work.

Limitations of the research design

A key limitation of this research design lies in the methodological positioning of myself as a researcher within a highly mediated and securitised field. While interviews and document analysis offer valuable insight into the epistemic and institutional logics of cybersecurity, they also foreground the necessity of reflexivity: My role as researcher is not external to the production of knowledge but embedded within the interpretive and representational dynamics that I seek to map. The partiality of access – especially in a domain characterised by secrecy and classification – means that what can be studied is not the 'entirety' of knowledge produced through technologies but the logics, imaginaries, and practices through which knowledge is made intelligible. Although ethnography is not employed in this study, its conceptualisation within STS offers a compelling framework for thinking about how knowledge and infrastructures are co-produced. In STS, ethnography is less about holistic cultural immersion and more a mode of empirical attunement to the mundane practices, devices, and relationalities through which technoscientific worlds are enacted (Mol, 2002; Suchman, 2007). Ethnographic sensibilities – particularly attention to situatedness, materiality, and multiplicity – can be valuable for exploring the fine-grained negotiations that stabilise knowledge for the functioning intrusion detection systems, certification schemes, or threat modelling protocols.

In the context of cybersecurity, such an approach could illuminate how anticipatory logics are routinised, how accountability is distributed across human and non-human actors, and how normative assumptions are embedded into sociotechnical configurations. However, the potential of ethnography is simultaneously curtailed by the limits of the access it demands. As Bosma, de Goede and Pallister-Wilkins (2019) argue, secrecy is not merely a barrier to research but a constitutive logic of security work itself, shaping what can be said, known, or even imagined. These conditions, then, exclude the sustained presence and observational intimacy that ethnography in the 'laboratory' often presupposes. Accordingly, while this thesis does not offer an ethnographic account of cybersecurity knowledge production, it draws on ethnographic commitments to situated inquiry to explore how cybersecurity is understood through the ways in which it is

envisioned and acted on among humans and technologies in their configuration (not in binary separation). It is not a question of creating an omniscient 'map' of knowledge but of understanding and studying the logics that underpin the different ways in which cybersecurity is made actionable and authoritative through omniscient promises of accuracy.

Finally, while there are always inherent limitations to any research project, this thesis has been based on a collection of independent research articles (all written within a three-year timeframe) rather than a monograph. An article-based thesis, while offering certain advantages, also presented me with limitations when compared to the traditional monograph format. Structurally, the article-based thesis allowed for the publication and peer review of the individual chapters as stand-alone scholarly contributions, facilitating the possibility of earlier engagement with academic communities and enhancing my visibility and academic credentials. Chapters 5 and 6 have been peer-reviewed and published. Chapters 3 and 4 are, as of June 2025, currently under review in high-ranking academic journals. Upon reflection, I am satisfied with the choice of writing an article-based thesis, especially because the format encouraged diversified and concise argumentation and methodological rigour tailored to journal standards. Also, as a result, I set shorter-term deadlines throughout the process for each article, which allowed better time management. However, an article-based format can pose challenges in achieving theoretical and conceptual coherence across the thesis as a whole. Furthermore, the need to conform to varying editorial guidelines can lead to stylistic and structural inconsistencies. There were, however, reformatted to fit the style of a coherent thesis as guided by the University of Amsterdam (Faculty of Humanities). Nonetheless, the article-based format has provided me the opportunity for interdisciplinary collaboration and co-authorship as offered in the comparative analysis in Chapter 5.

The next chapters of this thesis comprise four analytical studies (Chapters 3-6), each of which examine distinct empirical sites to show how categorical conceptions of danger, hereunder, 'vulnerability', 'risk', and 'threat' are produced. They focus on system design as epistemic devices to show how they enclose the world through calculable categories that delimit the enactment of cybersecurity. Each examine different configurations and their political effects, beginning with the study of the European Union standardisation project in the next Chapter 3, Norway's government IDS in Chapter 4, risk assessments across counterterrorism and cybersecurity in Chapter 5, and lastly the

discursive ramifications after the infamous Stuxnet malware in Chapter 6. Finally, Chapter 7 offers the thesis' conclusions, including conceptual, theoretical, and empirical contributions, as well as my reflections on political implications and avenues for further studies.