The technopolitics of cybersecurity

Sociotechnical configurations, epistemic devices, and the production of knowledge

Aanonsen, C.E.

Publication date
2025

1

Chapter one: Introduction

1.1 Introduction to the thesis

In 2010, two employees at a small Belarusian IT firm became aware of something out of the ordinary – a malware that would later become widely known as 'Stuxnet'. Little did they know that these pieces of code would go on to entirely transform global understandings of cybersecurity and the subsequent politics of securing our digital futures. Stuxnet is now notoriously famous for being part of 'Olympic Games' – a covert and complex operation organised to undermine Iran's nuclear programme from the early 2000s onwards (Sanger, 2012; Zetter, 2014). The American- and Israeli-led operation was allegedly arranged to sabotage centrifuges for uranium enrichment at the Natanz facility in Iran by distorting the display of sensor data, causing the rotation of the centrifuges to malfunction due to faulty settings. Eventually, the centrifuges physically broke (Falliere, O'Murchu and Chien, 2011). Stuxnet was quickly branded a new type of weapon, one where sabotage could be conducted covertly and by proxy through computational networks. The long history that has reoriented the focus of international security towards critical infrastructures as targets of warfare was now coupled with the fear that 'invisible' cyberattacks could cause physical harm through networks from afar.

The magnitude of reactions after Stuxnet was extraordinary. 'Cyber war' – the idea that war could be waged entirely though computers – was presented as a realistic scenario, supported by a series of alarmist political statements and media coverage. Strands of academia also oriented themselves toward the cyber war scenario, particularly focused on digital technologies as both a weapon and a deterrent in 'cyberspace' after NATO recognised it as its fourth military domain at the Warsaw Summit in 2016 (Libicki and Tkacheva, 2021). From 2010 onwards, Stuxnet has become regarded as a paradigm for contemporary discourse on cybersecurity. Its discovery and the subsequent proliferation of 'cyber doom' scenarios activated new military and political priorities for national and international security strategies. Cybersecurity has since become fully incorporated into the lexicon of states as an all-encompassing term describing the necessary means to engineer security into the design of critical infrastructures such as databases, communication lines, engines, and their control systems. Thus, cybersecurity became a key policy area, a major industry, and a top priority in most national security strategies across the globe.

Historically speaking, a lot appears to have happened in a short period of time. Under the aegis of 'rapid technological development', state leaders and private corporations have since stressed the need to 'keep up' with the world of technological developments – which is nearly impossible to legislate 'in time' – and the now-important demand to determine norms for acceptable behaviour in 'cyberspace' (Osula and Rõigas, 2016). Notably, however, in June 2025 (fifteen years after the discovery of Stuxnet) Israel and the U.S. again directly targeted the centrifuges at Natanz (Gritten, 2025). This time around there was no complex cyber operation, but a series of military airstrikes targeting Iran, including several other nuclear facilities. The idea that inherent vulnerabilities in digital infrastructures (online and interconnected networks and systems) would backfire to the degree that a 'cyber-Pearl Harbour'[3] would occur and switch off an entire country has, as of today, not materialised (Lawson and Middleton, 2019). It comes to show that the futurisms of cyber war as it was presented post-Stuxnet have not yet happened and that conventional bombing has not wholly been replaced by cyber weapons as predicted.

This is not to deny the importance, nor possibility of societal disruption caused by digital technologies and their interconnectedness. I do stress, however, that there is another side to the coin – a counterpoint to the essentialist descriptions of cyber incidents as existential threats, and cybersecurity as solely a technical or strategic tool. The problem for these accounts is that 'high politics' describe and enact a particular version of cybersecurity, one that only brings attention and offers solutions to cyber incidents concerning national security. They produce a universalised gaze on what constitutes danger and insecurity, and how to avoid it, sidelining the often-unintended effects of the design and engineering of

[3] 'Cyber-Pearl harbour' was stated as a possible outcome of future cyberattacks against the U.S. in a 2012 speech by then-U.S. Defence Secretary Leon Panetta.

cybersecurity technologies and how they are mobilised for security purposes, with already severe consequences. Accordingly, the world is enacted as a place of pervasive and inherent insecurity, producing a distinct and sometimes irrefutable sense of danger, with deeply problematic implications for societies and individuals. The question remains as to how these technologies are mobilised, and how it transforms modes of security governance that subsequently define security *for whom*, *by whom*, and *for what purpose.*

Instead of cyber war, the continuous digitalisation of societies and tools of warfare emphasises that computational infrastructures are politicised, contested, and technically contingent domains. In strategic plans and technical documents, cybersecurity is generally framed as the necessary protection of digital systems and networks harbouring data. Its conceptualisation ranges from a *technical capacity* (software, hardware and human skills to map and avoid the damage, theft, or disruption of systems and networks that harbour data), *strategic means* (a plan of action to avoid damage, theft, or disruption of systems and networks), and *policy* (standards or protocols for regulating behaviour). For instance, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) defines cybersecurity as

> the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. (CISA, 2021).

Said otherwise, for CISA, cybersecurity becomes enforced under a narrow understanding that conditions contemporary societies: The necessary means to 'discover' and counter potential criminal abuses of the confidentiality, integrity, and availability of information as inevitable vulnerabilities that accompany the proliferation of ever-advancing technology. But nothing is simply discovered, it is always made. The problem for cybersecurity is not only how it is treated among authorities, policy strategists, and oftentimes technical operators as a strategic tool, but universalist and imposing claims to *what* threatens. Enforced claims to what cybersecurity *is* culminate into the enactment of omniscience – a belief that technology can deliver 'total security', enabled through a militarised logic that rests on the equation that *more data equals better security* (Aradau, 2023; Aradau and Blanke, 2017).

Cybersecurity concerns a lot more than securing data from theft or sabotage. In this thesis, I critically challenge and reframe dominant understandings and rationalities of cybersecurity that are *designed* to enclose the world and stabilise a vision of order predicated on dreams of 'total security' – visibility, accuracy, and anticipatory control. There is no single, unified definition of cybersecurity and, by implication, insecurity: A politician, military strategist, or computer engineer will unavoidably have radically different ideas about what cybersecurity is, who it is for, and how to operationalise it. Cybersecurity is contingent on its operationalisation and how it is organised around the design, maintenance and use of technical mechanisms (e.g., encryption, sensors, and firewalls) and organisational routines, institutional cultures, socioeconomics, and political objectives. For instance, as shown in the empirical analysis in Chapter 4, cybersecurity operators rarely experience any influence over the purpose or implications of a given assignment. The objectives for cybersecurity are typically determined (and funded) by governments (non-technical experts) or vendors. They have their own ideas of what threatens (such as certain foreign states or 'criminals') and allocate the means to which threats can be seen, known, and dealt with. Therefore, I argue, cybersecurity must be studied as multiple knowledges, contingent on how social, political, technical, and historical knowledges are mobilised and enacted in different sites, and with largely different political effects.

To do so, I understand cybersecurity systems not as merely reactive but constituted by an ecosystem of mundane everyday practices of security that endeavour – intentionally or not – to align with a technopolitical logic that enforces a universalised gaze of what cyber threat is, and how to address it. As has been for long argued by critical theorists, claims to security politically enacts a world of pervasive and inherent *in*security, producing a categorical sense of danger that legitimises expansive surveillance practices under the guise of national security (Buzan, Wæver and de Wilde, 1998; Huysmans, 2006). These practices reflect dominant Western imaginaries, universalising specific cultural and political anxieties while potentially marginalising alternative epistemologies and lived realities. As a result, security is prioritised for certain populations – typically within powerful states – while others are subjected to heightened scrutiny and digital policing (Kazansky and Milan, 2021; Milan and Treré, 2019). This framing transforms conceptions of warfare and violence, normalising digital weaponisation and pre-emptive interventions as rational responses to a supposedly ever-present threat. It enables powerful actors to exert control in the name of protection, diminishing individual autonomy and eroding democratic oversight in both domestic and transnational contexts.

In a critique of normative assumptions embedded in the design and politics of (cyber)security governance that rely on power asymmetries to legitimise digital surveillance and preemptive intervention, I resist the closure of the world as a place of inherent insecurity. I do so to expose the perpetual and distinct ways of designing, using, and maintaining technologies for security purposes (Suchman, 2006). This thesis contributes with a conceptual vocabulary to empirically intervene on the engineering of fixed ideas of danger, and how cybersecurity might be enacted otherwise. Ultimately, this thesis contributes to a broader critical project that reasserts the political stakes of cybersecurity and insists that the question of how we respond to insecurity must remain open to democratic contestation and critical inquiry. Therefore, I ask: *How does the production of cybersecurity knowledge shape the technopolitics of security governance - and what are the implications?*

I approach this question through four empirical chapters to show how cybersecurity is a technopolitical project that reproduces new forms of hierarchy, erodes democratic oversight, and transforms everyday security practices into instruments of algorithmic governance and political control. Technopolitics, drawing on Gabrielle Hecht (2011), is the use of technology to enact political goals, in which “sociotechnical systems that emerge out of such arrangements tend to reflect, and seek to reproduce, the hierarchies and inequalities of particular societies” (Müller and Richmond, 2023, p. 4). While often considered circumstantial to great power technopolitics, transformative innovations, and large technology corporations, I explore how the mundane experiences of everyday technologies harbour, facilitate, maintain, and disrupt the means upon which we create technical, historical and scientific knowledge. Importantly, *knowledge is always local*. By local I refer not to a level of study, nor to partiality, but to *ways of knowing*. While always partial to some capacity, these ways of knowing are conditioned by specific environments that organise patterns of knowledge and behaviour (Haraway, 1988). Like historical knowledge, scientific/technical knowledge is also local: It is learned, maintained, forgotten, and remade. Human existence is intellectual and material, but also ontologically arbitrary and full of mystery. Yet the world is enacted as a rational and factual place. It is organised politically based on a selection of rational, intelligible and coherent knowledge composed and represented as logics of *reason*. The organisation – or *body* – of knowledge is labelled and engineered through technologies – books, databases, computers, algorithms – necessarily adapted to a given environment. Reason is, in other words, always made and remade, a fraction or glimpse that is local, contextual, and *situated* (Suchman, 2006; Haraway, 1988, 2016).

The history of the emergence of cybersecurity as key to identifying, mapping and knowing 'danger' reveals a gradual reconfiguration of ways of knowing threats to society and national security. Different and emerging strategies, methods, and tools (such as machine learning techniques) for calculating, capturing, and 'neutralising' danger have empirically relied on the enduring promise of accuracy and the premise that the world can be computed into a legible and calculable place (Bousquet, 2018; Suchman 2023). That means that the driving logic for cybersecurity is that the more data available, the more analysts and computers can 'see', 'know', and 'do'. Crucially, the digital technologies at hand to gather more data, better data – even synthetic data for training algorithms through machine learning – are not apolitical, neutral, or objective. In this vein, the relationship between humans and technologies is not fixed, not pre-given, but situated, and actively constituted through contexts where discourses, practices, and technologies 'come together'. They are, in other words, *configured*. Being 'configured' refers to the mutual constitution of users and machines (Suchman, 2006; see also Barad, 2007). Agency is an *effect of* configurations, meaning that a capacity to know and act is produced in constitution with machines. In this vein, cybersecurity knowledge always conditions, and is conditioned by the design and engineering of technologies. These technologies are highly political: They are flawed and they are *sociotechnically configured*.

Sociotechnical configuration is both a lens and conceptual tool to study how institutional norms and technical infrastructures collectively shape function and meaning – creating foundations for the technopolitics and security governance. Configurations *matter* and perpetually co-produce knowledge and ways of experiencing the world. As scholars of Science and Technology Studies (STS) have argued for decades, it conceptually resists binary and ontological separations of the social and the technical, resting on the mutual shaping of the world as it is experienced and enacted through material means (Barad, 2007; Edwards, 2002, 2010; Haraway, 2016; Suchman, 2006). With this in mind, I argue that understanding how cyber*security* is 'made' demands a focusing on how knowledge about *insecurity* is produced. Through configurations attention can be drawn to the fact that knowledge is created in unison with the means, or objects, used to understand the world. This includes how technologies are operationalised to see and know the world and its dangers, and the technopolitics aimed at preventing harm (such as cyber incidents) from happening.

It is well established that studying knowledge production is important for enactments of security, and how knowledge is tied up to the intended and unintended consequences of the design and maintenance of technical security infrastructures. Scholars of security have done so for critical infrastructure protection (Aradau, 2010; Collier and Lakoff, 2008; Dunn Cavelty and Kristensen, 2008; Hansen and Nissenbaum, 2009), borders and migration (Bourne, Johnson and Lisle, 2015; Dijstelbloem, 2021; Glouftsios, 2021), and financial flows (de Goede and Westermeier, 2022). Drawing on these literatures at the intersection of Critical Security Studies (CSS) and STS I offer empirically oriented analyses of how knowledge about *cybersecurity* is produced in sociotechnical configurations and subsequent implications for the technopolitics of security governance. My aim is to empirically highlight cybersecurity as part of unstable and open-ended ecosystems of matter and meaning. Instability is key here – there are no fixed, nor static dangers 'out there', nor an intelligible world to be 'discovered'.

Knowledge is, as mentioned, *local*, presupposing *particular* and *situated* actions and knowledges. Through textual analysis and interviews (see Section 2.3), this thesis explores distinct sociotechnical configurations and local – or situated – knowledges as empirical sites. As illustrated in Chapter 3, standards, and protocols for certifying compliance actively enables and constrains the design and distribution of digital technologies. It might appear to be an uneven process that quantifies values such as 'vulnerability' which become fed into a scoring system subsequently determining whether a product is suitable for distribution in a given consumer market. The design of the standardisation protocol is, however, by no means apolitical but informed by commercial interests and political preferences regarding what security *is*, on a contrary to what it is not. Furthermore, Chapter 4 illustrates how intrusion detection systems (IDS) for cybersecurity are commonly designed with the purpose of discovering unwanted activity within networks. IDS are not objective technologies for discovering danger, nor neutral methods upon which malware becomes visible. It is a sociotechnical process that *treats* data as objective representations and subsequently organises it into legible information to achieve or improve so-called situational awareness. The configuration of an IDS is a practice of assembling knowledge through a particular sociotechnical arrangement of information that is, in turn, accepted as a step towards discovering 'truth' (see also Bueger, 2015; 2024; Knorr Cetina, 1999).

The gradual incorporation of machine learning for training algorithms to distinguish normalcy from potential danger within computational networks further highlights how technologies are sociotechnically configured. As Chapter 5 shows, automation and machine learning transforms the premise of *how* danger becomes known (or 'sensed'). Conceptions of 'risk' are inherently partial, relying on the means of which it can be assessed relative to the harm it seeks to obstruct. Similarly, after Stuxnet was made public knowledge, as I examine in Chapter 6, a technical report based on so-called 'reverse engineering' was conducted by the multinational software company Symantec (now Gen Digital Inc.) to work out how the malware infiltrated the uranium enrichment facility in Iran. The report made several claims to Stuxnet being "entangled in the politics of nuclear proliferation, diplomacy, international law, and the mechanisms of global cybersecurity governance" (Stevens, 2020b, p. 130). 'Reverse engineering' is not some technically neutral or objective method. The process of investigating how Stuxnet infiltrated the Iranian facility, and the reporting of the incident was not an unbiased procedure but a lens and a specific tool that promoted certain interests and visions (e.g., commercial and political) over others – intentional or not. Symantec's report marked the beginning of commercial interest by articulating claims to how international dynamics were playing out through extension of states' so-called cyber capabilities (Falliere, O'Murchu and Chien, 2011). The history of cybersecurity as a remedy for the operationalisation of emerging technologies is one of how granting vast importance to new and emerging technologies guides *what* and *how* humans know – and what they *do not* know (Aradau and Perret, 2022).

The remainder of this introductory chapter outlines the thesis' main argument in Section 1.2, including how I respond to the research question, narrowing down to specific empirical questions posed in the analytical chapters. In Section 1.3, I outline the thesis' aim and contribution, especially focused on the empirical and conceptual contribution for studies on cybersecurity. Then, in Section 1.4, I situate the thesis within critical debates on cybersecurity and STS-informed perspectives for studying knowledge production in sociotechnical configurations. While drawing on these, I also emphasise limitations in dominating STS frameworks, including Actor Network Theory (ANT) and affordance literatures, that risk oversimplifying complex phenomena when they are generalised in ethnographic approaches for studies in the 'laboratory'. Turning to the merits of other STS frameworks, including infrastructures/infrastructuring, in Section 1.5 I conceptualise *epistemic devices* as a tool to empirically study local and contextual knowledge in a way that traverses scale. It supports an understanding of the ecosystems of infrastructural arrangements with implications for the technopolitics of security governance.

1.2 Cybersecurity as sociotechnical configurations

Thesis argument

In this thesis I argue that to uncover the way technology inhabits *ways of knowing* the world, enactments of (cyber)security, and the implications for the technopolitics of security governance, it is in due time that interdisciplinary studies of security advance decades of thinking about human-machine relations into more empirically oriented research. In the previous introductory section, I stated that studying knowledge calls for a commitment to grappling with cybersecurity or any technical infrastructure or device as inherently *sociotechnical* and *situated*. But to empirically study the production of knowledge and how it conditions future governance is contingent on examining ideas of cybersecurity for whom, by whom, and for what purpose. This thesis is inspired by Lucy Suchman's work on 'human-machine (re)configurations' (2006). With few (yet important) exceptions,[4] Suchman's framework has thus far not received much attention with regards to empirical questions of security. I take on the task of expanding on her significant work to study cybersecurity specifically, and to provide tools and critical thinking for grappling with the implications of emergent technologies that take centre stage in the technopolitics of security governance.

Sociotechnical configurations, in this context, *produce* meaning and thus the capacity of a given technology, agency, and the engineering of data that renders certain things knowable, and others not. This matters because problematising the driving assumptions of accuracy that underpin technopolitics, specifically contemporary discourses

---

[4] These exceptions have drawn on Suchman's work for studies on security, including algorithmic governance (Aradau and Blanke, 2022), warfare (Leese, 2019; Reichborn-Kjennerud, 2025), the work of sensors/sensing (Klimburg-Witjes, Poechhacker, and Bowker, 2021), and theoretical orientations at the intersection of CSS and STS (Evans, Leese, and Rychnovská, 2020) and IR and international politics (Hoijtink and Leese, 2019).

and computational practices and technologies of cybersecurity, is key to uncovering the perpetual taxonomical thinking and reproduction of what 'counts' as insecurity. In this vein, this thesis subscribes to the methodological principle that *materiality matters* (Aradau, 2010; Aradau, et al., 2014; Barad, 2007; Bennett, 2010; Kaufmann, 2024). I do not treat cybersecurity and the production of cyber threat as a solely anthropocentric affair but as an 'emergent security' (Fouad, 2021), by which the materiality of technologies activates a capacity to shape what security is and how it is understood. Technologies do not, however, exist independent of their inhabitancy of the social world or of human engineering. They are configured. The importance of this is the way sociotechnical configurations – such as those analysed in this thesis – embody a categorical production of 'vulnerability', 'risk' and 'threat' that reflect or reinforce dominant imaginaries – cultural, social or political – as *universal truths* (Dwyer, et al., 2022; see also Bellanova, 2023).

As will be detailed in the review of existing literature in Section 1.4, academic engagement has in recent years developed an agenda for research on cybersecurity beyond orthodox perspectives of International Relations (IR) as conditioned by the capabilities of states (Cristiano et al, 2024; Dunn Cavelty and Wenger, 2022; Fouad, 2021; Monsees and Liebetrau, 2024). However, for studies on cybersecurity there remains much to be gained from the plethora of research on knowledge production and technology to depart from dominant views of cybersecurity as merely a tool in the hands of state actors. I argue for drawing on the merits of STS, grounded in Suchman's aforementioned 'human-machine (re)configurations' and 'situated actions' (2006), as well as Paul N. Edwards' studies on 'closed-world discourse' (1996) and infrastructure (2002, 2010). Furthermore, this thesis is developed from the backdrop of International Political Sociology (IPS) (Bigo, 2006; Huysmans, 2006) and works at the intersection of Critical Security Studies (CSS) and STS (Aradau, 2017; Evans, Leese and Rychnovská, 2020; Hoijtink and Leese, 2019; Suchman, 2020). With these theories and frameworks on human-machine relationality in mind, I argue that now is the time to expand on these literatures towards more empirically grounded studies on knowledge production, (cyber)security, and politics as sociotechnical configurations.

I am not, however, concerned with the structuring and ordering effects of technology for governance and security (Adler-Nissen and Drieschova, 2019). Rather, I am attentive to perspectives that explore the configurations of matter and meaning (Barad, 2007) with an aim to traverse scale (Basaran, et al., 2017; Edwards, 2002). In IR, Latour and associated works are often critiqued for an exclusive focus on microprocesses, overlooking the necessary abstraction to the 'macro' as predominantly practiced in IR theory (Nexon and Pouliot, 2013). STS, however, has more to offer IR than just ANT and 'inscription' (as explained in Hoijtink and Leese, 2019; see also Latour, 1987; Latour and Woolgar, 1979; Walters, 2002). This includes, for instance, STS studies on infrastructures and infrastructuring (Blok, Nakazora and Winthereik, 2016; Bueger, 2015; Bueger, Liebetrau and Stockbruegger, 2023; Musiani, 2022). When studying infrastructure, as argued by Edwards (2002), micro, macro, and meso scales of force, time, and social organisation need not be synonymous with 'levels' of analysis, which are often reverted to in IR (see also Bowker and Star, 1999). Scale is not a natural or self-evident category, but rather constructed, tied to the epistemic and material conditions under which knowledge is produced and infrastructures are built. Elaborating on this, I show in my conceptualisation of *epistemic devices* in Section 1.5, building on Latour's 'inscription devices' (1987) and Amicelle, Aradau and Jeandesboz's (2015) 'security devices', that there are ways of studying the 'micro' that traverses scale. It allows for studying the making and maintenance of the ecosystem of uncertain, and unstable infrastructures, such as regulatory frameworks and infrastructural interdependencies for governance.

Epistemic devices are defined as *a tool for grappling with the vectors of knowledge production at the 'micro scale'*.[5] To study how the world is presented, interpreted, and subsequently enacted as a place of insecurity, the concept of epistemic devices is developed for examining the ecosystem of knowledge and practice, which as an infrastructure is open-ended and always in the making. Infrastructures, understood here as sociotechnical configurations, are the expansive and interconnected formations that shape, and are shaped by, epistemic practices across sites (Bueger, 2015). While useful for exploring the politics of governance, epistemic *devices* allow for exploration of micro processes, in other words, the mundane practices of everyday security that traverse scale and contribute to understanding, for instance, regulatory frameworks and infrastructural interdependencies (Edwards, 2002) – as ecosystems.

[5] 'Epistemic devices' has been used in other fields including linguistics (see Alonso-Almeida, 2014) and education (see Ramiel and Fisher, 2023). Here, I conceptualise it exclusively as an analytical tool for an STS-informed study of ecosystems of knowledge and practice for security.

For cybersecurity, 'staying with the trouble' (Haraway, 2016) of what 'counts' as security becomes imperative to understand how insecurity (such as categories of 'vulnerability', 'risk', and 'threat') is made (Bellanova, Jacobsen, and Monsees, 2020; Huysmans 1998; Buzan and Hansen 2009). What is at stake here is that cybersecurity knowledge shapes social and political orders as a condition of modernity and global (security) governance (Edwards, 2002). Through specific 'ways of knowing' security and, by implication, insecurity, enabled by practices of shaping (in)security through, for instance, risk assessments, intrusion detection sensors, and computational mapping of the world as a dangerous place, the world is also experienced as such. In other words, the world is (re)configured around the continuous and transformative digital development of 'high tech' and subsequent proliferation of insecurity (Suchman, 2006). Several political stakes emerge from computational representations of a dangerous world, in addition to the universalised gaze upon technologies and what counts as insecurity. One consequence is the continuous legitimisation and encouragement of invasive digital surveillance, further solidifying a world where digital domination subsumes everyday life. Ranging from commercialised market-driven logics to priorities of national and international strategists, it becomes a kind of strategic pre-emption that appears as the only rational approach to politics and security. The self-perpetuating, 'closed world' of cyber (in)security makes it more difficult to imagine alternatives than to try to 'keep up' with emerging and transformative technologies and attempt to legislate their design, production, and use 'in time'. Cybersecurity, through different operationalisations and tasks aimed at pre-emption, actively eliminates other possibilities for envisioning alternative futures – ones where digital (in)security is not an inevitable condition of modernity, nor a given way to prioritise someone's security over others.

The task at hand for this thesis, then, is to question, explore, open, and uncover how practices, knowledges, and technologies are *situated* (Suchman, 2006; Haraway, 2016). Thus, by empirically exploring *sociotechnical configurations*, the four independent empirical analyses in this thesis, presented in Chapters 3, 4, 5 and 6, illustrates how cybersecurity is enacted and in turn how this comes to shape social and political order. It bids an empirical question of how to explore the everyday practices and technologies of cybersecurity as an *interplay* of knowledge and technology. While research on human-machine relationality has hitherto been theorised in abundance across the interdisciplinary research detailed in Section 1.4, there is a space for assessing, or *diagnosing*, the present, namely the paradigm of cybersecurity that has brought into being a distinct role in shaping digital realities. I do so not with the intention to merely 'capture' the role of materiality or discourse, but rather to explore the relationality that underpins the nexus of technologies and social practises of knowledge production in the context of (cyber)security.

Research questions

Through the analytical Chapters 3-6, I explore and empirically illustrate knowledge production in distinct and situated sociotechnical configurations of cybersecurity. With the goal to show the implications for and by the technopolitics of security governance, I pose the following main research question:

How does the production of cybersecurity knowledge shape the technopolitics of security governance - and what are the implications?

While the main research question is addressed throughout the thesis, I respond to the query through four empirical analyses that zoom in on more specialised questions. First, in Chapter 3 I explore cybersecurity knowledge with regards to *standardisation* – not as an arbitrary process – but as epistemic devices that co-produce specific definitions of risk, vulnerability, and resilience. I ask: *How does standardisation enact political authority and render insecurity and risk calculable?* By empirically studying the standardisation of the production and dissemination of cybersecurity products and services in the European Union (EU), I show how this process has a profound political impact and does not only function as a technical, managerial or regulatory tool. There are no omniscient standards but various and perpetual consolidations of processes that shape and prioritise technological futures, power, and trust.

Second, in Chapter 4 I study the National Warning System for Digital Infrastructure in Norway – a sensor-based system that monitors networks by automatically notifying anomalous behaviour – through the lens of 'green boxing'. Green boxing is conceptualised to explore how imaginaries of omniscience (the militarised ideal to achieve 'situational awareness') permeate the production of threat. Thus, I ask: *How do automated machine learning systems aimed at enhancing 'situational awareness' reconfigure the production of security and threat knowledge?* I show how the sociotechnical configuration of these systems appropriate military imaginaries (a '*situated* awareness') aiming to achieve 'total security from within', only perpetuating a universalised gaze on what can be achieved with cybersecurity.

Third, in Chapter 5 I offer a comparative analysis of specific risk assessments in counterterrorism and cybersecurity to explore how these assessments are situated and therefore produce distinct conceptions of what 'counts' as dangerous. I ask: *How do the different sociotechnical configurations of risk assessments produce categories of 'risk' and 'threat'?* I show how risk assessments as they have evolved with automation and machine learning operationalise widely different ideas of harm and practices of pre-emption. With no presupposition of threat, detecting 'anomalous' behaviour is a practice of continuous sense-making, on a contrary to the more traditional and linear process of meaning-making for assessing risk.

Finally, while primarily concerned with discourse, in Chapter 6 I focus on the 'production' of cybersecurity as a strategic weapon, which, if seen as historically and politically situated, is contingent on the means available to imagine and act upon scenarios of cyber war. I ask: *How has discourses of 'cyber doom' been shaped by academic engagement, policy outcomes and military expenditures in the aftermath of the infamous Stuxnet malware?* I highlight the realities of reinforcing dominant political imaginaries of what security *is* and how conceptions of systemic 'vulnerability' was and is produced in this context.

Each of these questions speaks to the main research question but offer independent studies of configurations of cybersecurity knowledge production. However, they all focus on the categorical production of 'danger' that continuously emerges through situated contexts and with different political effects – a closing of the world (Edwards, 1996). While cybersecurity features as an empirical protagonist in this thesis, cybersecurity is *a case of* processes that isolate and stabilise particular ontologies – ways of experiencing the world. As a whole, the thesis raises questions that aim to offer a pathway for scholars of security across disciplines to do empirical research on the human experience with emerging and seemingly transformative technologies. This is particularly relevant for how knowledge produces, and is produced with, technologies. For example, artificial intelligence (AI) and different techniques for machine learning, presently subject to considerable excitement and anxiety, offer tools that ultimately transform the way information becomes organised, standardised, and consumed. Nevertheless, this only stresses the importance of critically engaging with the schema upon which knowledge is created. The overarching contribution, detailed the next Section 1.3, is to provide a theoretically rigorous, politically engaged, thematically focused, and empirically expansive account of the interplay of knowledges and materialities to foster empirical engagement for intervening on increasingly invasive technopolitics of security governance.

1.3 Aim and contribution of the thesis

At this stage, it is important to note that I do not propose a new way of studying knowledge production. Nor do I intervene on established methods and methodologies for STS, nor for critical theory. My contribution is rather to empirically study knowledge production and thereby enactments of cybersecurity with the wider aim of better grappling with the political stakes involved. I draw on well-established literatures – found primarily in STS, IPS, and CSS over the past three to four decades – on knowledge production and materiality that takes as its starting point the idea that knowledge production is sociotechnical and brings the world into being. I build on this important methodological and theoretical lens for a conceptual vocabulary to do empirical studies on *cybersecurity* specifically, which has largely gone below the radar (despite being a top priority for national security strategies today), and show how this can be done through the four independent studies in Chapters 3, 4, 5, and 6.

The political significance of security governance and the securitisation of certain phenomena is a question that has puzzled critical scholars of IR for a long time (Buzan, Wæver and de Wilde, 1998; Huysmans, 2006). There is, however (as I have alluded to earlier), analytical potential to expand on technopolitics and security, especially considering the lack of attention paid to the analytical richness offered by Lucy Suchman and others on the human-machine interplay thus far. Empirical research on cybersecurity knowledge production is, however, not a task at hand merely to 'fill the gap' of academic scholarship at the intersection of interdisciplinary studies on security. What is at stake here is inquiring about the social and political implications of disregarding the role of human-machine relationality for (cyber)security. These implications are multifaceted: Inquiry into the sociotechnical can reclaim the imaginary that we are entering a time in which knowledge production no longer relies on humans, hence a world that appears to run the risk of eliminating human agency and, consequently, space for critique (Bousquet, 2018).

Options for change and intervention cannot be considered something out of our hands. However, I do not aspire to suggest normative solutions to challenges and inequalities prompted and enforced by digitalisation. Rather, the point made through my analytical studies is precisely to encourage affirmative action through intervening in the normative assumptions that underly both research and the universalised gaze on security and technology. To do so, I take seriously the importance of empirical enquiry which has been made possible by the work done on theorising and understanding sociotechnical configurations and by taking to heart the methodological foundations for asking such questions of intervention. Unless scholars grapple with how meaning is produced in relation to matter, or technology, in these contexts, we cannot recognise how these taken-for-granted phenomena are co-productive in organising social and political life. Put simply: Understanding how knowledge is produced about phenomena (such as cybersecurity) is critical for uncovering assumptions about what constitutes a risk and/or threat to society and how to handle or avoid them. In my view, these assumptions have little to do with whether cyber threats are real or imagined. What matters is instead that knowledge about cybersecurity gives way to understanding an arrangement of social and political relations beyond existing efforts on the political significance of security.

Why cybersecurity?

I have stated that my contribution is to show the political stakes involved in enactments of cybersecurity by studying knowledge production through different sociotechnical configurations. Hence, it becomes my duty to situate the significance of this in the context of how digital realities are experienced and continue to grant cybersecurity its high-ranking position in international policy, strategic, and academic environments. While cybersecurity has been embraced across a variety of scholarly fields over the past fifteen years, as discussed in Section 1.4, there are important aspects from the plethora of literature that takes on questions of knowledge production to better understand the interplay between the political, social and technical in matters of security. While cybersecurity is indeed the *empirical* focus, my main argument speaks to critical perspectives on knowledge and how it is produced, offering tools to better grapple with security writ large. That is, this approach shows how the long history of problems (the vulnerabilities, risks, and threats) for national security and insecurity continue to emerge, and how they rest on the enduring reconfiguring of technologies. Irrespective of empirical case or field of security, technology continues to transform the interactions upon which the world is enacted as a dangerous and political place.

While cybersecurity serves as suitable illustration to highlight how technology transforms practices of security, digital technologies continue to impact how humans understand and exist in relation to one another in other environments too. While, as mentioned, the most rudimentary inventions like roads or water filtering have always transformed social well-being and social life, they become relegated to mere background conditions. Even recent inventions have become self-evident in the way we organise ourselves. Only since the mid 2000s have we been wholly absorbed into the experience of social media services that make it possible to communicate constantly in real time (Downing, 2023). Basic Internet applications have transformed our ways of working, moving around, and simply connecting. The diffusion of consumer software and technological advancements continuously introduce new devices and services that transform the opportunities and spaces for everyday operations, where more recent examples still considered ‘modern’ include smart phones (Markussen, 2022), cloud computing (Adler-Nissen and Eggeling, 2024; Amoore, 2020), and generative AI (Amoore et al., 2024). Digital technologies implicate the (inter)national security apparatus, too: The electronic governance of borders and modes of identification (Bourne, Johnson and Lisle, 2015; Dijstelbloem, 2021), the computational mapping and monitoring of financial flows (de Goede and Wesseling, 2016; de Goede and Westermeier, 2022), and conducting warfare (Bousquet, 2018; Reichborn-Kjennerud, 2025; Suchman, 2020, 2023). The normalisation and institutionalisation of digital screening, profiling, and surveillance (Amicelle, 2022; Hintz and Milan, 2018) illustrate ways in which a distinctive algorithmic reasoning governs the individual and populations (Aradau and Blanke, 2018, 2022), Even diplomacy has ‘gone digital’ as shown by Adler-Nissen and Drieschova (2019). These are not ‘new’ transformative modernisms, however. Seen through the lens of Foucauldian governmentality, these are supplementary ways of inscribing, or ordering, social and political life through a sociotechnical security apparatus (Foucault, 1991; see also 1977).

In the realm of national and international politics and security, the now-familiar notion of cybersecurity has evolved into a massive industry for technological innovation and defence politics. It has become a critical policy area with wide-ranging implications across most sectors of society. But cybersecurity, like all technological tools intended to solve problems in society, is never apolitical, neutral, or objective. Nor is it mere structuring or ordering objects. As seen with the example of lived experiences of war in Ukraine, technologies are political and transform not only *what* humans and technologies are capable of doing, but *how* they do things, contingent on how social beings imagine, debate, design, and use the available means. By that I refer to an understanding of the reciprocal and mutual production of our existence – not (pre-)determined by technological innovations and the future of advanced computation – but rather an understanding of social life as it is made and experienced in unanimity with the objects (such as digital technologies) we surround ourselves with.

Thus, there is a space and need for critical inquiry into how knowledge is produced, and in turn how knowledge plays into the enactment of cybersecurity. The aim is to better equip interdisciplinary research on politics, security, and technology to approach emerging technologies not as transformative in and of themselves but examine how they reproduce hierarchy and show where critical intervention is possible. Taken together, the thesis offers a critical lens for studying the enactment of cybersecurity and the political implications of specifically situated knowledge-producing activities. I encourage the need for reflexivity in engaging with cybersecurity epistemologies through sensitivity towards the human-technology relationality for better understanding how 'we' inhabit a sociotechnical environment. Most importantly, this draws attention to possibilities for intervention on social life and how to operationalise a desired future by extension of technological means.

1.4 Situating the study in existing literature

Studies on cybersecurity

The notion of cybersecurity is now incorporated into the lexicon of security politics, international relations, law, computer science, and social and political science (Whiting, 2020). Its conceptual genealogy reveals a rather recent but rich history, now treated as one of the 21st century's key national security concerns across the globe (Dunn Cavelty and Wenger, 2022) While cybersecurity has been rapidly incorporated into national security agendas, it has simultaneously been embraced by IR, and especially studies on war and conflict, as an object of study. When considered only as a national security concern, it lives on as a matter of technological efficiency and specialist expert area, focused on the ability to thwart issues that arise from the capacity of state and non-state actors to disrupt critical infrastructure, political stability, or economic continuity. There are, however, several problems that arise from these framings.

First, particularly in classical and neorealist forms, they privilege the state as the primary unit of analysis, overlooking non-state actors and subsequently taking for granted the international system as a given and level of analysis. Consequently, cybersecurity is framed in terms of 'cyberwar' and 'conflict', privileging militarised and adversarial interpretations. It obscures the broader spectrum of issues, such as crime, privacy, digital rights, and the sociotechnical production of insecurity. Second, they often attempt to fit cybersecurity into pre-existing models of conflict, such as deterrence theory. In the subfield of Strategic Studies, focused on the 'laws' of economic and political rivalry as constitutive of a global balance of power, cybersecurity becomes dealt with as an 'add-on' – a risk and a resource in the service of power politics – moulded into prevailing analytical frameworks in the discipline (e.g., Kello 2017; Nye, 2011; Rid, 2013; Valeriano and Maness, 2018). As discussed in Chapter 6, the academic debate in orthodox IR and Strategic Studies has gradually asserted the characterisation of cyber operations as strategically important. This powered the development of subsequent policy, the strategic and military fixation on the grandeur of 'potentials' and 'vulnerabilities' of digital infrastructures, and the development of notions including 'weaponised malware' and 'weaponised interdependence' (Farrell and Newman, 2019). Since then, studies have predominantly framed cybersecurity as a matter of pre-emption, deterrence, and resilience – a stratagem for state actors. These models were developed in the context of nuclear and conventional military capabilities. They struggle to capture the fluid, ambiguous, and continuously open-ended development of digital technologies that produced perceived ontologies about the 'nature' of global order. Third, these perspectives essentialise danger as pre-given or objective threats, rather than sociotechnically produced. Social actors are disregarded as passive, subsequently naturalising the existence of cyber weapons, attacks, and capabilities without considering how design, engineering, institutions, and epistemologies shape contingencies and values. The implications of classical or neorealist perspectives are therefore that they obscure how cyber phenomena such as threats are rendered legible and actionable, foreclosing alternative framings and responses.

In critical approaches to security, the framework of securitisation critiques narratives on national defence as the construction of dangers necessitating extraordinary measures (Buzan, Wæver and de Wilde, 1998), such as surveillance, legislative interventions, or cross-national political negotiations to develop ‘norms’ in cyberspace (Dunn Cavelty and Egloff, 2021, Hansen and Nissenbaum, 2009; Nissenbaum, 2005). These perspectives show how the process of securitisation is not merely descriptive but performative, in that it actively constitutes what is considered a security issue and who is authorised to address it. These studies draw attention to how authority and legitimacy are distributed among various actors, including states, private firms, and technical experts. The dominance of technical experts in cybersecurity governance often marginalises alternative voices and obscures the ethical, social, and political stakes involved in decision-making processes (Leese, 2014). In this context, cybersecurity functions as a form of technopolitics – an arena in which political struggles are played out through ostensibly neutral technical infrastructures and vocabularies. Legal discourses and computational sciences narrow the focus on cybersecurity as technical specificities and highlight definitional (and legal) ambiguity surrounding notions such as cyber threat, terrorism, and crime. Unstable definitions are not only tricky for legal frameworks but influence, and are influenced by, broader political discourses and academic incongruities that tend to stretch interpretations of ‘cyber’ to fit both emerging technologies and theory of international relations (Whiting, 2020; McCarthy, 2017). While securitisation approaches challenge technological determinism and technical rationality that frames it as a neutral and apolitical solution to technical problems (Hansen and Nissenbaum, 2009), there remains a tendency to treat technologies only as discursive objects rather than as active participants in shaping security knowledges.

Others, however, have claimed that ‘cyberspace’ has not necessarily been securitised, but rather subject to riskification (Backman and Stevens, 2024; Friis and Reichborn-Kjennerud, 2016; Stevens, 2022). As further explored in Chapter 5, riskification refers to the production of speculative security regimes based on the anticipation of future harm (Amoore, 2013; Corry, 2012). Although not explicitly concerned with cybersecurity, speculative risk governance drawing on practices of preparedness and anticipatory intervention has been studied with a focus on other security domains, such as counterterrorism and global health (Adey and Anderson, 2012; Eriksson and Rhinard, 2009; Lakoff, 2010). Foucauldian concepts such as governmentality and biopolitics have been especially influential, framing security not merely as protection from external threats but as the governance of populations and the management of risk (Aradau and van Munster, 2007; Foucault, 1977; Leese, 2014). For example, these frameworks support an understanding of how security policy comes to regulate not only threats or malicious actors but also ordinary users (Amicelle, 2011; Deibert and Rohozinski, 2010). Biopolitical approaches explore how cybersecurity discourses frame digital spheres as both opportunity and vulnerability, legitimising expansive surveillance and anticipatory governance aimed at pre-empting threats (Amoore, 2013; Collier and Lakoff, 2008; DeNardis, 2014; Krasmann and Hentschel, 2019). In this view, computational security infrastructures are thus not just reactive mechanisms but also anticipatory systems that work to project and pre-empt possible futures, and by implication risk. These systems embed uncertainty into governance, making ambiguity and indeterminacy central features of contemporary security practice. Those concerned with the riskification of cybersecurity argue that risk has become a key organising logic in the governance of digital systems, shifting attention from known threats to the management of unknown and emerging vulnerabilities (Aradau and Blanke, 2018, 2022; Backman and Stevens, 2024; Stevens, 2022).

Over the past decade or so, a growing body of critical scholarship has begun pointing towards how cybersecurity *knowledge* is embedded within structures of power and commercial interest, particularly though the centralisation of power through the epistemic authority of state and corporate actors (Cristiano et al., 2024; Dunn Cavelty and Wenger, 2022; Dwyer, et al., 2023; Monsees and Liebetrau, 2025; Stevens, 2020a). Specific knowledges inform not only governmental responses to danger, such as modes of anticipatory governance (Adey and Anderson, 2012; Amoore, 2013; Anderson, 2010) but also shape the conditions upon which danger can be imagined through categories of 'vulnerability', 'threat', and 'risk' that emerge though various expertise and technical capabilities that render information intelligible in different ways.

The specific attention to the social and political implications of how knowledge about technology and security is produced has prompted a scholarly turn towards reframing cybersecurity through its inextricable entanglement of technical systems, practices, and institutional and cultural imaginaries (Coles-Kemp and Hansen, 2017; Monsees and Liebetrau, 2024; Stevens, 2020a). Embraced by social and political science, Critical Cybersecurity Studies has become its own subfield in IR (Dunn Cavelty, Pulver and Smeets, 2024; Dwyer, et al., 2023 Liebetrau and Christensen, 2021). These works have, importantly, rejected the binary distinctions of cybersecurity as either as purely an anthropocentric matter or a static technological capability. Rather, cybersecurity is an 'emergent security', meaning that cybersecurity is produced from non-linear logics (Fouad, 2021), constituted by an interplay of social actors and technical capabilities and systems. In other words, these perspectives purport that cybersecurity is, inevitably, a technological, social, and political concern. These studies have focused explicitly on reconceptualising cybersecurity rather in terms of its ontology (Liebetrau and Christensen, 2021) and its embeddedness into complex sociopolitical, economic, and cultural contexts (Downing, 2023). By critiquing normative assumptions and power relations that shape cybersecurity practices and discourses, these works have importantly challenged ideas of cybersecurity functioning as objective and apolitical solutions (see also Deibert and Rohozinski, 2010; Monsees and Liebetrau, 2024). Thus, definitions of 'vulnerability', 'threat', and 'risk' are constructed through historically contingent and ideologically laden processes (Eriksson and Giacomello, 2006; Slayton and Muller, 2025).

The critical turn in studies on cybersecurity advances a more reflexive and politically attuned understanding (Cristiano, et al., 2023). It has reconceptualised the questions posed by critical theorists for decades (Guillaume and Grayson, 2023; Huysmans, 2006) on security *for whom*, *by whom*, and for *what purpose*, applying them to the context of cybersecurity. Thus, importantly, cybersecurity is increasingly problematised in terms of whose interests are served by dominant cybersecurity practices, and which alternative frameworks might better address the complexities of digital life. However, while critique of technopolitics and power asymmetries is vital for critically engaging with cybersecurity knowledge production, the methodological orientation has largely achieved this by focusing on the macropolitical and discursive, often neglecting the empirical and sociotechnical dynamics activated within various contexts and technologies. Despite reframing cybersecurity as a domain shaped by power and inequality, these perspective also remain committed to treating technologies as discursive objects rather than as active participants in shaping security knowledges.

Empirical studies on cybersecurity would benefit further from integrating methodological sensitivities that allow for treating cybersecurity technologies – such as cyber threat intelligence mapping, intrusion detection systems, or other types of sensor-based surveillance – as active phenomena that play into the inextricable entanglement of technical systems, practices, and institutional and cultural imaginaries. Sometimes drawing on Bordieuan and Latourian approaches, the 'material turn' (Aradau, 2010) and the 'practice turn' (Bueger and Gadinger, 2014) in CSS have rethought the effects of material-discursive practices for stabilising intersubjective understandings (Loughlan, Olsson and

Schouten, 2015). In this vein, I build on these literatures that pay attention also to “the entanglements of discourse, practice and materialities in specific security assemblages” (Loughlan, Olsson and Schouten, 2015, p. 46; see also Hoijtink and Leese, 2019). Especially, this concerns CSS and studies of technopolitics that have adopted a position at the intersection of STS and IR to appreciate how security and technology is ascribed meaning, which in turn conditions how they are designed and deployed within human-machine configurations (Stevens, 2020a; Hoijtink and Leese, 2019).

Studying human-machine relationality

STS offers key frameworks and concepts grounded in a methodological sensitivity to abstraction, enabling reflexivity for exploring human-machine relationality (Aradau et al., 2014). CSS has, as mentioned, been inspired by STS concepts, such as ‘inscription devices’ (Latour and Woolgar, 1979) and ‘boundary objects’ (Star and Griesemer, 1989) but most importantly, for thinking about how materiality *matters* and how ‘things’, such as maps, enable and constrain discourses and practices (Adler-Nissen and Drieschova, 2019; Aradau, 2010; Kaufmann, 2024). This has enabled studies of how objects render certain things (un)knowable, showing how technological ‘objects’ premise knowledge production in specific assemblages for security (Amicelle, Aradau and Jeandesboz, 2015). Such approaches have shown how materiality matters for making threats and (in)security visible and invisible, thus shaping knowledge and how that knowledge is enacted. Avoiding assumptions of the validity of science (such as facts), and turning towards *how* social beings understand and treat different meanings and the instruments used to interpret those meanings, offers a pathway towards exploring knowledge production as practice (Knorr Cetina, 2007, see pp. 363–364). For cybersecurity, STS frameworks can support an understanding of how technologies shape, and are shaped knowledge (Dunn Cavelty, 2018). This includes how technologies render some things known, and others not (‘non-knowledge’) (Aradau, 2017; Aradau and Perret, 2022). The point is not that there is one omniscient view of the world that asserts explanations to what phenomena such as (cyber)security mean and do. Rather, the plurality in methods, such as mapping, and ways of producing and interpreting information emphasise that different knowledge underpinnings lead to different ways of knowing an ‘object’ (Aradau, 2017; Aradau and Perret, 2022). In this vein, STS has a longstanding tradition of exploring human-machine relations, and how knowledge is produced and can be studied as open-ended in a given context and interaction.

Techno-feminist perspectives have especially provided key resources for rethinking the relationship between humans and machines (e.g., Barad, 2007; Haraway, 1988, 1991; Suchman, 2006, 2012). A central concern has been how knowledge is produced, stabilised, and made authoritative within sociotechnical systems. Donna Haraway's *Cyborg Manifesto* (1991) reconceptualises boundaries between human and machine, proposing the cyborg as a figure that blurs binaries such as nature/culture and male/female. Lucy Suchman (2006) critiques instrumentalist models of human-computer interaction, emphasising 'situated action' and the co-constitution of human and machine agency. Karen Barad (2007), through her theory of agential realism, further dismantles subject/object dualisms by arguing that humans and technologies 'intra-act', that is, emerge through mutual entanglement rather than pre-existing categories. Together, these perspectives foreground the relational, embodied, and political dimensions of human-machine entanglements, remain highly influential to date, and provide a methodological backdrop for this thesis.

Furthermore, Actor Network Theory (ANT), developed by Bruno Latour, John Law, and Michal Callon, emphasises how knowledge practices and scientific facts are stabilised through networks of human and non-human actors. Through this lens, texts, institutions, devices (such as algorithms, sensors, software), and infrastructures are not passive intermediaries but actors (or 'actants') that are active in shaping knowledge (Callon, 1986; Latour, 1987; Law, 1992). Further, ANT commits to the social world being organised through ontological symmetry, where humans are equal to non-humans as active participants, or actants, in constructing social life (Latour, 2005; Law, 1992). Ontological symmetry accepts the sociotechnical interplay between humans and non-humans, such as different technologies, by not giving precedence to one over the other as drivers of social change. Scholars of ANT explore 'sites' or 'objects' in the 'laboratory' (Latour and Woolgar, 1979) through ethnography, observing participants and discourse, the relational structure, or 'network', of actors as sites that produce the social world as it is sensed and experienced.

While classical STS is rarely focused on security, major strands trace back to Bruno Latour's work on the production of scientific and technical facts through the lens of ‘inscription’ (Latour and Woolgar, 1979) and ‘black boxing’ (Latour, 1987, 1999). The renowned black box has been widely used in STS to describe how scientific and technological systems become opaque as they stabilise. Once a device or system works reliably, its internal complexity disappears and it becomes taken for granted as a seamless, functional unit:

> scientific and technical work is made invisible by its own success…[w]hen a machine runs efficiently…one need focus only on its inputs and outputs and not on its internal complexity. (Latour, 1999, p. 304).

‘Inscription’ or ‘inscription devices’ are material and social tools that transform physical phenomena into stable, transportable representations like graphs, texts, or numbers. These devices allow scientific observations to be recorded, compared, and circulated within scientific networks. Crucially, they are not neutral instruments but active mediators in the construction of scientific knowledge. Inscription offers an analytical tool for understanding how complex or abstracted phenomena are rendered visible and/or knowable through *representations* (Walters, 2002). Focusing on how scientific knowledge is produced, epistemological studies of technology and social life explore humans and non-humans (e.g., computers) not as separate entities but co-produced (Jasanoff, 2004; McCarthy, 2017). Latour (1999) further emphasised that scientific facts are materially grounded and socially constructed. Knowledge, he argued, is produced through intricate processes through networks of people, instruments, inscriptions, and practices. The stabilisation of ‘facts’ is, in other words, co-produced through scientific activity. In this vein, Sheila Jasanoff and Sang-Hyun Kim (2015) argue that scientific knowledge and political institutions are always intertwined and enacted through sociotechnical imaginaries, defined as

> collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology. (Jasanoff and Kim, 2015, p. 4).

Sociotechnical imaginaries are advantageous for uncovering how normative political projects such as security governance inhabit an envisioned future by extension of technological means. A problem, however, for the idea that ‘collectively held’ visions of the future can be studied in their performativity is that it overemphasises coherence, intentionality, and stability in the relationship between technological visions and social order. By focusing on the ‘collective’ visions, it risks reductionism by portraying imaginaries as unified or monolithic, downplaying internal contestations, exclusions, and the fragmented, conflictual processes through which futures are imagined and enacted. In other words, there is a danger in overlooking whose visions are represented, marginalised or silenced, how, and for what purpose. This is particularly relevant in global contexts, where imaginaries often reflect dominant political priorities (i.e., Western) as universal truths, while obscuring uneven power relations, resistance, or alternative futures (Dwyer, et al., 2022).

A similar reductionism characterises 'inscription' and 'boundary objects', as well as ANT's 'actants'. These analytical concepts tend to oversimplify and translate complex phenomena into something that can be 'captured' or observed in the laboratory. Interpreting complex phenomena as simplified categories only confirms the knowledge basis through our (the 'scientists'') vocabulary and experience of the world. The concept of 'technological affordances', too – although an attempt to remedy actants and inscription as mere "representations of reality" (Adler-Nissen and Drieschova, 2019, p. 534) – bears the same shortcoming. Though these concepts highlight how technologies mediate action, they often reduce this mediation to either representational or enabling functions, neglecting the broader political and ontological implications of materiality. Technological affordances – defined as the possibilities for action that technologies offer to users – have been used to analyse how actors engage with digital tools in global politics (Adler-Nissen and Drieschova, 2019). Yet, they do not say anything about how digital tools are *made*. Like inscriptions, this concept isolates discrete interactions between humans and technologies, falling short of exploring how such interactions are embedded in, and productive of, infrastructures of power and meaning. Moreover, these concepts struggle with scale: While they work as tools for analysing localised microprocesses and representation, neither support an analysis that traverses scale beyond the contexts in which they occur as structuring effects of materiality that enable or constrain behaviour in a particular context.

How, then, might one study knowledge production through human-machine relationality, without yielding to oversimplifications and resist binary distinctions between the social and the technical? One way of doing so is turning towards studies on infrastructure and infrastructur*ing*. Infrastructures have long occupied a foundational role in STS, understood not as neutral backdrops but as active, sociotechnical arrangements that condition the production of knowledge and, by extension, modes of governance. Geoffrey C. Bowker and Susan Leigh Star (1999) emphasise the embeddedness of infrastructures in everyday practices and their capacity to shape what counts as legitimate knowledge. Rather than inert systems, infrastructures are deeply relational and social, often rendered invisible through their very success and ubiquity. Infrastructures are not generated by epistemic communities or institutions in isolation but are, rather, deeply embedded in, and co-produced by *sociotechnical configurations*: Arrangements of material infrastructures, digital systems, labour, interpretations, and normative/cultural epistemologies.

Sociotechnical configurations

By shifting the analytical focus away from situations or structures where technologies condition human behaviour through representation, studies on infrastructures and the framework of infrastructur*ing* highlight how discourses, practices, and technical systems 'come into being' (Bueger, Liebetrau, and Stockbruegger, 2023; Edwards, et al., 2009). As frameworks that shape, and are shaped by, social interactions and technologies, hierarchy and power (a)symmetries can be explored: Indeed, the lens I employ in this study considers infrastructures as sociotechnical configurations, highlighting how they enable and constrain behaviour, but more importantly *how they co-produce expansive social, political, and epistemic orders over time.* They draw attention to the mundane but essential systems (Edwards, 2002; Suchman 2000), such as communication networks, logistical chains, or protocols, that underpin discourses and practices of knowledge production, even as they most often exist below the threshold of visibility (Bowker and Star, 1999).

Perspectives that approach infrastructures as frameworks to analyse knowledge production as relational and situated processes present a suitable option to studying them as static or cognitive/ideational structuring objects. From this point of view, these arrangements are not produced as isolated representations of knowledge but are embedded within infrastructures, systems and practices (routines/protocols), and epistemologies ('ways of knowing') (Edwards, 2002). Network surveillance sensors – such as intrusion detection systems (IDS), examined in Chapter 4 and 5 – do not simply collect, analyse, and distribute data as information. They actively co-produce taxonomical structures that define what can be known, by whom, and under what conditions. Whether open-ended or rules-based, thresholds are set to distinguish between what is treated as anomalous or safe/unsafe, secure/insecure, and normal/abnormal computational patterns of behaviour. Exploring infrastructure as an analytical concept foregrounds the politics of relationality, as well access and power, highlighting how knowledge production is tied up to global asymmetries through infrastructural control, governance, and standards. This is shown in Chapter 3 which offers a study of standardisation: Conformity assessments – highly complex quantified scoring systems – for digital products and services in European Union (EU) exercise power through global influence by constructing ideals (standards) for the production and distribution of distinct products and services offered in consumer markets.

As infrastructures are increasingly conceptualised by authorities as critical for survival (Collier and Lakoff, 2008; Dunn Cavelty and Kristensen, 2008; Hansen and Nissenbaum, 2009) and sites of geopolitical contestation (de Goede and Westermeier, 2022), they can be studied not as facilitating or structuring tools but as ongoing sociotechnical contingencies that (re)configure relations between technologies, systems, spaces, and temporalities. For example, financial banking infrastructures such as SWIFT banking system has been studied as a way of organising international political dispositions: As an infrastructure, financial flows can be governed (politicised, depoliticised), (re)structure political practices and, upon its discernibility, highlight new or different avenues for organising social and political spaces (de Goede and Westermeier, 2022). Starlink's satellite network, as mentioned earlier, is another example that shows how satellites as infrastructures organise not only access or visibility, but who gets to own, see and interpret information, and to act upon it. This way, the analytical lens of infrastructures as sociotechnical configurations allows scholars to uncover the logics that underpin how authority and power is mobilised, how it materialised, and how their configuration co-produce spatial and temporal conditions under which knowledge becomes intelligible and actionable.

Infrastructures theoretically occupy a variety of meanings. Christian Bueger, Tobias Liebetrau, and Jan Stockbruegger (2023) outline distinct styles of theorising infrastructure in global politics, each offering a different lens for understanding the political significance of infrastructures. *Infrastructuring*, and, similarly, *epistemic infrastructures* (Bueger, 2015), allows for focusing on processes, drawing on practice theory, New Materialism, and STS (to some extent ANT). Here, infrastructures are relational and dynamic, embedded in power relations and shape behaviour, norms, and agency through everyday practices as political forces with their own agential capacities, foregrounding the ongoing, situated work of building, maintaining, and modifying infrastructural arrangements (e.g., Blok, Nakazora and Winthereik, 2016; Bueger, 2015; Musiani, 2022). Like ANT (where infrastructures are treated as networks of heterogenous human and non-human actors), New Materialism offers a reorientation by attributing agency to non-human *matter* itself (Aradau, 2010; Barad, 2007; Bennett, 2010). Infrastructures are lively material assemblages, where matter exerts its own force and participates in political life. From this perspective, infrastructures are not simply the settings within which action occurs, but actors that influence outcomes, shape intentions, and enact power (Kaufmann, 2024). For example, in the context of cybersecurity, emphasis on material agency comes to the fore when considering the performativity of code, sensors, and algorithms in influencing how, for instance, risk is conceptualised and responded to. Another example is how machine learning systems and real-time monitoring sensors do not merely register and alert threats but actively generate them through probabilistic classification and behavioural modelling (Amoore, 2020; Edwards, 2010).

These processual perspectives capture how infrastructures are dynamically shaped, and how they interplay with institutional norms, power relations, and sociotechnical imaginaries. Fransesca Musiani (2022), for instance, highlights how such practices are deeply political, such as in contexts where states seek to assert digital sovereignty. This example is useful also for studies of international relations and politics, where infrastructures mediate transnational flows of information, authority, and resources. It closely aligns with thinking about infrastructures as sociotechnical configurations and how *epistemic devices,* as I further conceptualise in Section 1.5, can support an empirical study thereof. By attending to how infrastructures are open-ended, always 'in the making', differentially accessible, unevenly distributed, and politically contested, scholars can more effectively 'map' the structural *and* relational logics of agency – dimensions that 'inscription devices' and affordance theories often overlook or treat as secondary.

Similarly, while not entirely different, another style of theorising infrastructures is identified as *infrastructuralism*, whereby infrastructures are seen as a foundational concept for understanding global order. It proposes a new ontology where infrastructures are not simply empirical objects or relational phenomena, but the very conditions that organise and stabilise social and political systems. This style seeks to develop infrastructure as a core analytical category, capable of rethinking key IR concepts such as structure, agency, and order (Bueger, Liebetrau and Stockbruegger, 2023, esp. pp. 5–7). This invites critical investigation of cybersecurity infrastructures not as reactive but as *world-making*. Infrastructuring and infrastructuralism as analytical frameworks partially remedy the mainstream IR critique of Latourian perspectives' excessive focus on microprocesses and difficulty in abstracting to macrostructural dynamics of international relations (Nexon and Pouliot, 2013). Infrastructure frameworks grounded in STS afford the possibility to traverse scale (Basaran, et al., 2016; Edwards, 2002; 2010) by situating material infrastructures not solely as tools or representations but as co-productive foundations of social and political worlds (Bueger, 2015).

By treating infrastructures as sociotechnical configurations (as conferred in the styles of infrastructuring/infrastructuralism), it becomes possible to study open-ended arrangements of material infrastructures, digital systems, human labour and interpretations, and normative/cultural epistemologies. While these literatures provide a useful lens to examine how social, technical, and institutional arrangements stabilise and legitimise forms of knowledge, there remains a potential to use this abstraction to study the localised enactments through which knowledge is produced and rendered actionable. Thus, if sociotechnical configurations are the loci of study (the configured conditions upon which knowledge is produced), the concept of *epistemic devices* offers a tool for traversing scale by studying the situated vectors of knowledge production. In other words, it allows for 'mapping' the functions of dense ecosystems of knowledge producing tools (conceptual, methodological, and material) that enable the production, stabilisation, and circulation of knowledge on and through infrastructures.

1.5 Conceptualising epistemic devices

The concept of epistemic devices foregrounds the contingent, tactical, and performative mechanisms – such as protocols, documents, forms, evaluation templates, taxonomies, and scoring systems – that constitute the microdynamics underpinning the authority and intelligibility of technopolitical regimes or infrastructures. Epistemic devices are defined as the *vectors for knowledge production* (i.e., conceptual, methodological, and material tools) *that enable the production, stabilisation, and circulation of knowledge through sociotechnical configurations.* In practical terms they can be studied within specific configurations by rendering certain interpretations of knowledge authoritative while potentially marginalising others. While inspired by Latour's (1987) 'inscription devices', epistemic devices are not reducible to a 'tracing' of how phenomena become visible, structuring inscriptions. Instead, the concept of epistemic devices problematises how specific configurations become infrastructurally significant in producing epistemic legitimacy, particularly in regulatory and technical environments such as cybersecurity standardisation (Chapter 3), through intrusion detection systems for identifying anomaly as ‘threat’ (Chapter 4), or risk assessments powered by machine learning algorithms that are built to thwart ‘risk’ without a categorical presupposition of ‘danger’ to begin with (Chapter 5).

Bruno Latour focuses on how facts travel and how phenomena become simplified and rearticulated as stable representations in scientific discourse. These transformations facilitate comparability, scale, and coherence, but they underplay the interpretive and normative politics embedded in classification systems and evaluation matrices. Such processes are not only about ordering phenomena but also about delimiting ontologies. Epistemic devices attend to these ontological effects, particularly in areas where calculability is wedded to political order, such as cybersecurity. Here, the certification schemes and conformity assessment examined in Chapter 3 operate not only as mechanisms of technical control but as devices that enact particular imaginaries of vulnerability, risk, threat, and resilience. They are deeply performative and closely aligned with how Amicelle, Aradau and Jeandesboz (2015) conceptualise ‘security devices’: They do not merely represent security but enact it through routines, forms, and scripts that organise expertise, define thresholds, and distribute institutional responsibilities. Yet, while security devices tend to foreground the affective and disciplinary dimensions of security enactment, epistemic devices prioritises the epistemic vectors that make such enactments legible in the first place.

Importantly, epistemic devices does not exclusively focus on microprocesses. The conceptual move is in their ability to traverse scale. By highlighting the dense ecosystem of ‘objects’ that constitute infrastructural arrangements (understood here as sociotechnical configurations), it challenges conventional analytical frameworks in IR and political sociology (Basaran, et al., 2016). As mentioned earlier, traditional scales (such as the local, national, and international) are not natural, fixed, or given, but rather socially and politically constructed. These scales are often reified in mainstream IR as ‘levels’, which tends to privilege the state as the dominant analytical unit and presumes a hierarchical spatial order. Traversing scale, in this context, involves breaking away from the assumption that politics unfold within clearly demarcated levels. Instead, it emphasises the fluidity, intersectionality, and multiplicity of situations and contexts where power, subjectivity, and security are enacted. The transversal move is meant to ‘cut across’ scales rather than merely move between them (Basaran, et al., 2016). Influenced by traditions in IPS, integrating poststructuralist, critical, and Foucauldian insights, traversing scale brings attention to issues such as migration, surveillance, borders, and identity that cannot be meaningfully understood within rigid 'territorial traps' (Agnew, 1994). In other words, epistemic devices allows for studying political practices, discourses, and technologies as they are co-produced through interactions that are not limited to a single level but operate across and through multiple spatial and temporal registers (Edwards, 2002). It also offers an alternative to frameworks of ANT and affordance literatures that oversimplify complex phenomena as observable within the laboratory.

The conceptualisation of epistemic devices also challenges the emphasis placed on infrastructural (in)stability (e.g., de Goede and Westermeier, 2022). Edwards (1996, 2002) illustrates how infrastructural systems such as military computing and environmental monitoring embed epistemic assumptions (decisions about scale, scope, temporality, and authority). Yet, in framing infrastructures as large-scale, durable, and often invisible support systems that enable knowledge-making, these accounts risk 'flattening' the microprocesses through which infrastructures are continuously reconfigured. Importantly, these configurations are sociotechnical and *situated*. As Lucy Suchman (2006) argues, human behaviour cannot be fully understood or 'predicted' through abstract plans, rules, or formal representations such as protocols for standardising behaviour or 'compliance' (Chapter 3). Instead, actions emerge dynamically from the interplay of individuals and the specific – *situated* – social, material, and temporal contexts in which they are embedded. Models (such as assessments, schemes, or maps discussed in Chapter 3, 4, and 5) are not strict determinants of action but flexible resources interpreted and adapted *in situ*. Real-time contingencies are improvisational – environmental and social cues guide activity more than rigid models. Devices, such as technical systems or tools for cybersecurity, are epistemic because they acknowledge contextual adaptability rather than the outcomes of fixed workflows. Knowledge, by extension, is also situated; it is partial, shaping, and shaped by, social contexts, technologies, economic means and political will (see also Haraway, 2016). Thus, the analytical scale of infrastructure risks overlooking operational density of devices such as the protocols, evaluation forms, certification schemes, and scoring systems examined in this thesis – which configure how security is interpreted, calculated, and legitimised. In this context, the concept of epistemic devices offers a tool to remain focused on the mundane 'little things' while acknowledging the political and social consequences of their existence and role within infrastructures and thus relations as they are configured.

Unlike the way in which inscription devices and related concepts are associated with the *circulation* of knowledge, epistemic devices is concerned with the situated *production* and *operationalisation* of knowledge. This marks a critical distinction with implications for regulatory politics. Standardisation processes for digital products and services in the EU (Chapter 3) underscore how epistemic devices is a lens to examine technologies of verification, legitimation, and control. Devices do not simply translate standards into assessments. They enact a regime of evaluative rationality that determines what ‘counts’ as (in)security, how it can be measured, and who is authorised to make those definitions. This is evident in the layered system of different assurance levels in standardisation protocols, such as Attack Potential (AP) score and routines for technical documentation, which transform abstract principles into actionable knowledge. The performativity of these devices thus lies not in their representational function but in their constitutive capacity. They create perceived realities, rather than merely inscribe them.

Furthermore, by focusing on devices within sociotechnical configurations, this concept invites critical reflection on the modalities of inclusion and exclusion that are embedded in regulatory rationalities. As Bowker and Star (1999) argue, classification systems and standards inevitably marginalise alternative epistemologies, prioritise certain forms of knowledge, and stabilise particular ontologies. Epistemic devices highlight these exclusions not only through what and how things made visible, or perceivable (Bousquet, 2018), but through what becomes actionable. They render some risks governable, while relegating others. In the context of cybersecurity – mechanisms to evaluate risk, detect threat, and pre-empt harm within networks and systems – this includes the privileging of technocratic expertise and standardised protocols, routines, or thresholds, over contextual, lived, or experiential knowledge.

In this respect, the concept of epistemic devices functions as a critical vector to explore regimes of knowledge. While infrastructures can (de)stabilise regimes of knowledge production, epistemic devices is analytically sensitive to contestation and performativity at the operational level. Edwards’ (2007, 2010) insight that infrastructures are not inherently legible or complete but require constant calibration and maintenance underscores this distinction. He shows, particularly in his analysis of Cold War computational systems and 'closed-world discourse' (Edwards, 1996), how infrastructures enact specific visions of control, rationality, and authority, but only by means of recursive inscription, classification, and verification activities. These same dynamics are visible in cybersecurity governance, where standardisation, for instance, is not merely an outcome of institutional coordination but demands active epistemic labour. Thus, epistemic devices traverses scale not as byproducts of institutional design but through production of legibility, actionability, and authority within configurations expertise, trust, routines, evaluations, digital technologies, and so on.

This conceptual framework is offered to better understand cybersecurity knowledge production. If understood as a sociotechnical configuration enacted through an ecosystem of epistemic devices, it can uncover how these discourses, practices, and technologies co-produce and privilege dominant perspectives on security *for whom*, *by whom*, and for *what purpose*. Rather than treating scale as fixed, the concept of epistemic devices reveals how it is produced through situated actions and how microprocesses – tools such as scoring schemes, classification protocols, and standards – materialise broader infrastructures of governance. As situated knowledges and practices, it highlights the recursive, often invisible work through which cybersecurity knowledge is produced. Epistemic devices makes visible the contingent, institutional, and political processes that define what counts as risk, threat, or vulnerability. In doing so, it shifts attention from abstract accounts of infrastructure to the everyday practices that enact it, showing how local actions are translated into systemic security imperatives through recursive feedback loops and computational logics. Thus, the concept offers a powerful analytic for showing how cybersecurity governance emerges from configured technical systems, institutional cultures, and political and social imaginaries.

1.6 Overview of thesis

So far, Chapter 1 has set out the thesis' aim and contribution by situating the study within critical debates on (cyber)security and STS-informed theory for studying knowledge production through humans and technologies as they are not binary but configured in infrastructural ecosystems. It has outlined how this thesis, particularly speaking to interdisciplinary research at the intersection of CSS and STS, contributes to debates on technopolitics, cybersecurity, and theoretical frameworks for studying the sociotechnical production of knowledge. What is particularly important for the sake of this thesis' argument is showing how there are limitations to nearly canonised STS concepts – especially 'inscription' and related concepts – for studies of politics and security. While I pay attention to the merits offered by analytical tools associated with ANT, as well as sociotechnical imaginaries, they risk reductionism in oversimplifying and translating complex phenomena into something that can be 'captured' in the laboratory as collective truths. Remedying this tendency for studies on politics, technology, and security, I then argued that infrastructure/infrastructuring perspectives highlight the ongoing, situated work of building, maintaining, and modifying knowledge regimes. Finally, the chapter presented the theoretical framework by conceptualising epistemic devices as an analytical tool for empirical studies showing how knowledge is produced in sociotechnical configurations and how epistemic devices traverse scale and play into infrastructural arrangements.

Chapter 2 draws out the thesis' research design, including a discussion of the methodological orientation in Section 2.2, grounded in interpretive and reflexive approaches. I highlight the bricoleur of the study and elucidate the case selection which I outline as distinct, contextual, and situated research sites and the merits of their homogeneity. In Section 2.3 I then provide details on my data collection and analysis, which combines textual analysis of various types of documents with informal interviews. The multilayered methods has allowed for an in-depth examination of how cybersecurity knowledge is produced, mobilised, and stabilised across discursive, institutional, and technical fields. Finally, Section 2.4 discusses ethical considerations. This includes how I have 'navigated secrecy' as a reflexive practise when studying a field oftentimes characterised or limited by scarcity in public information due to security concerns. Moreover, I draw out the thesis' ethical considerations for academic integrity, including how I have handled interviews and data storage management. Lastly, I reflect on the limitations of the research design, including the inherent confinements of reflexivity, the potentials of doing a more ethnographic oriented study of sociotechnical configurations, and the limits and possibilities of doing an article-based doctoral thesis.

Chapters 3-6 are the thesis' analytical chapters. First, in Chapter 3, I explore standards – specifically standardisation of cybersecurity products and services through conformity assessments and certification schemes in the EU. Standards are not arbitrary but emerge in sociotechnical configurations. To illustrate this, I present a theoretically informed analysis of the EU Cybersecurity Certification Scheme based on Common

Criteria (EUCC). Moving beyond normative or institutional accounts of standards, in Section 3.5 I examine how conformity assessments materialise political authority and render (in)security and risk calculable. By analysing how security becomes operationalised through these quantified evaluation schemes and standardised certification protocols, the chapter shows that these processes are not solely managerial, regulatory, or technical. Expanding on the thesis' theoretical conceptualisation of epistemic devices in Section 3.3, it uncovers how to study the dense ecosystem that constitutes infrastructures of digital governance. It shows that the emergence and maintenance of these infrastructures can be understood through how they operationalise the mundane yet powerful work of standard setting. Ultimately, the chapter contributes to the thesis' core argument – standardisation serves as an illustration of standards as they are sociotechnically configured, where knowledge, authority, and political order are co-produced on and through the technopolitics of (cyber)security governance.

Chapter 4 explores IDS, specifically Norway's National Warning System for Digital Infrastructure. It illustrates how anomaly detection (a method which incorporates automation and machine learning for detecting threats in systems and networks) reconfigures the production of knowledge about cyber threat and (in)security. The chapter draws on interviews with technical operators, engineers, and institutional actors involved in the warning system. It shows that anomaly detection does not deliver the seamless oversight or predictive control often promised in cybersecurity and military imaginaries of 'total security'. Instead, it produces more uncertainty, and thereby new forms of interpretive labour. By exploring the sociotechnical conditions under which threats become knowable and governable – a situated awareness – the chapter also conceptualises 'green boxing' as a tool to understand the sociotechnical production and stabilisation of knowledge about threats, turning cybersecurity into a performative space where uncertainty is not eradicated but operationalised. Green boxing contrasts the well-known STS concept of 'black boxing' by acknowledging that while technologies are deeply embedded in routine practices, they are not experienced as settled or self-evident by their users. By foregrounding the recursive, contingent, and negotiated character of cybersecurity practices, this chapter expands on challenging deterministic views of algorithmic security governance and further emphasises the political implications of automation, control, and the governance of uncertainty.

In Chapter 5, I foreground the 'riskification' of cybersecurity, comparatively analysed with counterterrorism. When analysing risk assessments across different systems

– exemplified here through the U.S. intrusion detection system EINSTEIN and parts of the UK counterterrorism programme Prevent – the chapter highlights important differences. Whereas Prevent more clearly presupposes normative subjects and standards of (in)security, EINSTEIN's anomaly detection engenders threat not as a binary or normative distinction but a separate category of risk. The chapter underscores what configurations *do* for the categorical production of 'vulnerability', 'risk', and 'threat'. It shows how the different logics of 'meaning-making' and 'sense-making' are processes that shape both security responses and timelines through which risk is conceptualised in different ways. Moreover, it reveals that rather than being fixed, risk and (in)security are perpetually co-produced with the tools used for assessment. This highlights that production of knowledge about (in)security has little to do with real or imagined risk but rather emerges from a particular configuration of social, political, and technological relations.

In Chapter 6, I return to the infamous malware introduced in Chapter 1. While the chapter diverges from the rest (focusing on discourse explicitly rather than a sociotechnical configuration), it provides a historical and discursive analysis of Stuxnet as a pivotal moment in which 'cyber' emerged as a key notion in the lexicon of orthodox IR, hereunder Strategic Studies. The chapter outlines academic, media, and political attention to cyber doom scenarios after the discovery of Stuxnet, and how this has shaped contemporary understandings of what cybersecurity is, and does, as a deterrent or strategic tool for states. The imaginaries that commenced in the wake of Stuxnet cannot be seen as isolated or collective ideas, but as historically and politically situated and produced. Hence, this chapter analyses the importance of discourse, and how dominant perspectives devised in academic circles continue to inform the commercial design, maintenance, and development of technical systems and capabilities to 'achieve' cybersecurity for and by states. As an independent analytical contribution, the chapter encourages scholars of security to critically challenge the promises of 'new' technologies (such as the thrills and terrors of AI) and how they emerge as potential threats and/or 'strategic' capabilities.

Finally, Chapter 7 presents the thesis' conclusions and reflects upon the potential for further research. First, I return to the main research question and the distinct empirical questions posed in each of the analytical chapters, offering a general conclusion based on the overall argument that studying situated and contextual knowledge is key to uncovering the production of ostensible insecurity and the ensuing technopolitics of security governance. I provide an outline of the thesis' conceptual, theoretical, and empirical contributions in Section 7.1, before stressing important political and societal implications of perpetual digitalisation and imaginaries of omniscience. I emphasise the importance of addressing these questions – in academia and the public, as well as for policy strategist and technical operators – and their implications to uncover the often-invisible yet deeply invasive technopolitics of (cyber)security governance. Finally, in Section 7.2 based on the conclusions, I distil areas this thesis has inspired for further research.