The technopolitics of cybersecurity

Sociotechnical configurations, epistemic devices, and the production of knowledge

Aanonsen, C.E.

Publication date
2025

7

Chapter seven: Conclusions, contributions, and further research

7.1 Conclusions

From Stuxnet and cyber doom, this thesis has reoriented the focus to the mundane, everyday practices of cybersecurity. While often relegated to the background as circumstantial to the 'high politics' of national and international security, I have examined cybersecurity *knowledges* and their constitutive role in shaping technopolitics of security governance. Through a series of empirically grounded analyses across four distinct but interrelated chapters, I have shown how cybersecurity cannot be reduced to solely regulatory and managerial processes, nor as mere technical tools or security domains. Rather, the making of cybersecurity is embedded in sociotechnical configurations that organise, disrupt, and remake knowledges, producing political rationalities that both reflect and reinforce existing power asymmetries. What is often framed as objective danger is, rather, contingent on situated practices, epistemic devices, and local/contextualised *ways of knowing*, sensing and producing to (in)security. Central to these ways of knowing is the imaginary of 'total security' – a vision of omniscience that underpins human-technology relations and operationalises the enactment of technopolitics. This dream largely derives from the assumption that the world is a rational, calculable, and homogenous space where threats can be anticipated, identified, pre-empted, and ultimately eliminated. The belief that 'more data equals better security' substantiates this technopolitical logic, striving through its many interpretations and enactments in contemporary security practices to render the world and its associated dangers discoverable and governable. Consequently, cybersecurity emerges not as a response to 'objective' dangers, but as a performative political and technical field through which insecurities are constituted and governed in ways that reinforce dominant epistemologies and structures of power.

How then, *does the production of cybersecurity knowledge shape the technopolitics of security governance, and what are the implications?* Empirically, I have shown how the mundane and situated practices of *standardisation* (Chapter 3) condense complex and contested issues for cybersecurity into calculable categories. Quantified scoring assessments of 'vulnerability' are not neutral variables but epistemic devices that actively produce and legitimise some visions of security over others through normative commitments. Furthermore, intrusion detection systems (Chapter 4) – powered by machine learning techniques – 'map' the world of danger into a legible and calculable place, subsequently co-producing a *situated* awareness where humans navigate data outputs in a way that legitimises policy and security intervention. In a similar vein, I have highlighted how risk assessments produce various representations that determine what 'counts' as risky tied up in political choices and techniques to thwart presumed dangers (Chapter 5). Increasingly automating human tasks with machine learning techniques for cybersecurity operationalises a different way of knowing the 'unknown' enemy, with no preconception of harm. Finally, I have explored how cyber operations like Stuxnet have fed into catastrophic scenarios of future harm, ultimately transforming the means, resources, and political will towards fighting an invisible and unknown yet ostensibly inherent threat within computational networks (Chapter 6).

Through these empirical chapters I have responded to the question by problematising the concrete implications of perpetual political and technical struggles towards achieving 'total security' in contexts of security and technological developments. This has been made possible by drawing on a diverse and interdisciplinary literature from Critical Security Studies (CSS), International Political Sociology (IPS), and Science and Technology Studies (STS) to examine the implications of security practices through a focus on how human-machine relations *work* to produce security problems and with what consequences. Mainly building on frameworks that do not concentrate on a level, nor distinct object of study, I have been focused on traversing scale (Basaran, et al., 2017; Edwards, 2002) to explore relations between meaning and matter (Barad, 2007) and the situated actions and practices in human-machine configurations (Suchman, 2006; Haraway, 2016). This enabled an empirical study of infrastructures (Bowker and Star, 1999; Edwards, 2002, 2010), more recently studied as infrastructur*ing* (Bueger, Liebetrau and Stockbruegger, 2023; Musiani, 2022). Together, in this study I refer to this approach as studying the *enactment of sociotechnical configurations through an ecosystem of devices*

that produce knowledge. Thus, I have reckoned with the political consequences that emerge from enforcing a universalised gaze on technology as something accurate and fixed or as solely objects in the hands of actors. At the intersection of these literatures, I have studied how knowledge is produced *in situ*, and how humans operationalise cybersecurity together with technologies.

The overarching contribution of this thesis has been the operationalisation of a conceptual vocabulary to analytically and empirically approach sociotechnical configurations. The importance of this has been to challenge universalised gazes and trust in the accuracy of technologies and their effects on humans as they become assumed in form. I have both shown and encouraged interdisciplinary research on security to critically and empirically examine how politics unfold, rather than as results or effects of given or static technologies. The remainder of this chapter draws out the thesis' conceptual, theoretical, and empirical contributions, followed by a discussion of the normative ambitions of the research, grounded in the political implications that ensue imaginaries of omniscience and practices of cybersecurity. Finally, I reflect on areas this thesis has inspired for further research.

Theoretical and conceptual contribution

The methodological commitment to studying cybersecurity knowledge production – the situated practices that produce particular ways of representing and acting in the world – has supported the exposure of dominant views and priorities that prevail irrespective of ostensible good will or intent. What is key here is that different tools and techniques, such as the incorporation of machine learning to gain 'better' knowledge about threat and insecurity (i.e., improving 'situational awareness') renders some things known, while obscuring others. Knowledge is not an anthropocentric nor discursive affair alone but a result of particular historically situated configurations. This includes the techniques, protocols, routines, and tools, operationalised to see and know the world and efforts aimed at preventing harm from materialising. For cybersecurity, I have shown how particular practices are shaped by security imaginaries of omniscience. These practices are the assemblage of mechanisms for assessing 'vulnerability' or 'risk'. An idealised omniscience becomes designed into technologies with intent: Therefore, they are *situated* practices with consequences – both intended and unintended - for the enactment of security. How knowledge is produced through a computational world where representations of reality are

accepted as given, or absolute, knowledges, nevertheless highlights some issues while excluding others. In this sense, knowledge about security is always a question of how security *for whom*, *by whom*, and for *what purpose* is produced. The consequence of this is that it simultaneously obscures alternative visions. The world, its political environments, and dealings with security becomes governed to cater to the needs of some – needs that are conceptualised not in apolitical spaces, but through the computational infrastructures infused with preconceptions about who and what threatens and who and what is in need of protection.

Theoretically, I have expanded on Lucy Suchman's human-machine (re)configurations (2006, see also Barad, 2007; Haraway, 2016) for a critical examination of the political implications of emergent technologies that make up the centre stage of contemporary security governance and envisioned futures. By engaging with classical theoretical concepts in STS, including 'inscription devices', 'black boxing' and the related affordance literature, I have recontextualised these for contemporary security environments characterised by automation/autonomous technologies and machine learning devices. STS literatures that have embraced infrastructures/infrastructuring (Bowker and Star, 1999; Bueger, Liebetrau and Stockbruegger, 2023; Edwards, 2002, 2010) have offered a way to address materiality not as a structuring effect, nor in the 'laboratory', but as emergent and contingent on its context. From this end, I conceptualised *epistemic devices* (see Section 1.5) which has theoretically guided the analytical chapters. It was especially operationalised for the study of standardisation in Chapter 3, where protocols for certifying compliance to standards were studied as knowledge producing activities, contingent on conceptual, technical, and methodological instruments (devices) to facilitate the emergence, stabilisation, and circulation of standardised 'best practices'. It has been the conceptual tool through which I have highlighted the critical, yet dense ecosystem of the mundane, 'little things' which are contingent on the 'macro' – the interconnected and political world as it is experienced. Hence, epistemic devices traverse scale (Basaran, et al., 2017; Edwards, 2002). I have in this sense been able to show how the often invisible and seemingly circumstantial devices – protocols, routines, models, data – are never fixed, nor permanent or stable. They are constitutive of the world by co-producing technopolitical imaginaries and materialise political imperatives under the guise of national security.

A second conceptual contribution in this thesis – *green boxing* – builds on the theoretical basis of black boxing (Latour, 1999) yet offers a new perspective on the

sometimes-obsolete commitments to human agency as backgrounded and insignificant. For the purpose of this study, specifically Chapter 4 (Section 4.2), I have used green boxing to explore how imaginaries of omniscience (the militarised ideal to achieve 'situational awareness') permeate the production of threat. While referencing camouflage aesthetics, green boxing does not refer to a specific object but rather seeks to study the sociotechnical configurations through which threats are rendered knowable. Unlike black boxing, which obscures inner workings of technology through routinisation and stability, green boxing remains sensitive to human interpretive labour, where operators are actively engaged in reflexive interactions with technologies for making sense of danger and the production of concrete threats. The concept foregrounds how technologies are neither neutral nor fully autonomous but shaped through this contextualised interaction, where human judgment remains crucial for dealing with the outputs of configured technologies. It highlights the tensions between immateriality and operational clarity, where automated systems promise control and pre-emption yet rely on dynamic human engagement with data outputs for security results. Through the study on IDS and anomaly detection in Chapter 4, green boxing revealed how such techniques enact a warlike posture towards uncertainty, reconfiguring the boundaries between visibility and invisibility, knowability and unknowability, governance and resistance – ultimately offering a more nuanced understanding of the *enactment* of cybersecurity.

Empirical contribution

Empirically, this thesis has shown how multiple cybersecurity knowledges across empirical sites produce understandings of danger. Threats and vulnerabilities are not passively 'discovered' 'out there' but produced in relations that entail different political or technical commitments with normative implications (Suchman, 2006). I have examined the configurations of discourses, practices, and technologies that undergird pathways enforcing visions of 'total security' and the extent to which these imaginaries of omniscience are mobilised. It has shown that they justify increasingly invasive forms of surveillance, militarisation, and market-driven control. The empirical chapters have posed sub-questions to elucidate different and situated configurations as distinct research sites and their political effects. The first empirical site that was explored was the standardisation of cybersecurity products and services in the European Union (EU), specifically the EU Cybersecurity Certification Scheme (EUCC). Standards are by no means arbitrary nor solely

negotiated/contested agreements on 'best practices' but rather an expression where meaning meets matter. In asking how standardisation enacts political authority and renders vulnerability and risk calculable, quantified scoring evaluations that assess product vulnerability versus robustness were shown to be epistemic devices that actively produce and legitimise some visions of security over others. Some concrete political effects include that certain vendors are prioritised, and that the EU exercises global power through normative commitments that restrict market flows and consumer patterns. These normative commitments effectively distinguish security from insecurity, producing a world that is forced to align with the technical vocabulary of vulnerability (that must be eliminated) and security (that must be achieved). In that sense, the mundane and situated practices of standardisation were studied in their rendition of complex and contested issues into calculable categories, where certification is granted a commitment and status that simultaneously functions as an instrument of power and governance by obliging alignment.

The second empirical site explored in this thesis was Norway's National Warning System for Digital Infrastructure, a sensor-based intrusion detection system (IDS) for alerting anomalous behaviour within a network. In questioning how automated machine learning systems aimed at achieving 'total security' reconfigure the production of security and threat knowledge, the analysis showed how IDS have appropriated the militarised logic of 'situational awareness' – omniscient imaginaries that treat irregularities, or anomalies, as inherent dangers. Through interviews with technical operators and strategists involved directly or indirectly with the warning system, I found that rather than automating the identification of threats, these systems generate new forms of uncertainty that demand continuous human interpretation. In here, operators are not passive overseers of automated outputs. Instead, they play a critical role in interpreting, calibrating, and stabilising what counts as a threat within an evolving landscape of ambiguity. The concept of green boxing illuminated how the sociotechnical configurations of IDS are an expression of militarised imaginaries of omniscient oversight, even as these imaginaries remain fragile and incomplete. Importantly, the empirical analysis showed that automated cybersecurity practices are never purely technical but are shaped by anticipatory logics, technical systems and protocols, and imaginaries that make threats knowable and governable. These imaginaries, grounded in a trust that predictive computation produces accurate results, are sustained through recursive engagements between human actors and the design of technological systems. The empirical site thus showed that situational awareness is not a

fixed achievement but a dynamic, reflexive process – revealing cybersecurity as a contingent, contested, and politically charged domain of knowledge production and security governance.

The third empirical site, systems and practices aimed at assessing risk, foregrounded risk as a dominant rationality in contemporary governance across security fields. Here, cybersecurity was shown to operate through preemptive logics that do not rely on discrete, identifiable threats, but on the continuous recalibration and anticipation of the 'unknown' as dangerous. Through systems like EINSTEIN (the U.S. government IDS), threat detection is enacted via searching for anomalies, or irregularities, in patterns of online behaviour, rather than fixed enemy profiles. It produces a dynamic epistemology of risk that privileges sense-making over meaning-making in the timeline of 'detecting' threat and vulnerabilities. In this view, sociotechnical systems not only detect but actively perform security, rendering risk a moving target constituted through behavioural patterns and deviations rather than essentialised adversaries. This *way of knowing* enables governance based on future uncertainty, broadening the scope of what is deemed a security concern and legitimising an increasingly expansive and interventionist security apparatus.

The final empirical contribution of the thesis showed that cyber incidents effectively play into political and economic justifications for maximising threat scenarios and countermeasures. Consequently, alternative epistemologies fade, ultimately transforming conceptions of warfare and violence, normalising digital weaponisation and pre-emptive interventions as rational responses to a supposedly ever-present threat. Questioning discourses of 'cyber doom' after Stuxnet in Chapter 6 demonstrated how singular cyber events can catalyse discursive shifts in both scholarly, media, and policy imaginaries. The strategic relevance ascribed to cyber capabilities post-Stuxnet was not merely the result of empirical effects but was discursively and materially produced. This 'strategic relevance', imagined and projected onto future scenarios, served to reconfigure global security postures – encouraging rearmament, transforming international norms, and embedding cyber operations within normative 'escalation ladders' of conflict. Thus, Stuxnet was explored not only as an operation but as an epistemic event – one that reoriented how cyber capabilities are known, discussed, and institutionalised.

Through these various explorations the thesis has illuminated how cybersecurity knowledge is fundamentally constituted through sociotechnical configurations that not only

produce *understandings* of danger as computational 'vulnerability', 'risk', and 'threat', but actively shapes political imaginaries of digital futures and henceforth the technopolitics of security governance. These profound implications (further detailed in the next sub-section) have manifested in the technopolitics of security governance: The perpetual force of categorising danger into technical and institutional practices subsequently normalises alignment of these as unified and fixed understandings of threat across global institutions. These become amplified by profit seeking corporations that have little interest in guaranteeing equal distribution of 'security'. Rather, they propagate expansive surveillance practices and the normalisation of anticipatory governance that acts upon uncertainty as if it were empirical fact.

The production of cybersecurity knowledges in sociotechnical configurations has not been solely a technical or academic exercise. It has commenced as a study of profoundly political processes with far-reaching implications for how security is imagined, operationalised, and contested. These processes configure not just political orders but the very conditions under which governance claims legitimacy and knowledges claim accuracy and truth. As such, critically interrogating cybersecurity knowledge as normative commitments and how these commitments are produced is imperative for understanding the political intended and unintended effects technopolitics. In that sense, scholars – but also practitioners of policy and security – can be equipped to intervene on embedded assumptions about the world and strive to enact a desired future.

Normative and political implications

Although committing to a reflexive and interpretive methodology, I have not embarked on this thesis devoid of normative ambitions. First and foremost, I have sought to challenge and reframe dominant understandings of cybersecurity, specifically those that pursue – intentionally or not – a 'closing' of the world through technical rationalities of anticipation, surveillance, and control. Through my critical engagement with the imaginaries of omniscience and infrastructures that underpin contemporary security governance, I have intervened on the epistemological and political project that Edwards (1996) termed 'the closed world': A regime of computational and discursive ordering that aims to render the world fully knowable, governable and ultimately securable. In the sociotechnical configurations of cybersecurity, such as standardisation projects, sensor-based monitoring mechanisms, and risk assessment protocols, infrastructures and technological devices do

not simply *respond* to threat but actively *produce* a bordered, legible and manageable world that reflects geopolitical desires, ontological commitments, and asymmetrical relations of power.

Together, my critique that forms the conceptual and empirical contribution of the thesis sheds light on important implications for future security governance and political order. The world becomes simulated through technologies that replicate the world to 'see', 'know' and 'do' security (Suchman, 2023). The promise of accuracy encodes assumptions about agency and legitimacy, thereby contributing to constructing 'apparatuses of recognition' (Suchman, 2020). The apparatus dealt with in this thesis – the appropriation of military logics for cybersecurity – promises to achieve 'total security' through recognition of patterns of suspicious behaviour within networks, subsequently normalising categories of difference, stereotypes, and profiles as dangerous and ensuing countermeasures (Amoore, 2009). These systems are *designed* to enclose the world and stabilise a vision of global order predicated on total visibility, anticipatory control, and the privileging of particular (Western, state-centric) security logics.

I have been geared toward showing how omniscient imaginaries of cybersecurity do not emerge in a vacuum. They are deeply embedded in post-Cold War epistemologies and infrastructures of control (Edwards, 1996), where the world is rendered as a space of ubiquitous threat requiring perpetual monitoring and regulation. The basis for my critique through the course of this thesis has this not been merely descriptive but grounded in normative ambitions. I have sought to challenge strategic narratives of cybersecurity and how the world is constructed as one of pervasive and inherent insecurity, technically producing categories of danger that substantiate expansive surveillance practices under the guise of national security. 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 by profit seeking corporations within and for powerful states – while others, such as in the Global South, are subjected to heightened scrutiny and digital policing. This framing transforms conceptions of warfare and violence, normalising digital weaponisation and pre-emptive interventions as rational responses to a supposedly ever-present threat. Politically, 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.

Cybersecurity is by no means solely a technical or strategic object or goal, but a technopolitical reproduction of hierarchy. Security is afforded some while others are disproportionately subjected to digital suspicion, targeted interventions, and forms of algorithmic governance that reflect neocolonial continuities. This has come to light through the logics underpinning the mundane and the everyday practices of security. Practices that materialise regimes of anticipatory action, such as the design of risk assessments shown in Chapter 5, blur the boundaries between peace and conflict. The use of cyber capabilities in and beyond warfare is legitimised and framed as rational and necessary responses to an ever-present threat. The question of cybersecurity for whom – what counts as risk or violence – becomes obscured. In this thesis I have resisted the closure of the world, and opened up spaces for alternative, non-totalising, and pluralised perspectives on security. Ultimately, my ambition has been to decentre the technological determinism that often accompanies cybersecurity discourses and to foreground the political choices embedded in digital infrastructures. In doing so, the thesis contributes to a broader critical project that seeks to re-politicise security, reassert critique in the face of technological abstraction, and challenge the technopolitical formations that seek to render the world secure by enclosing it. The goal is not to deny the material realities of digital insecurity, but to insist that how we respond to them is always a political question – one that must remain open to contestation.

7.2 Further research on a closed world

Challenging the strategic narrative of cybersecurity has been necessary to remedy the dogma that there are inevitable vulnerabilities and threats that can be 'discovered' and to show that rather than objective dangers, practices and technologies of cybersecurity can only fractionally represent some things, while obscuring others. The political implications of the 'closed world' of cybersecurity are, however, not confined to it. Technology can be explored far beyond the realm of security toward the social and political conditions upon which 'modern' computation is built. As STS scholar Paul N. Edwards called attention to more than two decades ago, new and emerging technologies tend to steal the stage of human awareness. Yesterday's technologies are a thing of the past. They even "reside in a naturalized background" (Edwards, 2002, p. 185). The granting of greater importance to new and emerging technologies in policy forums, among strategists, and in academia neglects the underlying foundations of our societies that shape, and are shaped by, "the

condition of modernity" (Edwards, 2002, p. 186). There is a tension between what is paid attention to – driven by the dominant technodiscourse – and an appetite for intervening on the naturalised assumptions of technology as universal laws that "promote some interests at the expense of others" (Edwards, 2002, p. 191). One might forget, amid commercialised artificial intelligence (AI) and other consumer technologies augmenting everyday tasks, that even the most rudimentary infrastructures of society (roads, electricity, plumbing, the Internet) continue to shape the limits and possibilities of imagining and enacting a world humans can and continue to operationalise.

The impulse to render the world a calculable place can likely be traced back to the Enlightenment (Suchman, 2006). As a modernist assumption and effort to liberate humanity from myth and superstition through *reason*, mythic thinking has instead sustained under a new guise. Instrumental reason, where thinking becomes a tool for control and calculation rather than critical reflection, emerges as a central concern. In this form, reason serves the perpetuation of existing power structures, a model for social domination. From this thesis's critique of enclosed worlds of anticipatory security for rendering the world a dangerous and calculable place, I am motivated to further explore similar configurations in domains such as artificial intelligence (AI), humanitarian aid, border surveillance, predictive policing, and algorithmic welfare.

One need not look far to find sociotechnical configurations with political implications beyond dominating discourses of technopolitics. Take, for instance, Space X's Starlink satellites: Significant attention was directed towards Elon Musk's initiative to provide satellite coverage to replace damaged communication networks for government, military, and civilians in Ukraine (despite the U.S. government ultimately picking up the bill). By contrast, comparatively little attention has been paid to the subsequent threats of rebuttal and restricted coverage (Sabbagh, 2023). Starlink satellite coverage has, for one, been denied in Crimea. It highlights the lived experiences of war today, far from doomsday scenarios that reckon with the terrors of digital futures. It also shows that technologies and digital infrastructures are configured: The design, use and maintenance of satellites for communication, for instance, is not simply a technical system, but contextualised political and economic arrangements that enable and condition possibilities for access. Put simply, the locus of power is inescapably linked to the arrangement of the material means available, economic interests, and political will. In the example of Ukraine, the risk of harm takes a new form in the shape of potentially denied access to communication infrastructures, with

the political undertone of control and threat – but not from a cyber weapon through faraway networks. A different kind of vulnerability comes to light, in this case animated by rich technology conglomerates and avaricious individuals like Musk with a grip on global political issues.

Research in adjacent fields has already begun to surface how sociotechnical configurations function as apparatuses of anticipatory control, often under the guise of neutrality and efficiency – including studies on the work of sensors/sensing (Klimburg-Witjes, Poechhacker, and Bowker, 2021). Some have been particularly attentive to the effects of an enclosed world, including climate governance (Edwards, 2010), warfare (Leese, 2019; Reichborn-Kjennerud, 2025; Suchman, 2023), and algorithmic governance and violence (Aradau and Blanke, 2022). Building on from here, these critical trajectories can benefit from further interdisciplinary and empirical work by bridging Critical Studies on Security (CSS) and Science and Technology Studies (STS). While CSS contributes to foregrounding power projection and asymmetries through discourse and practice, through which security is constructed and operationalised, STS offers the rich toolkit that supports a 'mapping' of how human-machine relations emerge, stabilise and interact in the social world. If research on security and governance can embrace the formation of (in)security not merely as something that has been negotiated and contested, but as agencies, responsibilities, and accountabilities produced from relations, empirically grounded studies will be better equipped to expose universalist claims to security. Such an interdisciplinary synthesis can foster empirically grounded analyses that are sensitive to both security, political epistemologies *and* the materiality of technological artefacts. In doing so, it opens up new avenues for investigating how security regimes are enacted, *how they might be otherwise*, and how moments of resistance can be made legible – not only as empirical events but as political possibilities.

These critical trajectories can be significantly enriched through situated empirical studies that attend closely to the everyday enactments of sociotechnical configurations. While theoretical critiques are vital for exposing the broader political logics and normative stakes of the technopolitics of security governance, empirical inquiry grounds these critiques in lived realities, revealing how power is operationalised, negotiated, or resisted in practice. It can illuminate how actors interact with or make sense of ostensibly closed systems, such as communities affected by algorithmic policing (see Kaufmann, 2024). Empirical research also exposes the contingency and incompleteness of enclosed systems,

showing that infrastructures do not function monolithically but are subject to breakdown, reconfiguration, and appropriation. By studying sociotechnical encounters, researchers can generate critical intervention into how orders are maintained or challenged, and in doing so, make space for alternative imaginaries and interventions attuned to justice, accountability, and democratic possibility.

I stress that empirical studies on security obtain the tools necessary to explore the heterogeneity of sociotechnical configurations. Continuously (over)theorising human machine relationality to a fault, studies of technical and governance regimes risk becoming monolithic and reproducing a universalising gaze. An empirically oriented approach, as this thesis has shown, can foreground variation across domains, contexts, scales and situations. Irrespective of the given research site, one will always and perpetually encounter different observations. The key, then, is to begin not with a sociotechnical configuration in assumed form but instead relish in the heterogeneity of the world. It is essential for understanding how knowledge, authority, and security are co-produced not in the abstract, but through ongoing, situated contexts. Whether studying the use of AI in schools, battlefield simulations, surveillance, biometric borders, transnational financial flows, or undersea cables, empirically situated studies allow scholars to study documents, protocols, manuals, drawings, models – the mundane but powerful devices that implicate social and political orders and security governance. It contributes to a nuanced, accountable, and reflexive mode of analysis that considers lived experiences and political effects of knowledge produced from sociotechnical configurations.