WORK RESEARCH INSTITUTE AFI

National Security, Regulatory Compliance and Insider Risk

A Foresight Report

Tereza Østbø Kuldova, Jardar Østbø, Anna Wangensteen, Arne Lindseth Bygdås, Jason McKillen, Emily Mary Weitzenboeck

OSLO METROPOLITAN UNIVERSITY
WORK RESEARCH INSTITUTE AFI

AFI REPORT 2026:04

THE WORK RESEARCH INSTITUTE'S REPORT SERIES
ARBEIDSFORSKNINGSINSTITUTTETS RAPPORTSERIE

AFI report number 2026:04

Title: National Security, Regulatory Compliance and Insider Risk: A Foresight Report

Authors: Tereza Østbø Kuldova, Jardar Østbø, Anna Wangensteen, Arne Lindseth Bygdås, Jason McKillen, Emily Mary Weitzenboeck

Quality Assurance: Per Martin Norheim Martinsen

Project: Insider: National Security through Private Sector Regulation? Critical Evaluation of Insider Threat Programs and Security Compliance in Current Geopolitical and Regulatory Context

Project leader: Tereza Østbø Kuldova

Funder: Norwegian Ministry of Defence

Published: 24 April 2026

Pages: 104

Illustration/cover image: Photo by Alina Grubnyak on Unsplash

Key words: national security, compliance, insider risk management, preparedness, social dialogue

Abstract: The Norwegian state pursues national security not only through military means and deterrence but also by means of regulation and the imposition of security compliance obligations on regulated entities. Today, the regulatory security state is under increasing pressure from the re-emergence of hard security threats, while failing to address systemic risks. This foresight report explores the possible futures of the Norwegian regulatory security state. In this foresight report, 1) we explore the potential risks associated with *overreliance* on the regulatory security state and its compliance-oriented solutions. To do so, 2) we utilize a combination of critical future studies methods, expert assessments (2-round Delphi survey) and insights from (our) research to think possible futures. We point to the 3) risks of epistemic closure. The report is structured as follows: In chapter 1, we lay the conceptual foundations, place the Norwegian regulatory state in a larger socio-political and technological context, and assess future big-picture challenges. We ask: What could be the future of the regulatory security state considering the current (2026) security environment? In chapter 2, we move from the (inter)national to the organizational level and use the exemplary example of security compliance – insider risk management – to explore the risks associated with a regulatory, risk-based and compliance-oriented approach to national security. In this way, we link macro-trends to the dynamics at the organizational level and reveal several problematic assumptions behind contemporary compliance-oriented security regulation. We ask: What are the potential risks associated with the regulatory tools and solutions favoured by the regulatory security state? In chapter 3, we develop four future scenarios designed to provoke and make us think more seriously about the relationship between national security and regulation. We argue for the need to *expand* our futures imagination, think more holistically about security and build critical futures thinking capacity as part of security and preparedness. In chapter 4, we offer a few actionable recommendations for relevant stakeholders.

ISBN 978-82-7609-503-6

ISSN 2703-836X

DOI: https://doi.org/10.21378/y8xy-2s65

Arbeidsforskningsinstituttet AFI
OsloMet – storbyuniversitetet
Pb. 4 St. Olavs plass
0130 OSLO

Work Research Institute (AFI)
OsloMet – Oslo Metropolitan University
P.O.Box 4 St. Olavs plass
N-0130 OSLO

Telefon / phone: +47 93 29 80 30
E-post / e-mail: postmottak-afi@oslomet.no
Nettadresse / Web address: oslomet.no/om/afi

Preface

Norway has declared 2026 a *Total Defence Year*. All of Norway is to defend Norway – the Norwegian Armed Forces, civilian authorities, the business sector, voluntary organisations, and the population writ large. All are to 'pull in the same direction'[1], as we can read on the website of the Armed Forces. One way – but by no means the only way – in which the state seeks to ensure this alignment in matters of (national) security is by means of regulation. Since the end of the Cold War, we have witnessed the increasing rise and consolidation of the 'regulatory state', including in the security domain. This so-called 'regulatory security state' has benefitted from the peace dividend as states moved from ensuring security largely through direct force, deterrence and coercion ('positive state') to cost-effective regulatory tools and compliance, expert-agencies and private-public partnerships to manage security risks (e.g., Security Act, Digital Security Act, export control and sanctions regimes). Today, the regulatory security state is under increasing pressure from the re-emergence of 'hard' security threats, but it also struggles with regulatory enforcement, capacity, built-in tensions in its model, unintended consequences, and conflicts of interest, as well as failures to deliver on its security promises when faced with systemic risks. What could be the future of the regulatory security state in light of the current security environment? What are the risks associated with the regulatory tools and solutions favoured by the regulatory security state? Should we think differently about regulating *for* (national) security and preparedness? While the regulatory security state relies on risk-based and anticipatory governance solutions, it is rarely subjected to the same gaze. Such an exercise is more urgent than ever given the current security situation and pressures on the international rules-based order. This report is conceived as a contribution to such an imperative foresight exercise.

This report stems from the project *INSIDER: National Security through Private Sector Regulation? Critical Evaluation of Insider Threat Programs and Security Compliance in Current Geopolitical and Regulatory Context* (project no. 203480; 2024–2026), led by Tereza Østbø Kuldova; we thank the Norwegian Ministry of Defence for supporting this independent fundamental research. We would like to extend our sincere gratitude to all the experts that have contributed to this report and to the project at various stages. While the vast majority has chosen to remain anonymous, we would like to acknowledge and thank the following individuals by name: Hans Petter Graver, Inger Marie Hagen, Kristin Reichborn-Kjennerud, Cathrine Lagerberg, Sebastian Larsson, Robert Gjønnes, and Shivangi Narayan. We also thank Per Martin Norheim Martinsen for a quality assurance of this report. This foresight report is also part of the work of the Policy Lab, a strategic initiative building critical future studies research at OsloMet to support policy development for just, secure and equitable societies and human flourishing.

Oslo, 22 April 2026

[1] https://www.forsvaret.no/en/news/articles/total-defence

Contents

Table of Figures

Short Abstract

The Norwegian state pursues national security not only through military means and deterrence but also by means of regulation and the imposition of security compliance obligations on regulated entities. Today, the regulatory security state is under increasing pressure from the re-emergence of hard security threats, while failing to address systemic risks. This foresight report explores the possible futures of the Norwegian regulatory security state. In this foresight report, 1) we explore the potential risks associated with *overreliance* on the regulatory security state and its compliance-oriented solutions. To do so, 2) we utilize a combination of critical future studies methods, expert assessments (2-round Delphi survey) and insights from (our) research to think possible futures. We point to the 3) risks of epistemic closure. The report is structured as follows: In chapter 1, we lay the conceptual foundations, place the Norwegian regulatory state in a larger socio-political and technological context, and assess future big-picture challenges. We ask: What could be the future of the regulatory security state considering the current (2026) security environment? In chapter 2, we move from the (inter)national to the organizational level and use the exemplary example of security compliance – insider risk management – to explore the risks associated with a regulatory, risk-based and compliance-oriented approach to national security. In this way, we link macro-trends to the dynamics at the organizational level and reveal several problematic assumptions behind contemporary compliance-oriented security regulation. We ask: What are the potential risks associated with the regulatory tools and solutions favoured by the regulatory security state? In chapter 3, we develop four future scenarios designed to provoke and make us think more seriously about the relationship between national security and regulation. We argue for the need to *expand* our futures imagination, think more holistically about security and build critical futures thinking capacity as part of security and preparedness. In chapter 4, we offer a few actionable recommendations for relevant stakeholders.

Chapter-by-Chapter Summary

Chapter 1, *Regulatory Security State and its Futures*, introduces the reader to the concept of the 'regulatory security state' (RSS), the emergence of the regulatory security state in Norway, its role in the current geopolitical situation and the forces that will shape its future. The chapter builds on the emerging academic literature on this subject, our own previous research, and a 2-round Delphi expert survey conducted specifically for this Foresight report. The expert opinions collected are used to assess both the weaknesses of the prevalent regulatory approach to national security identified in the literature and the challenges this regulatory security state might face in the future. Why is this important? The Norwegian state pursues national security not only through military means and deterrence but also by means of *regulation* and the imposition of *security compliance obligations* on regulated entities, across both the public and private sectors. We explore what this *indirect* provision of security through non-state actors and leveraging of internal organizational management means in practice. We also assess the inherent and potential risks associated with this regulatory and risk-based approach to national security. We zoom in on the tensions between national security interests and organizational interests which challenge the somewhat naïve assumptions that compliance obligations will automatically lead to an alignment around the state's national security goals. Ensuring such an alignment around *Norwegian* national security interests is important but extremely challenging in a context where 80 % of critical national infrastructure is in the hands of the private sector, where the state depends on multinational corporations, complex global supply chains with obscure ownership structures, on subcontracting and outsourcing and an internationally mobile labour force, and most importantly on private expertise. Systemic interdependencies accentuate the challenges of pursuing 'national control' and demanding loyalty to *national* security interests – both from individuals and companies – in a complex globalized market. The increasing threat of 'weaponization' of this interdependence, which we can observe in action in the Strait of Hormuz as we write, has spurred the state's efforts to reclaim national control. But the answer to regaining this national control is predominantly one of 'securitization' of ever more organizations and societal functions through *more* regulation and security compliance: more ownership registers, more screenings, more due diligence, more risk and vulnerability assessments, more personnel security management and so on. These solutions are ever more detailed, ever more technical, legalistic and techno-bureaucratic, and ever more complex, requiring increasingly specialized expertise. As such, they are largely removed from public debate, suffering from a democratic, legitimacy and accountability deficit. Big Tech, security, legal, audit and consulting firms have become the key actors in the 'compliance-industrial complex', where regulation drives compliance and security markets, while regulation becomes a *de facto* commodity increasingly removed from notions of public good or *national* security. These powerful market actors shape regulation and security management practices through their products; we question their disproportionate epistemic power and authority in the security field and its consequences. We discuss challenges for the regulatory security state 1) in the current security environment, 2) in the current technological environment, and 3) in the global regulatory environment. We identify risks stemming from regulatory and epistemic capture, from the increasing regulatory complexity, from the very delegation of responsibility to regulated entities, from the conflicts of interest between national security and organizational interests, the risks of mission and function creep. The key risk is that compliance systems provide 'ontological security' rather than real security and that the gap between the compliance maps and the actual territory increases. Or else, that we end up with mere compliance illusions that not only do not serve security in the long-run but risk creating epistemic closures, preventing us from thinking better, more seriously and more long-term about security in *public* interest, while hollowing out the values we seek to protect. The juxtaposition of compliance fictions with material realities and the realities of global interdependence also meant that experts

largely agreed that national security cannot be understood separately from preparedness. While this insight may seem intuitive and even banal, in practice this would mean a fundamental rethinking of the national security compliance frameworks and their integration (and thus also transformation) with preparedness frameworks and a more serious refocusing on the material conditions on the ground. This would require a rethinking of preparedness as well, as it has come to suffer from some of the same compliance-driven weaknesses. Our Delphi survey reveals an expert consensus about the failures and structural weaknesses of the regulatory security state. But it also shows how extremely difficult, despite this consensus, it is for experts to imagine better alternatives for future security governance and how unlikely they deem alternatives emerging. This inability to imagine better systems coupled with lacking faith in the possibility for change is particularly troubling in the case of (national) security and speaks to the need to actively cultivate the capacity and capability to imagine better futures.

Chapter 2, *Exemplary Case of Security Compliance: Insider Risk Management*, zooms in on the case of insider risk management to help us better understand how the injunctions of the regulatory security state become translated into concrete security compliance practice. Insider risk management strikes at the heart of personnel security management and thus implies measures that impact workers and employees across Norwegian society. We look beyond the security clearance regime as such and instead consider what it means when managerial approaches originating from the military and intelligence contexts are rolled out as 'best practice' in personnel security management for *all* organizations, including those not subject to the Security Act. Insider risk management has gained momentum following the Russian full-scale invasion of Ukraine in light of the renewed concerns about hybrid threats, espionage, sabotage, and influence operations. The war has reignited Cold War fears of spies, traitors, and leaking of classified information – albeit in a radically transformed geopolitical, economic and security environment. The case of the Russian spy Mikhail Mikushin at the University of Tromsø, returned to Russia in August 2024 to a warm welcome from Vladimir Putin, gave a face to the annual threat and risk assessments by the Norwegian intelligence and security agencies. In response to the security authorities' calls to prioritize personnel security and manage 'insider risk', organizations – both those subject to the Security Act and those that are not – are implementing new comprehensive personnel security policies, systems, and practices such as background checks, monitoring, risk flagging, or vulnerability conversations (*sårbarhetssamtaler*) aimed to tackle the 'threat from within' organisations. A plethora of market-based solutions, consulting products, cybersecurity and monitoring software, have emerged. And while these tools promise to manage insider risk (i.e. risk posed *to* organizations by employees and others with legitimate access), the risk these technologies themselves could pose is rarely considered. In chapter 2, we unpack the relation between the concept of the 'insider' and national security and trace the history of these managerial approaches – from the Cold War intelligence context, via cybersecurity, to their commercialization in the Anglophone contexts of corporate and enterprise risk management divorced from national security considerations. Next, we trace their evolution and translation into the Norwegian context. We show how the fact that it is organizational security and not national security that eventually becomes the object of securing is largely glossed over, as is the conceptual shift from treating workers as a valuable resource towards treating them, and others with legitimate access, as organizational risk and as *potential* threat actors. We show how personnel security management becomes a pre-emptive *management of the potentiality* of anyone with legitimate access becoming a threat to the organization. Following these brief historical excursions, we investigate more closely the key assumptions and blind spots of insider risk management, reading these managerial technologies through a sociological lens. We focus on how these technologies shape our thinking and understanding of security and security threats, what is left out, and how

this thinking reflects particular interests. In particular, we discuss the negative consequences and limitations associated with the hyperfocus on the individual over organizational and contextual factors and the dominance of psy-sciences in the insider risk discourse; we further link these back to how these technologies reflect managerial and organizational interests over national security interests. We then move to a discussion of the legal balancing acts that are required when implementing such technologies and warn against their implementation without considering key regulation such as the Working Environment Act, anti-discrimination or collective agreements. In particular, we warn about their potentially negative effects on the psychosocial work environment. Consequently, we present the expert assessments from our Delphi survey, where we attempted to reverse the risk gaze and asked an expert panel to assess the potential risks stemming from security compliance and insider risk management systems. The gap between compliance maps and realities on the ground emerged as a key concern, as did the dependence on external vendors and complex supply chains weakening internal expertise, accountability and responsibility for security decisions. The top concerns in regard to insider risk management systems were the following: 1) the concern about increasing managerial power and shifting responsibility and placing the blame on the individual, 2) negative effects on employee well-being and the psychosocial workplace environment, such as chilling effects and surveillance-induced anxiety, and 3) the risk of false positives, stigmatization, and discrimination as a result of being subject to opaque managerial technologies. These critical reflections strike at the core premise upon which insider risk management systems are built, forcing us to consider the inherent riskiness of these systems – not a mere 'unintended consequence', but a built-in design feature. The core issues discussed take on an epistemic character, pertaining to the knowledge/power nexus and to the politics of knowledge in (national) security. The implication is that taking security seriously in the future requires sustained attention to who owns and controls the infrastructures of security knowledge, how platform dependencies shape state capacity, and whether AI-enabled governance strengthens or erodes democratic accountability. Without that wider perspective, the likely result is a more deeply technologized form of dependence, in which public institutions become increasingly reliant on black-boxed systems and concentrated corporate power to govern uncertainty.

In Chapter 3, *Future Scenarios: The Possibilities and Limits of Security Compliance*, we look into the future, regarding this exercise as a strategic imperative: the historical home of the RSS was the era of peace and free trade, a period that is ending as we write. The sheer complexity of the present polycrisis makes it important to think again about security. By building future scenarios, we engage in speculation that is necessary to break through the 'epistemic closure' that often limits security discourse to technical fixes. We engage in prospective theorizing, a future-oriented framework dedicated to the active cultivation of desirable futures, considering possible, plausible, and even preposterous eventualities. Moving beyond the traditional research aim of explaining a fixed reality, we recognize that social sciences research also forms part of a world-shaping endeavour. The future cannot be captured by mere linear projections from the present; therefore, we create social imaginaries that allow us to exaggerate, explore, and decisively break with established narratives. The four scenarios are the outcome of a one-day seminar that began with reflections on the results of the Delphi expert surveys, with an eye to the emerging trends and contradictions. The scenarios are not authoritative, methodologically vetted models that seek to represent reality as it currently exists or predictions of what *will* happen, but generative outputs designed to stimulate discussion, provoke debate, and engage practitioners in imaginative accounts of what the future could be. In round 1 of the Delphi, we asked the experts to evaluate a series of statements on possible future developments on two scales, desirable or undesirable and likely or unlikely in the near future (2026–2035). We also asked them to evaluate a series of statements on possible shifts in power and agency as thinkable or unthinkable by 2040. By

framing empirical data within speculative accounts, we invite the reader to look past the 'illusion of control' and engage with the fundamental political and normative questions that will define the security of tomorrow.

The Potemkin World (Scenario 1) was created by taking today's tendencies to their logical extreme. This is not only a way of imagining the future, but also a way of clarifying where we are. Here, states still exist, and they still have laws and nominal constitutions, but these are said to have been integrated into the regulations, and their original letter and spirit are generally forgotten. Social problems, unrest, and environmental damage are persistent and increasing. These issues are not addressed directly, but through regulations, as direct measures addressing causes are deemed too expensive. There is a 'regulatory divide' between white-collar employees responsible for keeping the regulatory machinery going, and menial workers as well as the unemployed residing in favelas outside the regulated zones. Big Tech and Big Audit have merged, having continually sold their allegedly cost-effective solutions ostensibly guaranteeing security to other actors, including the states themselves, thereby gradually taking over their functions, reshaping them in the process, strangling politics, law, and society as such. The positive state with its rule of law has withered away, and the regulatory state is in this sense complete.

The Open Panopticom (Scenario 2) – Panopticom being a reference to Peter Gabriel's song – takes popular discontent and mobilizational potential seriously but also shows the limitations of a radical opposition that nevertheless is epistemically closed, essentially staying inside the logic of the Potemkin World, or else, the regulatory and techno-solutionist logic of today. Here, a popular rebellion has turned the Potemkin World upside down. The regulatory state still governs, its systems largely intact, churning out regulations, but it has succumbed to popular demands of radical transparency. Every procurement contract, every intelligence assessment, and every automated risk-score is reviewed by a global network of citizens and independent analysts. The unelected technocrats and corporate actors of the Potemkin World have lost their epistemic monopoly to metanational forensic collectives. However, monitoring is soon automated, putting enormous strain on the computer centres and the energy infrastructure in its algorithmic war against regulatory and compliance technologies.

Primordial Oligarchy (Scenario 3) is envisaged as what comes following a civilizational collapse. Either the regulatory complex of the Potemkin World or the forensic complex of the Open Panopticom has melted under its own weight, as the result of external shock, or a combination of the two. In the Primordial Oligarchy, the world is essentially a battlefield in a war of all against all. The state system has disintegrated, with armed gangs fighting over spoils, resources, and territory. The Internet as such is down, as the gangs are unable to agree on who is to run the infrastructure, and most computer centres are damaged by hacking, sabotage, and lack of maintenance. Violence is endemic but as time passes, territory and resources are divided between gangs and a more stable stage is reached. Gang leaders discover that to increase their power and popularity, they must provide the population on their territory with security from external threats, basic goods such as housing, food, water, and clothing, and a sense of belonging and meaning. Some oligarchs, as they are now called, even start supporting culture.

Pragmatic-Idealistic Naiveté (Scenario 4) inverts the relationship between 'the good life' and risks/threats familiar from the Potemkin World. Instead of attaining the goal (an undefined good life) indirectly, by eradicating all evils, in the pragmatic-idealistic naiveté we focus on the good life – sovereignty, meaningful relationships, the common good, community, individual freedom, culture, social and physical security and social and environmental sustainability. The cognisance of what we are protecting therefore increases our ability to protect. Here, the positive security state has regained its epistemic authority and expanded its horizons of imagination.

Democratically elected political institutions make political decisions, which are subsequently implemented by dedicated public servants. The democratic state controls what remains of the private security sector, not the other way round. National security is clearly defined as the security of the nation state, not the sum of the self-centred and mercenary interests of commercial and other organisations/institutions. The rule of law is absolute. A strong welfare state provides social security, and culture and education are seen as aims in themselves, not only means to problem-solving, economic growth, and entertainment. This scenario represents an active choice in distinction to the first three scenarios' respective trajectories of total surveillance, total sousveillance, and systemic collapse; it is born from a conscious rupture of the epistemic closure that once limited security to technical fixes.

It is easy to imagine dystopian scenarios, but far harder to address questions of public, social and collective good and how they are to be achieved. It has by now become clear that we need to think harder about the relationship between the state, the private sector and (national) security. If we shift gears and think more in terms of preparedness, we may realize that we need to think far more holistically, and we may reorient security around the concept of the social, around informal capabilities rather than formal compliance fictions. In the world increasingly flooded by AI-generated slop, threatening to fundamentally destabilize knowledge production, we must cultivate the power of critical judgement and imagination. This may be the time for the return of the humanities and social sciences to the fore. Without them, we may have compliant workers and brilliant military engineers, but we may not have a society we wish to live in or a planet to thrive on. And so it might be that the war ahead, might be first and foremost an epistemic one.

In Chapter 4, *Recommendations*, we offer a few actionable take-aways relevant for different stakeholders. We address three key areas which emerged from this report as particularly challenging: 1) the tensions between national security interests versus organizational interest, 2) risks and unintended consequences of security management in the workplace and 3) the need for a more democratic, open and enlightened public debate as well as critically informed futures thinking about security.

1 Regulatory Security State and its Futures

The Norwegian state pursues national security not only through military power and deterrence, but also through regulation and the imposition of security compliance obligations across the public and private sectors. Security is therefore provided not only directly by the state, but also indirectly through non-state actors and through the internal organisational management of regulated entities. It also relies on mobilizing organizations and citizens around concepts such as 'total defence', 'total preparedness' or resilience (Berndtsson et al. 2023; Rongved and Norheim-Martinsen 2022). The current geopolitical and security situation has spurred a revitalization of the whole-of-society approach to national security and preparedness from the Cold War era (Wrange et al. 2024) – albeit in a radically transformed global socio-economic context, following decades of privatization, demilitarization and neoliberal restructuring (Norheim-Martinsen 2019). Ensuring such an alignment around *Norwegian* national security interests is important but difficult in a context where 80 % of critical national infrastructure is in the hands of the private sector, and the state depends on multinational corporations, complex global supply chains with obscure ownership structures, on subcontracting and outsourcing, and an international labour force. These systemic interdependencies only accentuate the challenges of pursuing 'national control' and demanding loyalty to *national* security interests – from both individuals and companies – in a complex globalized world and market with a mobile transnational labour force. The increasing threat of 'weaponization' of this interdependence (Gjesvik 2023; Farrell and Newman 2019) has further spurred the state's efforts to reclaim national control. The answer to regaining this national control is increasingly one of 'securitization' (Mügge 2023) through *more* security-related regulation: more ownership registers, more screenings, more due diligence, more risk and security vulnerability assessments, more security compliance and more personnel security management – all of which are also often more detailed, more technical and more complex, due to digitalization and the embedding of regulation and rules into digital monitoring and compliance platforms.[2] This regulatory complexity poses its own challenges: from increasing dependence on private and corporate expertise and delegating power to unelected experts, technocratic agencies, and regulated entities, to stimulating technological solutionism at the expense of political decision-making (Obendiek and Seidl 2023; Kruck and Weiss 2025). These challenges are even more acute when it comes to the attempts to regulate 'national security' through the instruments of the 'regulatory state' (Veggeland 2010), i.e. through *delegation* of national security-related tasks to an ever broader range of actors, which relies on their *responsibilization* for national security in a context where the state's power and capacity for actual enforcement remains fairly limited.

In this chapter, we briefly introduce the concept of the 'regulatory security state' (RSS) as it emerges from recent international academic literature and translate it into the Norwegian context where it remains understudied. We also map some of the identified challenges and its underlying peace-time logic which can become problematic as the RSS faces increasing pressures in the current geopolitical and security situation. In doing so, we seek to stimulate academic interest in the Norwegian RSS, while also offering some thoughts on the challenges ahead, informed by the expert opinion collected for this report. So far, there has been very limited debate about the use

[2] A case in point is the report by the expert committee on national control with critical digital infrastructure, which proposes to increase governance capability of the Norwegian state through more regulations, ownership control, screenings, due diligence and risk-reduction measures when it comes to vulnerabilities stemming from interdependence. The digital realm is probably the best example of global interdependence, and the challenges associated with reasserting national control (Nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur – målbilde og virkemidler, 2025, https://www.regjeringen.no/contentassets/2e1a90bedf6648f89c1a37d0f99dabf1/no/pdfs/ekomsikkerhet.pdf). For an analysis of this dynamics in relation to EU and 'the security logics invading the domain of technology regulation' (Mügge 2023, 1432).

of regulatory tools in the context of national security, both internationally and in the Norwegian context. We can speculate that the reason behind this lack of research and public debate has been the fact that the RSS had been restricted to designated and limited areas prior to the Russian full-scale invasion of Ukraine in 2022, and therefore also relatively hidden from the public view and hence also from public debate. However, following the invasion, and the increased threat of hybrid warfare from Russia, China and other state and non-state actors, we have seen a sharpening of security measures and their proliferation across the whole of society. A case in point is the Security Act, which has both expanded its reach and acquired a unique ideological force, profoundly impacting security management practices in the years since the invasion. This has also coincided with the use of other regulatory tools, be those export control or sanctions regimes or the Digital Security Act.

Another reason for the rather limited debate about the regulatory security state and how (and even whether at all) national security can be achieved through *regulatory* tools, may be the regulatory complexity itself. This includes the competence required to orient oneself in the regulatory maze, and the techno-bureaucratic character of measures imposed. The level of regulatory complexity makes it particularly difficult to lift our gaze and think in a more principled manner about these regulatory tools – their making, their blind spots, their enforcement, their interaction, and their intended and unintended consequences. This speaks to the *epistemic* and *infrastructural* power of this regulatory model of governance, and to the *epistemic authority* of certain forms of expertise upon which it relies (Obendiek and Seidl 2023; Kuldova 2022; Schilde 2023). However, the current security situation, not to speak of the polycrisis we are facing (Lodge 2025), is already revealing the cracks in this regulatory logic. We need to ask whether security compliance works as regulators intend, whether it *effectively* serves long-term national security interests, whether it is *legitimate*, or whether it is a box-ticking and report-generating exercise that perpetuates a mere illusion of state control. We also need to ask whether the RSS can eventually fall victim to its inherent contradictions and/or generate new security threats. And if so, what would this mean and what can be done to mitigate this. We see this as a necessary and rather pressing speculative exercise, which could help us break through what we view as a pervasive 'epistemic closure' in this field (Kuldova and Østbø 2026). Therefore, in this chapter, in addition to the introductory review of recent academic literature and insights drawn from our own research on this subject as part of this project (Kuldova 2024; Kuldova and Østbø 2026; Norheim-Martinsen 2026), presented in 1.1., we present results from an expert Delphi survey on the potential futures of the regulatory security state. The results of the survey are presented in 1.2. This chapter lays the conceptual foundations and framework for the discussions to follow across this report – as we zoom in on security management in the workplace in chapter 2, present further results from the Delphi survey in 2.2. and move to the explorative sections and future scenarios in chapter 3 designed to force us to think of some fundamental underlying challenges identified across this material. We therefore strongly recommend a linear reading of this report, as we move from the level of the state, placed within a larger context, to the organizational level and then pick up the threads across these levels, and look into the future. Understanding the recommendations presented at the end presupposes such a linear reading. We hope that this report will help open a more principled debate around security and about the ways in which we seek to achieve this necessary goal for the state and society – or else, how we go about achieving the very *raison d'être* of the state.

1.1 National Security and the Regulatory Security State

The concept of the 'regulatory state' was famously launched by Giandomenico Majone in his influential article 'The Rise of the Regulatory State in Europe' (Majone 1994), which documented its emergence in the context of privatization, deregulation and introduction of neoliberal policies. It may be instructive to return to this seminal piece and remind ourselves of the fundamental premise upon which this crucial shift in state governance rests, one that we today largely take for granted and rarely question, but the inherent contradictions of which become ever more pressing. This is how Majone contrasts the dirigiste or positive state with the regulatory state and sums up the shift towards the use of legal and regulatory instruments over redistribution and other tools of stabilization:

> 'the purpose of public ownership was not simply to regulate prices, conditions of entry and quality of service, but also to pursue many other goals including economic development, technical innovation, employment, regional income redistribution, and *national security*. While nationalisations and other traditional forms of direct state intervention were thus justified by appealing to a variety of often conflicting goals, regulation has a *single* normative justification: improving the efficiency of the economy by correcting specific forms of market failure such as monopoly, imperfect information, and negative externalities.' (Majone 1994, 79, emphasis added)

To put it simply, the origins of the regulatory state lie in the faith in the market and its ability to resolve most of our problems, provided it is regulated for *efficiency*. At the same time, regulation itself is posited as a cost-efficient way to achieve this goal. The rise of the regulatory state has benefited from the so-called peace dividend following the end of the Cold War and must therefore be understood in the context of globalization, demilitarization, the hopes of democratization through marketization, and visions of the 'end of history' and of the ultimate triumph of Western liberal democracy (Fukuyama 1992). Fukuyama's prophesies, which at one point appeared accurate, did not age well after all. The question is – how do national security and the *public and common good* of security fit into regulatory architectures designed around *market efficiency* and liberalization and an assumption of deep peace? Are there fundamental tensions between profit interests and national security interests (Notaker 2023) that we disavow in our quest to enlist and mobilize all in the service of *national* security (Petersen and Tjalve 2015)? These questions become more acute today as we bear witness to the emergence of the 'regulatory security state' (Kruck and Weiss 2023b; Levi-Faur 2023). But before we turn to this recent evolution of the regulatory state, it may be helpful to recap some of the core features and criticisms which have been raised against the 'regulatory state' as such – and which, as we shall see, also resonate across the expert perspectives collected in our own survey.

In theory, we distinguish between two states: the 'positive' state and the regulatory state. The positive state operates through spending, ownership and direct provision and is focused on outcomes. The regulatory state operates by setting, monitoring and enforcing rules and relies on steering, rules, standards, compliance, reporting duties, risk management, oversight, monitoring, *delegation* of power to specialized expert agencies, regulated enterprises, the private sector and (international) standard-setting organizations, and on the creation of frameworks for *how* outcomes are produced. In this sense, it is *decentred*: governance is spread across different ministries, agencies, regulators, standard-setters, auditors. It also relies to a large degree on private sector and corporate expertise and private standard-setting. As such, it can be understood as a form of meta-regulation, responsibilizing organizations to develop their own compliance and risk-management systems in response to the (often rather general) guidance provided. This effectively turns the regulated entities and private actors into *de facto* co-regulators and shapers of regulation as they translate open-ended demands of the regulatory state into operational rules

and practices and technical standards which are positioned as the answer to the regulatory demands of the state (Carrapico and Farrand 2017; Diller 2012; Olsen et al. 2019). The regulatory state tends to frame problems as *risks* to be managed, and can therefore also be understood as a 'risk state' (Levi-Faur 2023). This already implies particular ways of understanding the world at the expense of others, shaping what is visible and thus governable. The regulatory risk state is predominantly *process-oriented* rather than necessarily outcome-oriented; it tends to focus more on audits, documentation and management systems than actual realities on the ground. What tends to be disavowed in these regulatory approaches is the fundamental fact that public objectives do not automatically converge with private interests; the *risks* associated with this mismatch of objectives and interests, are, curiously enough, rarely openly discussed by policymakers. This can be seen as an interesting and rather paradoxical feature of the risk state, which articulates certain risks but disavows and neglects others. This points to the obvious socially constructed character of risks. The question we should be asking is: what risks are being made *not* to matter? '[H]ow is risk being made *not* to matter? And what are the ramifications for the risk paradigm as a mode of managing uncertainty?' (Stavrianakis 2020, 234).

Most contemporary states are *hybrids* of these two forms; the distinction between the regulatory and the positive state may be considered an 'ideal type' (Weber 2012) that does not exist in any pure form in actual reality. But the concept helps us immensely to think and conceptualize recent developments. However, it cannot be used alone. In addition, we also need to consider the increasingly dominant element of 'algorithmic governance' (Kuldova, Gundhus, et al. 2024; Katzenbach and Ulbricht 2019), as rules become inscribed into digital and algorithmic infrastructures. In Norway, the positive welfare state persists, but even here the regulatory state is experiencing significant growth, exerting substantial ideological force at the expense of the positive state, with digitalization playing an important role in this process. Noralv Veggeland has documented in great detail the rise of the Norwegian 'regulatory state', the effects of European integration and the transformation of the welfare state through the introduction of market mechanisms, privatization, and technocratic arm's length bodies, agencies and regulatory institutions and public-private partnerships, to deliver public services (Veggeland 2010, 2020). Veggeland has pointed to several challenges related to the regulatory state, which have also been raised by other scholars (e.g., Veggeland 2020; Majone 1997; Kruck and Weiss 2023a; Levi-Faur 2017; Kenneth et al. 2017). Key among these are: the democratic and legitimacy deficit (less government for and by the people); lack of accountability and transparency; fragmentation of governance creating overlapping jurisdictions and challenges for coordination; the enormous complexity and layering of regulatory systems making it difficult for policymakers, citizens and stakeholders to navigate the system; delegation of responsibility to regulated entities and experts across the public-private divide; excessive regulation, or 'hyper-regulation' and frenetic institutional innovation; rising transactional costs burdening public budgets and inefficiency; marketization of public services undermining universal and collective welfare and public goods; proliferation of new risks, negative externalities and vulnerabilities such as social inequality, deterioration of social cohesion, erosion of trust in governance, environmental degradation or security risks related to interdependence, and the hollowing out of ethics.

While the logic of the regulatory state pervades most areas of policy making, only recently has its role in the matters of foreign and national security policy come to the forefront. Historically, national security sat at the very core of the sovereign 'positive state' with its armed forces, police and intelligence agencies (Majone 1997; Genschel and Jachtenfuchs 2023). The transnational and interdependent character of modern 'hybrid threats' (e.g., cyber threats, dual-use technologies, supply chain vulnerabilities), however, spurred risk-based regulation and the increasing delegation of security functions to private actors. This has turned these into co-

producers of security and co-regulators in security matters precisely at the same time as investments in the positive security state diminished, i.e. in the period of demilitarization. In simple terms, the regulatory security state relies on 'setting regulatory incentives for other non-state actors to make security' (Kruck and Weiss 2025, 149). This means that the very content and understanding of 'security' and of the domains to be securitized are shaped by a broad range of actors, well beyond policymakers. What is considered as security and the proper object of security measures is to a large degree contextual, historically contingent and changing in tandem with political, social and economic interests (McDonald 2002; Buzan et al. 1998). This means that security and how it is to be achieved has been and can be conceptualized in different ways and is a result of epistemic, political, and economic power struggles, despite its deceptively intuitive meaning. The present regulatory arrangements also make 'security' inherently prone to regulatory capture, beyond the obvious concerns about lobbying; 'epistemic capture' and reliance on particular forms of expertise and experts makes active regulatory capture *de facto* redundant. Moreover, the number of actors engaged in security governance across multiple levels – from multinational, national to organizational – keeps on increasing. The core question is whether the alignment of these actors around the security interests of any *particular* nation in a complex and interdependent global market and regulatory environment is a mere regulatory fantasy – albeit one that has very real consequences (intended or not).

Over the past years, the use of sanctions regimes and export controls, although not new, has ballooned. We have come to routinely speak of geoeconomics, 'chokepoints' and the 'weaponization of interdependence' (Fishman 2025; Farrell and Newman 2019). Or else, of pursuing national security policies by leveraging global regulatory and financial architectures and bureaucracies and internal managerial infrastructures within businesses and regulated entities. These can be seen as part of the toolbox of the 'regulatory security state' (Kruck and Weiss 2023b; Levi-Faur 2023). These tools rely on regulatory compliance and their operationalization and interpretation by regulated entities who become co-producers of security, supported by consultants, legal experts, and digital tools. '*De facto*, sanctions regulations delegate decision-making power to for-profit actors because the latter are required to assess the risk of specific transactions' (Giumelli and Onderco 2021, 193). In response to the demands of the regulatory state, new markets in regulatory compliance have emerged. These are today key actors shaping *how* security is conceptualized (Kuldova 2022; Tsingou 2018). However, despite the ever-increasing number of regulations, guidelines, surveillance architectures, control regimes, reporting, and compliance products, we struggle with proliferating security threats and uncontrollability (Rosa 2020). We have come to speak of 'regulatory capitalism' (Farrand and Carrapico 2018) as regulatory compliance became commodified and regulation aligned with profit interests. And we have come to speak of 'decentred regulation' (Black 2002), that is, the ways in which regulation no longer centres on the state, but is diffused through society and markets. While the security compliance markets have grown and security regulation is diffused across society, it is questionable whether we have become more secure. Have we created elaborate systems, bureaucratic routines and organizational *rituals*, that merely perpetuate an illusion of security? Could it be, as Aradau suggests, that 'responsibility' is in the context of the regulatory security state 'artifice, appearance rather than substance' and that 'the response to an unexpected event is ordered at the level of appearance'? (Aradau 2010, 5). Asking such questions may appear theoretical and far-fetched for security, intelligence and military practitioners. However, we believe it is necessary if we are to take long-term security seriously. These questions and concerns also echo in the responses of our experts. Another question is whether we have become more *resilient*, more prepared, or whether the ways in which security is understood by the dominant security compliance regimes and industry conflicts not only with the

goals of the national security state, but also – and likely even more fundamentally – with the goals of preparedness, resilience and human-centred security.

Could it be the case that compliance systems contribute to *ontological* security rather than physical or substantial security? Sociologists (Giddens 1991) and international relations scholars (Steele 2008) have pointed to how individuals and states alike deal with the anxiety stemming from the uncertainties of the late modern world by establishing routines of behaviour and cognition that uphold their 'biographical continuity'. Ontological security is not an *a priori* bad thing or necessarily counter-productive or detrimental to physical security. But when ontological security is connected to an identity that is obsolete or even delusional, not recognized by others, and resistant to changes in the surrounding world, it becomes a problem. Translated to our topic at hand, we could argue that the regulatory routines and rituals uphold the state's self-identity of a Fukuyaman early post-Cold War, liberal, flexible, cost-reducing, optimizing entity entering into contractual relationships with other law-abiding domestic or foreign entities on a win-win basis. Self-identity is relational (Mitzen 2006), and when confronted with a lack of recognition from others, including non-state actors, the state may react, sometimes frenetically, with more of the same routinized behaviour. For instance, some theorists of ontological security argue that when other great powers refused to recognize Russia as a great power entitled to rule-breaking and a sphere of geopolitical influence, it reacted by behaving as if it was such – by launching the full-scale invasion of Ukraine (Słowikowski and Klonowski 2025). This decision did by no means improve Russia's physical security, but it confirmed the West's allegedly ingrained hostility towards Russia, thus sustaining the Russian identity trait of being misunderstood and groundlessly feared by the West (Hansen 2016). Although there is a great difference between Russia's criminal regime and the Western regulatory security state, the dynamics are basically the same: Confronted with anxiety stemming from uncertainty, a rapidly changing geopolitical situation with unclear threats lurking and ever-new risks and vulnerabilities emerging everywhere, the regulatory state responds by generating ever-new regulations, transforming anxiety into fear, acting as if history had ended like Fukuyama said, as if the liberal, rules-based order was not in terminal agony. In short, could it be that we are ontologically secure but *de facto* unprepared?

For now, suffice it to say that these systems have, on top of displaying ritualistic tendencies (Aradau 2010), also been shown to be prone to evasion, as both recent research (Kuldova, Østbø, and Shore 2024) and the annual threat assessments from the Norwegian Intelligence Service make clear.[3] Next to evasion and defiance, there is a simultaneous issue of over-compliance and derisking (Giumelli and Onderco 2021). The unintended consequences and counterproductive results of these measures have been meticulously documented by Agathe Demarais in her book *Backfire: How Sanctions Reshape the World Against US* (Demarais 2022). The failures of sanctions regimes to function as intended by the regulator reflect to a large degree both the complex global and interconnected nature of markets and societies, as well as the profit-maximizing interests and risk-calculations made by business actors translating these sanctions into concrete practices. It is precisely this dimension – of how regulated entities interpret and translate regulations into concrete practice – that is widely understudied. Legal, political science and IR perspectives, often rather detached from actual realities on the ground, dominate in security and foreign policy discourses. Alas, the fact that this dimension remains understudied is not surprising given the difficulties of accessing corporate compliance departments; public documents can only reveal so much. This is even more difficult in the context of security, where security compliance measures are actively kept under the locker and beyond the reach of independent researchers. This means that we have to rely on a multitude of open sources and documents, perspectives of interviewees with industry insights, participation at open industry

[3] *Focus* 2026, p. 45. https://www.etterretningstjenesten.no/publikasjoner/focus

events, and expert assessments when studying the regulatory security state in practice (M. Ericson and Wester 2022). At the same time, we have enough research-based insight to argue that the widespread circumvention, evasion and counterproductive repercussions point to the inherent challenges of aligning national security interests with the profit interests of regulated entities, to the limits of the regulatory approach – and to the challenges of controlling its actual *outcomes*.

Furthermore, the approach of the regulatory security state is by no means unique to Western liberal democracies; weaponization of regulation is widespread across jurisdictions, often placing multinational corporations and other organizations operating across jurisdictions into what can be deemed 'regulatory crossfire', as organizations get caught up in competing regulatory demands. China has been expanding its regulatory toolbox: The Chinese National Intelligence Law, to give an example, imposes its own compliance obligations on Chinese companies to share data with the authorities; the 2021 Counterespionage Law compels businesses to work with national security agencies to train staff in counterespionage techniques targeting foreign intelligence and 'Chinese collaborators' alike (Cunliffe 2021) – targeting 'insider threats'; and the Anti-Foreign Sanctions Law (2021) established a toolkit of countermeasures vis-à-vis Western sanctions, such as asset freezes, visa cancellations, restrictions on conducting business and more, to safeguard its national security and sovereignty. We are likely to see more tit-for-tat anti-foreign sanctions measures in the future (Yang 2025). Operating across jurisdictions can mean that obeying US and EU sanctions can be treated as a violation of Chinese law. Russia has similarly weaponized a series of laws regulating internet and data privacy to ensure the FSB's access to data held by private companies on its territory, and developed elaborate top-down regulations to protect its critical infrastructure, including monitoring by state agencies and requirements to implement malicious insider threat detection systems (Pursiainen 2021). Where Western actors seek to enlist private actors as partners in ensuring national security and societal resilience, resorting to the imposition of compliance obligations and (moral) responsibilization (Petersen 2012), authoritarian states weaponize laws in a more direct and top-down manner. Both liberal and illiberal states, however, seek to leverage the managerial infrastructures and data of businesses for their own national security interests, however these may be defined in any particular political, economic, and cultural context.

But the 'regulatory crossfire' does not only pertain to questions of jurisdiction: regulatory compliance obligations are imposed in many domains of policymaking at the same time, with different or even competing policy objectives, underlying rationalities, normative assumptions and historical trajectories. Yet there is no *holistic* understanding of how rulemaking in one domain translates into another domain and how different social goals are to be weighed against each other within one and the same organization. To the contrary, we live in times of regulatory complexity, legal fragmentation and regime-collisions in both national and global law, in addition to the increasing role of private standards and compliance frameworks (Fischer-Lescano and Teubner 2019). In practice, the concrete balancing acts between different goals – e.g., equality and non-discrimination, civil liberties, freedom of speech, privacy, due process, fairness vs. national security – are *delegated* to the regulated entities, opening up a large space for discretionary judgement and for new markets in compliance products. This is both an effect of state agencification and sectoral fragmentation along narrow sectoral expertise, and of legal globalization, legal pluralism and proliferation of autonomous private legal regimes; these processes in themselves challenge the rule of law and civil rights. The collisions of these regulatory regimes raise issues of norm conflicts, competing rationalities and the proportionality of measures that are being implemented. But they also reflect the underlying fundamental societal contradictions of the globalized, interconnected and interdependent world.

At the moment, we are witnessing the simultaneous growth of the regulatory security state and a return of the 'positive state' as high-intensity threats return, large-scale interstate war in Europe and the Middle East is a reality, and the future of the NATO alliance is increasingly uncertain. It is yet unclear what this simultaneous growth will imply and what the consequences of the expansion of security measures will be. While funds channelled into the armed forces increase and regulatory architectures expand, this re-armament and securitization happen increasingly at the expense of the welfare state, with its fundamental role in human security, societal trust and legitimacy of government appearing to be increasingly forgotten. Unlike in the Cold War period, when the welfare state was being built alongside strong militaries, the 'warfare' state today *competes* with the 'welfare state'. Citizens are told to prepare to sacrifice (at least some) welfare goods at the altar of military spending, while both welfare and some of the security goods are to be delivered by the efficient market through the regulatory arm of the state. The latter, however, has been shown to generate new security threats of its own, from increased inequality and poverty, precarity, societal polarization, declining public trust, etc.

The question is whether this regulatory approach, in the long-term, will serve national security or if the abandonment of more holistic visions of human-centred security (McDonald 2002) will create more and deeper security issues in the long-term. This is ultimately both a political and a normative question which is, almost per definition, outside of the bounds of the regulatory security state as it currently exists. Below, we will delve a bit deeper into the character of the Norwegian regulatory security state and the challenges associated with it, before we move to how the expert panel looks at the future of RSS in the current geopolitical and security context.

1.1.1 The Norwegian Regulatory Security State: From Threat Assessments to Risk Management and Private Standardization

In the white paper *National control and cyber resilience to safeguard national security* we can read that the Security Act is the Norwegian state's 'most important tool for safeguarding national security' (Meld. St. 9 (2022–2023) 2022, 15), while also being 'cost-effective' (Meld. St. 9 (2022–2023) 2022, 14) for the state. The Security Act[4] and the Security of Undertakings Regulations[5] are indeed central for the Norwegian regulatory security state as the regulations responsibilize organisations who fall under their purview, who must comply by implementing a broad range of protective risk-based security management measures and be audit-ready at any time. Other key laws, such as the Digital Security Act[6] which applies to providers of essential services and digital services providers and implements EU's NIS1, imposes parallel obligations to implement technical and cybersecurity measures informed by risk-management, due diligence, reporting, notifications etc.; non-compliance can result in fines and administrative sanctions, and leadership can be held personally liable. We also see a proliferation of new instruments of more direct governmental intervention, such as investment screenings, which impact corporate transactions, symptomatic of the aforementioned weaponization of the economy and economic coercion. This has been described in the US context as the 'national security creep' into the domain of corporate transactions (Eichensehr and Hwang 2023); Norway, has, under the Security Act,[7] implemented a similar Foreign Direct Investment screening mechanism and transactions review, which has so far

[4] Act relating to national security, LOV-2018-06-01-24 https://lovdata.no/dokument/NLE/lov/2018-06-01-24
[5] Regulations relating to the protective security work of undertakings, FOR-2018-12-20-2053, https://lovdata.no/dokument/SFE/forskrift/2018-12-20-2053
[6] Lov om digital sikkerhet, LOV-2023-12-20-108, https://lovdata.no/dokument/NL/lov/2023-12-20-108
[7] Vedtak til lov om endringer i sikkerhetsloven (eierskapskontroll og lovens virkeområde) https://www.stortinget.no/no/Saker-og-publikasjoner/Vedtak/Beslutninger/Lovvedtak/2022-2023/vedtak-202223-116/

focused largely on companies in sectors such as defence, telecommunications, energy and other critical infrastructure.

While laws and regulations are indeed central to the Norwegian regulatory security state, it also relies on *normative* power, seeking to influence security practices *beyond* those regulated. In response to a question by Mari Holm Lønseth (The Conservative Party of Norway) on the current standing of the implementation of the Security Act, Astri Aas-Hansen, the Minister of Justice (Labour Party), responded:

> 'All Norwegian businesses should have an overview of their assets and ensure a proper level of security, even if they are not subject to the Security Act. The work under the Security Act to subject businesses and identify assets worthy of protection is a continuous process. The assets, threats and vulnerabilities, and with it also the risk, change, among other things, with the security policy picture and changes in society in general. The national asset mapping will therefore never end up in a static list of objects and infrastructures. There may be assets that are designated today that do not need shielding tomorrow, and it must be assessed and reassessed whether these are the right assets that have been designated over time.'[8]

This statement is interesting in itself as it translates 'total defence' into an imperative for organizations to map and protect their assets against threats identified by the intelligence agencies, be they subject to the Security Act or not. National security thus emerges in this discourse as a sum total of each individual organization's protective and preventive security management. This approach also encourages the *expansion* of security management principles originally developed first and foremost for the protection of highly sensitive *classified information* and *critical infrastructure* from *espionage* and *sabotage* as a general 'best practice' approach, whether the assets to be protected are of any relevance to national security or not; this immediately raises the question of *proportionality* and the consequences of delegating responsibility for *national* security to the organizational level. It also raises more fundamental questions. Hans J. Morgenthau in 1955, following the Red and Lavender Scares and McCarthy's purges in the US Department of State and Eisenhower's Executive Order 10450 that institutionalized the hunt for 'subversives' and 'sexual perverts' and ousted hundreds of competent diplomats as 'security risks', asked the following questions:

> '(1) What is to be secured? (2) Against whom is to be secured? (3) By what means is it being secured? (4) What is the cost of security in terms of other objectives to which the nation is equally committed?' (Morgenthau 1955, 9)

While the context has changed, these questions re-emerge as relevant today and should in each instance be carefully considered against actual national security interests. In practice, the first three questions tend to be reduced to a matter of risk management, while the highly important question 4 is rarely explicitly dealt with in the context of the regulatory security state. The balancing acts are in practice delegated to the regulated entities with their own interests and objectives. Moreover, it is not their task to evaluate either the costs in terms of other state objectives or risks posed by their security management systems to society, public good, or other collective interests. Ensuring a balance between different state objectives and proportionality in implementation should be the proper responsibility of the state. However, this becomes a difficult if not an impossible task for the regulatory state relying on expert agencies and multi-agential and networked governance. This is precisely why locating accountability and legitimacy becomes exceedingly difficult within this system and why researchers speak of democracy, legitimacy and

[8] Skriftlig spørsmål fra Mari Holm Lønseth (H) til statsministeren, document nr. 15:1507 (2025-2026) https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qnid=114698

accountability deficits. Outlining the contours of the Norwegian regulatory security state and all the players involved at different levels can provide some hints at how these deficits emerge in practice: Laws and regulations are one thing, their operationalization, interpretation and translation into organizational practices is another matter. Where law ends, the sociology and anthropology of law begin; the latter implying a consideration of the power of different actors shaping the field, its epistemologies and the actual ways in which threats and security are understood and managed.

There are the obvious state actors: The Storting (Parliament) with its legislative power, the Department of Justice and Public Security and the Department of Defence are responsible for national security strategies and policy and the intelligence agencies – the Norwegian Police Security Service (PST) and Norwegian Intelligence Service (NIS). The Directorate for Civil Protection and Emergency Planning (DSB) is primarily responsible for societal security, preparedness and emergencies, and is central in total defence and can be understood as a generalist for societal security. While it complements the National Security Authority (NSM), discussed in more detail below, it operates with its own understandings of security, which are anchored in discourses of *resilience*, *preparedness* and *crisis management* primarily in the physical world. We will briefly address some of the contrasting perspectives towards the end of this report.

The National Security Authority (NSM), Norway's specialized agency for national protective security, an expert and advisory body, supervisory authority and operator of a national warning and coordination system for critical infrastructure and cybersecurity, is a central node in the Norwegian regulatory security state. In addition to a plethora of guidance documents on the aforementioned legislations[9] which it is tasked to enforce, it also issues general guidance in the form of 'basic principles' intended for *any* organization[10], in alignment with the statement by the Minister of Justice above. An important function of NSM is to translate the annual threat assessments by the PST and NIS into the logic of risk management; as such, the agency is the primary expression of what Levi-Faur analysed as the 'risk state' (Levi-Faur 2023). Through its annual *Risk* report, NSM sets the tone for the operationalization of the threat assessments by intelligence agencies in Norwegian organizations and society. It is also tasked with awareness raising about security risks and their management; from the annual security conference to podcasting, courses and media presence or participation at Arendalsuka, NSM has in the past several years become increasingly visible in the public discourse. This has also been the case for PST, which, too, hosts a podcast and has been increasingly open and concerned with threat awareness raising in the Norwegian population. The increased presence of these agencies in the media also raises the question of how these communication acts are understood and translated into practices within organizations. As an expert agency, NSM has both considerable epistemic power and authority in the field, and as such shapes the 'episteme' of the regulatory security state (Adler and Bernstein 2004), but it is not the only actor with such power. Three main strands of thought inform how NSM understands security management primarily in terms of its *operationalization* at the organizational level: 1) general *organizational* risk and security management, including physical/object security, 2) cybersecurity and cyberthreat management and 3) personnel security management which builds on the security clearance regime and

[9] The guidance and handbooks by NSM can be accessed here: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker/
[10] The basic principles for security management, physical security, personnel security and ICT security can be accessed here: https://nsm.no/regelverk-og-hjelp/grunnprinsipper/

focuses on the management of individual vulnerabilities. It is immediately clear that much that is relevant to national security falls outside the scope of these approaches.[11]

Given this focus, NSM guidance also incorporates references to private technical and management standards, from standards on cybersecurity to the risk management of unwanted events, such as the popular NS 5814 and the NS 5830-series. The market offers a plethora of security standards, national and international, be these supplied by ISO, Standard Norway or other standardization actors (Mehus et al. 2026). This incorporation of private standards into public guidance speaks to the power of private standardization bodies and technical standards developed by stakeholders and technical experts. While these processes are in theory open to anyone with the time, funds and interest to participate in standardization, in practice standards are developed by those with a stake and/or profit interest in any particular standard (e.g., consulting firms selling managerial products to comply with these standards); participating in the standardization processes is prohibitively costly and stretches over long periods of time for any independent researcher to participate (Timmermans and Epstein 2010; Diller 2012; Forsberg 2012). Hence, to a large degree standards reflect industry interests, even if public sector representatives occasionally participate in standardization processes; and while the latter may superficially provide more legitimacy, these processes remain fundamentally non-transparent. Privatized standard-setting (ISO, Standard Norway etc.) is particularly prevalent in cybersecurity and in the governance of cyber risk which relies to a very large degree on private expertise – to the degree that cybersecurity is unthinkable without the private sector and cybersecurity strategies rely explicitly on public-private partnerships and responsibilization of the private sector for national security (Smeets 2023). Despite longstanding questions regarding the efficacy of market-driven approaches to security and the fundamental disjuncture between private interests and national security interests, this interdependence has only further deepened (Carr 2016). Not only are we dependent on private infrastructures and products, but also on security standards developed by the same industries that the state seeks to regulate; this speaks to the profound shift in the relationship between the regulator and the regulated as the regulated become co-producers of security and co-regulators and as technical-operational standards come to structure security governance and permeate public guidance (Bellanova and De Goede 2022a). The industry is actively shaping the standards and the very regulation to which it then becomes subject (Carrapico and Farrand 2017). Standards become effectively depoliticized carriers of security priorities; but while they may appear technical, they are deeply political and reflective of market interests and the struggles to establish ‘epistemic authority’ (Dunn Cavelty and Smeets 2023) – one that can be translated into profit – from certifications to consulting.

Risk management standards are some of the most popular types of ISO and NS standards. Risk management is sold as an answer to any number of contemporary problems – what David Garland has analysed as the ‘rise of risk’:

> ‘Today’s accounts of risk are remarkable for their multiplicity and for the variety of senses they give to the term. Risk is a calculation. Risk is a commodity. Risk is a capital. Risk is a technique of government. Risk is objective and scientifically knowable. Risk is subjective and socially constructed. Risk is a problem, a threat, a source of insecurity. Risk is a pleasure, a thrill, a source of profit and freedom. Risk is the means whereby we colonize and control the future. 'Risk society' is our late modern world spinning out of control.’ (Garland 2003, 49)

[11] This approach is of course in no way unique to NSM; it is aligned with the approaches of the likes of the National Protective Security Authority (NPSA) in the UK and other western agencies of the same kind. This also speaks to the policy mobility, mutations and imitation; a more detailed discussion of this phenomenon falls outside the scope of this report. https://www.npsa.gov.uk/

Much could be said about the evolution of the regulatory security state as a risk state (Levi-Faur 2023). But if we are to select one crucial shift in thinking about risk in Norway, it would be the progressive displacement of probabilistic thinking about risk by a national security understanding of risk management in terms of asset-threat-vulnerability (‘*verdi-trussel-sårbarhet’*, VTS) – a shift towards a precautionary logic of risk and the politics of possibility (Amoore 2013). While threat-assessment informed risk management can be traced both to the military and cybersecurity milieus, it was only after the terror attacks of 22nd July 2011 that this model began to spread, first as a counterterrorism measure and then eventually becoming a best practice approach to security management. Both the Security Act and standards such as the NS 5832:14 *Societal security – Protection against intentional undesirable actions – Requirements for security risk analysis* which are commonly used to operationalize the security compliance requirements under the Act, are founded on the principles of the asset-threat-vulnerability model. The threat-centricity of this approach decouples risk management to a large degree from considerations of probability. Instead, it starts by mapping assets to be protected, proceeding to a threat assessment and consequent identification of vulnerabilities – be these in personnel, or digital and physical infrastructures- based on which a risk assessment is then performed. Threat assessments, an integral part of this form of risk management, require an approach styled on intelligence analysis. This has led to a proliferation of practices that imitate the work of intelligence analysts, from the widespread use of OSINT to the writing up of internal organizational intelligence reports to support leaders’ decision-making. Large organizations, from banks and hospital trusts to the Norwegian Broadcasting Corporation (NRK), now publish their own annual threat assessments. Corporate intelligence functions, formerly reserved to large multinationals, have become increasingly common across different types of organizations (Sage-Passant 2023; Robson Morrow 2022; Petersen and Tjalve 2018; Petersen 2012, 2013). These threat assessments include anything from cybersecurity to the threat posed by insiders, i.e. employees and anyone else with legitimate access to the organization. If we zoom in on these threat assessments, we quickly see that they are concerned first and foremost with the threats to one’s organization well beyond ‘national security’ – as such, they include matters such as reputational damage, workplace violence and harassment or minor fraud. Where state authorities are concerned with espionage and sabotage, the organization is concerned with any behaviour it itself defines as threatening or counterproductive and as a threat to its continued operation. In NRK’s threat assessment from 2024,[12] we can for instance read of the high risk posed by climate activists and other activists, who can potentially disrupt programming.

On the one hand, minor issues are managed through frameworks designed for serious threats to national security. This raises not only questions of proportionality, but also of the larger effects of reducing national security to a matter of ‘good security management’. On the other hand, ideally, this approach allows one to manage threats that are highly unlikely, but that, if materialized, would have massive impact. But even here, this decoupling from probability is not unproblematic. While it may be reasonable to think in terms of threats in military or critical infrastructure organizations, it is questionable to what degree such thinking is appropriate for *any* organization. The decoupling of risk management from probability raises the questions of how proportionality and legitimacy are ensured and function-creep mitigated as we shift from probabilistic to threat-based risk models.

This regulatory set-up rests on five underlying notions which are rarely explicitly spelled out: 1) that national security interests and those of regulated entities coincide, or can be more or less unproblematically aligned, 2) that protection of any given organizations’ key assets serves

[12] NRKs trussel-vurdering 2024, p. 14, https://www.nrk.no/informasjon/pavirkning-gjennom-ki-og-aksjonisme-er-blant-nrks-storste-trusler-i-nrks-trusselvurdering-2024-1.16815159

national security, 3) that national security interests can be pursued by leveraging the internal organizational managerial structures to pre-empt security threats against these organizations, 4) that standards, technical, bureaucratic and managerial solutions are the best possible way to protect national security and 5) that national security is a sum total of each organization's security compliance. There is a reason to question the validity and soundness of these underlying assumptions. One reason being the commodification of regulatory compliance and its costs which automatically insert profit logics into the national security realm. Laws and regulations may have their explicit goals and intentions, but they are open to interpretation and translation. This is even more so the case for risk-based regulatory tools which delegate considerable discretionary power to the regulated entities. This is why we cannot stop at the level of legal and regulatory analysis, but, instead, need to turn to sociology and anthropology of law to understand the social dynamics of regulation and its effects in society. This means understanding who translates laws and regulations into concrete *practices* and with what effects.

1.1.2 Security Markets and the Privatization and Pluralization of Security and Intelligence

Organizational compliance is no longer a mere organizational duty. While the regulatory state delegates responsibility for compliance to the regulated entities, these entities are increasingly less frequently able to comply without seeking external help. A common complaint among regulated entities is that the state suffers of a regulatory fever, churning out complex regulations and vague open-ended guidelines, but that it is up to each entity to translate these and calibrate them to their organization while making sense of how any particular regulation, such as security, aligns with other regulations, such as labour law or anti-discrimination or GDPR. While the sector-driven state agencies, such as NSM, care only for the narrow area within their mandate, regulated entities must typically relate to several agencies and supervisory bodies at the same time. This is often described as creating confusion in terms of how to comply with multiple laws and public interest demands pointing in different directions at the same time, while keeping the costs of compliance as low as possible – or at best, making compliance work in the profit interest and thus making it pay for itself (be it in terms of reputation management, or reuse of compliance data). Delegation and responsibilization are at the very core of the regulatory state, including in the realm of (national) security. In response to these increasing regulatory demands and the regulatory crossfire, as well as actual risks in global markets and the expanding needs of regulated entities, the global markets in security, cybersecurity, and GRC (governance, risk, compliance) have witnessed remarkable growth.

The same trend can be witnessed in Norway, accelerated by evolving geopolitical uncertainty and the security situation. But it is difficult to estimate the market size of security compliance, as GRC is often separated from security markets (such as physical security, security equipment, security guards and protection, etc.). There are, to our knowledge, no reliable estimates that would capture the 'security compliance' dimension of the market where physical security intersects with security and compliance software, legal and consulting services, certifications, accreditations, background checks, screenings, KYC and other forms of due diligence. However, there is little doubt that the 'market for ontological security' (Krahmann 2018) and security compliance has been rapidly expanding over the past decades.

When we speak of the privatization of security, we often think of the commodification of security and policing, of private security firms such as Securitas or Avarn, of private military companies (PMCs), or the markets for various security gadgets and surveillance systems (Loader 1999). This privatization of security and security outsourcing is by now well-documented (Carmola 2010; Berndtsson 2012; Jäger and Kümmel 2007; Berndtsson and Kinsey 2016). Here we are more concerned with the privatization – and pluralization – of security and intelligence in response to

the regulatory security state (O'Reilly 2015; Ben Jaffel and Larsson 2022). By pluralization, we allude to the increasing security role of actors traditionally not understood as such, from consulting to the role of the regulated entities themselves (Bures and Carrapico 2018) and to the 'compliance-industrial complex' (Kuldova 2022): the various actors involved in compliance and the production of security, who not only translate regulation into practice, but who also to a large degree shape it through their epistemic and ideational power (Obendiek and Seidl 2023) and expert authority, who create the standards that become written into the law and who define what is a 'reasonable' level of security and how security is to be understood in the first place or balanced against other interests.

The 'regulatory security state' (Kruck and Weiss 2023b) and its efforts to align the population, organizations and businesses around the aims of national security while at the same time not hindering market competition and innovation, have thus led to the growth of new security markets and deeper and likely more hidden privatization of security and intelligence. As the regulatory security state seeks to leverage the internal managerial infrastructures of organizations for its own ends, it comes to depend on the security products and market actors who assist these organizations in compliance. This 'reflects the increasing dependence of state authorities on private actors in security provision – a power shift away from state actors' (Mügge 2023, 1432). These technical experts, lawyers and consultants translate and *de facto* shape regulation into concrete organizational practice, routines and rituals. Since security compliance is not the primary task or core function of organizations, it is often easier to (at least partially) *outsource* this function to various providers and experts on the market, further adding to the complexity of regulatory compliance supply chains. Indeed, powerful transnational market actors, such as professional service, audit and consultancy firms should be seen as powerful transnational private rule-makers in both a complementary and competitive relation to the state.

> 'Professional service firms such as audit and consultancy firms lobby for industry-driven governance in emerging regulatory domains. Similarly, third-party certifiers pressure public regulators to adopt measures which are nimble, auditable, and take the form of management-based standards as adopted by private rule-makers. Auditors pressure for measures which would benefit both the pro-vision of the services they offer, as well as the industry's preference for lighter private rules. As private regulators become part of regulatory arrangements, their direct and indirect influence expands even more. They also lobby proactively for further privatisation of regulation, including monitoring and certification, as well as for the creation of new, more complex and frequently amended rules—primarily to expand their markets and the related services they offer.' (Partiti et al. 2022, 459)

An immediate question arises: how do public interest and national security fit into the profit-oriented market dynamic?

The market for security compliance, which encompasses a broad range of specialized solutions, is populated by large multinational professional service corporations as well as boutique and more specialized firms. For some, security compliance is just a small part of their overall portfolio, for others, it is their core offering. In Norway alone, among these actors we can list the large audit and consulting firms, such as EY, KPMG, PwC, Deloitte, McKinsey, or outfits such as BDO, Sopra Steria, Tietoevry, Bouvet, Capgemini, Accenture, Atea, Norconsult, Multiconsult, Afry, Rambøll, or more specialized actors such as Mnemonic, Orange Cyberdefence, Safetec, Advansia, Proactima, Semac, InSilent, Agenda Risk, SeeMore and legal firms such as Schjødt, Wikborg Rein or Thommessen. The sheer number of actors and security products, software, consulting and legal services available speaks volumes about both the demand and the power – both economic and epistemic – of these market actors. These are the market actors behind the diffusion of security management practices across Norwegian organizations. These firms are also often staffed by former police, military, intelligence analysts, and other state functionaries, the

private sector offering an attractive career while drawing legitimacy for its services from the public sector expertise of its staff. To take an example, BDO markets its Security and Emergency Services in the following manner:

> 'BDO's security environment consists of almost 30 specialists with backgrounds from such organisations as NSM (the Norwegian National Security Authority), the Norwegian Intelligence Service, Norwegian Armed Forces, PST (the Norwegian Police Security Service), Økokrim (the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime) and the Norwegian Data Protection Authority.'[13]

Blurring the boundaries between public and private has indeed become normalized; hybrid actors proliferate (Petersen 2013); this goes also for the regulatory domain. These market actors are in many ways also trend-setters, norm and regulatory entrepreneurs in the areas of security, risk and threat management, always eager to not only develop new products, standards, governance frameworks, managerial and compliance strategies but also always ready to shape threat and risk narratives to create more demand for their services. This *commodification of regulation* is often neglected as we continue to imagine regulation as a matter of state governance. While we have become accustomed to the commodification of security and intelligence, the state even procuring private sector intelligence for its own intelligence services (Chesterman 2008; Berrefjord and Bjørstad 2025), we still lack a thorough understanding of what this *commodification* of security regulation, compliance and *de facto* provision of national security means. We can only speculate in relation to the long-term consequences of the commodification of compliance. However, the destiny of GDPR could serve us as a warning. Or as de Olazábal puts it in a recent article:

> 'The commodification of compliance, in this sense, turns regulatory adherence into performance, privileging procedural visibility over substantive accountability. Commodification manifests in two interconnected ways. First, it displaces responsibility from controllers to third-party providers that package compliance as a technical or administrative add-on. Second, it converts compliance into a competitive differentiator, valued less for its contribution to accountability than for its marketing potential. The result is a market in appearances: compliance becomes a signal of legitimacy rather than a demonstration of lawful practice. This theatrical logic sustains an 'illusion of order:' regulators, consultants, and controllers co-produce a sense of effective governance that depends on continuous performance rather than genuine restraint of harmful practices. This phenomenon mirrors broader dynamics in corporate sustainability and due diligence frameworks, where certification and reporting regimes frequently substitute for substantive accountability.' (De Olazábal 2026, 3)

While epistemic and regulatory capture by market and profit interests represents one key challenge for the regulatory security state, the illusions of compliance are another. There appears to be an increasing gap between compliance fictions and the realities on the ground – and the actual public interest and real security aims behind the regulatory efforts.

1.1.3 Challenges of the Regulatory Security State in the Current Security Environment

During the run-up to the Russian full-scale invasion of Ukraine on 24 February 2022, we could observe the regulatory security state in 'action'. Russian force posturing and sharp rhetoric, which had been going on for almost a year, were met with threats of 'crushing' sanctions – arguably a reaction typical of the regulatory security state. Observers who until the very last moment doubted the Russian intention to invade typically did so by pointing to the costs it would entail, mostly in terms of damaged reputation and sanctions leading to economic loss for Russia (Ullman 2022; Yilmaz 2022). As became clear later that year, this mode of thought was shared by Russian

[13] Security and Emergency Services, BDO Norway: https://www.bdo.no/en-gb/services/consulting/security-and-emergency-services

insiders of a market-oriented leaning (so-called 'systemic liberals', or, increasingly correctly, technocrats), who in January 2022 indeed had warned President Putin of those very consequences if he would exacerbate tensions with Ukraine (Seddon and Ivanova 2022). More broadly, this is symptomatic of the proponents of the (neo-)liberal or 'rules-based' world order, with law- (and regulation-)abiding entities engaging in economic exchange to maximize profits – and everybody allegedly getting richer as a result. The former free-market advocate Putin was entirely uninterested, immersed as he now was in geopolitics and (pseudo-)history. The almost pathological shock experienced by these technocrats when he brushed them off testifies to their (perceived) epistemic authority, which was swiftly shown to be ill-founded.

Although US and UK intelligence had expressed near certainty that an invasion was imminent in the preceding weeks, the Russian move came as a shock in the West as well, bringing a rude awakening to the hibernating (Genschel and Jachtenfuchs 2023) positive security state. Famously and emblematically, within days, then German Chancellor Olaf Scholz reversed the country's post-World War II cautious defence policy and the peace-through-trade approach to Russia, announcing a EUR 100 billion increase in military spending. Since then, European defence spending has soared, with Norway passing the 2 per cent of GDP mark as regards defence spending in 2024 and planning to surpass 3 per cent within ten years. Military support to Ukraine from European nations has increased in volume and lethality, from helmets and sleeping bags to tanks, fighter jets, and long-range precision strike missiles.

The regulatory security state emerged in the context of the end of the Cold War and the following unusually peaceful period, when the geopolitical challenges were comparatively few and weak. Immediate threats to territorial integrity and survival receded into the background, but 'new' security concerns were identified, or, rather, the concept of security came to encompass a wider range of issues. Less acute and life-threatening risks were thought to be efficiently managed using a regulatory logic (Genschel and Jachtenfuchs 2023). The peacetime, perhaps even Fukuyaman (Fukuyama 1992) hallmarks of the regulatory security state are clear: '[…] networks of decision makers, experts, polycentric institutional designs, indirect accountability, and governance by proxies and intermediaries' (Levi-Faur 2023, 1462). It is about trade, win-win, profit, and efficient management.

With the return of geopolitics, the regulatory security state has not gone anywhere. On the contrary, it has blossomed. Regardless of its profoundly 'peaceful' roots, the regulatory security state was already awake on 24 February 2022 and went into action immediately. We can argue that it followed the logic established in its formative phase (Kruck and Weiss 2023b; Sivan-Sevilla 2023). Hence, the geopolitical challenge – the return of large-scale interstate war to the European continent – missile attacks, drone swarms, advancing tanks and infantry – was met with frantic regulation. The sanctions regime is a telling example. Economic sanctions are of course a tool as old as the international trade itself, but the present sanctions regime carries the unmistakable hallmarks of the regulatory state. As of the time of writing (April 2026), there are 26,655 specific sanctions,[14] making Russia the most sanctioned country in history, or more correctly, the most complicatedly sanctioned country (Østbø 2024). The EU, for instance, maintains a list of Russian citizens who are subject to restrictive measures, containing, as of April 2026, 2,031 persons.[15] By contrast, in 1990, Iraq was sanctioned by immediately freezing all foreign assets and a complete and militarily enforced oil boycott (van Bergeijk 2022). It is of course exceedingly hard for companies to keep track of all the sanctions against Russia, which helps explain why the compliance industry is experiencing a boom, as is the closely related defiance industry. Although

[14] https://www.castellum.ai/russia-sanctions-dashboard
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32026R0613

the threat of sanctions was initially presented as a means to deter Russia from invading[16], the sanctions regime, including export control, has become a 'natural' part of security policy. The EU regulatory security state has also responded to the Ukraine war by launching several regulatory initiatives to stimulate increased defence production (Hellemeier 2025) and in cyber security, where strategic autonomy takes precedence over globalization and internationalized trade (Farrand et al. 2024).

In short, although the RSS grew out of a context that was very different from the present one and has continued to act according to the pattern established in its formative period of globalization and relative peace, it has taken on a new and even expanded role. Earlier, it dealt with 'soft' security threats and operated under the main banner of globalized trade, but now, it inserts itself into rather hard, military affairs, where the positive security state is re-energized on the national level. European nation states increase military spending, expand compulsory military service, and build military capacities, but this happens in symbiosis with the regulatory state, embodied by the EU. Private actors, many of which are multinationals, are also part of this complex relationship. Ideally, the RSS should play a supporting role to the PSS (Schilde 2023). But the regulatory logic carries the risk of a virtualization of security and excessive focus on the regulations themselves, at the expense of the physical reality; put otherwise, it risks mistaking the map for the terrain (Kuldova and Østbø 2026).

Regardless of the ongoing securitization, the RSS is a peacetime phenomenon. We are not directly engaged in the war in Ukraine, and if war arrives, the awakening will likely be much harder than that of 24 February 2022. While Russia is by no means a model to be emulated in any way – politically, administratively, militarily, or otherwise – it can be worth pausing for a moment, if only to see what we are up against. The Russian economy is on a war footing. The defence industry is working around the clock to meet the state's demand. Export and import are rerouted to 'friendly' or 'neutral' partners. Businesspeople, who some hoped would rebel against the regime when they felt the pain of the sanctions, have been repatriated and domesticated to toe the Kremlin line, also via direct monetary contributions to the military. The Russian technocrats mentioned earlier, who initially opposed the war (and perhaps still do, on a strictly personal level) in practice rapidly turned into the war machine's indispensable supporters, as their bold macroeconomic moves and efficient management saved the economy and society from a breakdown (Seddon and Ivanova 2022). The Russian regime's willingness to break the rules, creatively defy and even revel in the sanctions, to squander resources, including the lives of its own soldiers, not to mention enemy combatants and civilians, all in the service of a 'higher' goal, should suffice to question the very essence of the regulatory logic.

1.1.4 Challenges of the Regulatory Security State in the Technological Environment

The technological environment sharpens several core contradictions of the regulatory security state. The regulatory security state relies on Big Tech and digital companies, both for the digital infrastructure and cybersecurity but also for regulatory compliance (so called RegTech or regulatory technologies). In other words, contemporary security governance increasingly relies on digital solutions, expert authority and delegated implementation to secure national interests in a risk environment marked by cyber threats, geopolitical volatility and deep societal interdependence. Yet the same technological developments that make such governance appear necessary also make it harder to render effective. In Norway, the Security Act is presented as a central instrument for safeguarding national security, but official policy also recognises that critical assets are increasingly complex and that they change rapidly over time (Meld. St. 9 (2022–2023)

[16] Secretary Antony J. Blinken With Dana Bash of CNN State of the Union, US Department of State, https://2021-2025.state.gov/secretary-antony-j-blinken-with-dana-bash-of-cnn-state-of-the-union-2/

2022). This creates a central problem for the regulatory security state: legal and compliance architectures seek to stabilise and classify a technological environment that is structurally dynamic, opaque, and difficult to bound (Bellanova and De Goede 2022b; Yeung and Lodge 2019). This typically further exaggerates the dependence on external expertise discussed above. The NSM, to take an example, has its own vendor certification and quality schemes to designate quality suppliers in the digital market;[17] hence, managing the complexity through its own due diligence practices and determining who in the market can be *de facto* trusted; these of course require periodic updating and continuous vigilance.

A first challenge thus concerns the epistemics of algorithmic security. As security governance becomes increasingly datafied and technologically mediated, it depends more heavily on the integrity of the data, classifications, and models through which threats are rendered knowable. This is especially significant for AI-enabled compliance systems, as where data is flawed, error can be scaled rather than corrected. In such settings, AI systems correlate, infer, and prioritise in ways that actively participate in *producing* what counts as suspicious, actionable, or dangerous behaviour (Amoore and Piotukh 2015; Amoore and Goede 2008). The consequences of algorithmic classification in security settings are therefore political as well as technical: they shape intervention in ways that may appear objective while embedding specific assumptions about uncertainty, normality, and threat (Amoore and Piotukh 2015; Mittelstadt et al. 2016). This translates into the ideational power and epistemic authority of tech companies (Obendiek and Seidl 2023), who have disproportionate say in how threats and risks are conceived and to be managed through algorithmic architectures in the first place.

A second challenge concerns the limits of transparency and explainability. In current regulatory debates, transparency and explainability are often treated as solutions to the opacity of algorithmic systems. However, greater visibility into a model does not necessarily make a complex socio-technical system intelligible, contestable, or governable in practice (Obar 2020). Explanations may be partial, post hoc, or narrowly technical, while leaving untouched the deeper assumptions embedded in training data (Burrell 2016). In security governance, this creates a risk that systems become formally explainable while remaining substantively difficult to scrutinise or challenge. Transparency can therefore improve procedural visibility without resolving the deeper question of whether a system is epistemically reliable or institutionally accountable (Ananny and Crawford 2018; Veale and Brass 2019). In the regulatory security context, this is particularly significant because the appearance of explainability may itself help legitimate systems whose broader effects pose potential harm.

A third challenge is temporal. Technological systems evolve quickly, while the law and compliance regimes tend to evolve slowly. This produces a structural lag between the tempo of technical change and the tempo of regulatory adaptation. Under such conditions, compliance risks becoming oriented toward auditability rather than long-term resilience or infrastructural redesign. More broadly, attempts to govern uncertain futures through risk management and anticipatory intervention can generate security practices that promise readiness while struggling to engage substantively with emergent and systemic forms of vulnerability (Aradau and Blanke 2015, 2018, 2017). The drivers between the gap between compliance maps and the territory discussed above are thus also technological.

A fourth challenge is political and institutional. The technological environment strengthens the role of private firms not only as suppliers of infrastructure but also as producers of standards, classifications, and security knowledge. As a result, public authorities may retain formal legal

[17] Kvalitetsordning for leverandører som håndterer IKT-hendelser, NSM: https://nsm.no/fagomrader/sikkerhetsstyring/leverandorforhold/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser

responsibility while becoming increasingly dependent on vendors for the practical means of governing insecurity. This matters because corporate actors shape how security problems are framed, what counts as risk, and which solutions become thinkable and actionable. In practice, the expansion of digital security markets can therefore deepen the privatisation of epistemic authority and narrow public control over the infrastructures through which security is governed (Bellanova and De Goede 2022b; Pasquale 2015).

Taken together, these dynamics suggest that the challenge is not simply how to regulate more technology. It is how to prevent technology-centred regulation from displacing preparedness, democratic accountability, and meaningful public control over the infrastructures and knowledge systems on which national security increasingly depends.

1.1.5 The Regulatory Security State and the Rule of Law

In a state governed by the rule of law, everyone – individuals and state powers (i.e. executive, legislative and judicial) alike – is subject to and protected by the law. Put simply, no one is above the law and everyone is protected from the exercise of arbitrary power. An important aspect of the rule of law is the principle of legal certainty, i.e. the law must be clear and foreseeable such that persons are able to find out what their rights and obligations are, allowing them to act accordingly.[18] In case C-588/21 P,[19] the Court of Justice of the EU (CJEU) held that free access (i.e. without charge) to EU law is a rule of law requirement (para. 81) that 'is inextricably linked to the principle of openness' (para. 83 and 84). This principle, according to the CJEU in case C-588/21 P, also applies to harmonized standards adopted on the basis of an EU directive or regulation and the references to which have been published in the EU's *Official Journal*. Although the development of harmonized standards is entrusted to a body governed by private law, only the European Commission is empowered to request that a harmonised standard be developed in order to implement a directive or a regulation. Though compliance with harmonised standards is not compulsory, products which comply with those standards benefit from a presumption of conformity with the essential requirements relating to them laid down in the relevant EU harmonisation legislation, c.f. Article 2(1) and recital 5 of Regulation No 1025/2012.[20] As the CJEU explained, 'by the effects conferred on it by EU legislation, a harmonised standard may specify the rights conferred on individuals as well as their obligations and those specifications may be necessary for them to verify whether a given product or service actually complies with the requirements of such legislation' (para. 82). However, access to a document may be refused where its disclosure would undermine the protection of commercial interests of a natural or legal person, including intellectual property, unless there is an overriding public interest in disclosure. The CJEU concluded that there is an overriding public interest that justified the disclosure of (i.e. free access to) such harmonized standards.[21]

Thus, when it comes to the use of harmonized standards that are granted legal effect in EU law as discussed above, the CJEU has recognized a right of free access (i.e. without charge) to such standards. There is no analogous recognition by the CJEU of a right of free access to other standards that are not harmonized standards, e.g. those developed by national standardisation bodies. If a presumption of conformity develops with respect to such other standards, or the use

[18] See case C-160/20, judgment of 22 February 2022, Stichting Rookpreventie Jeugd and Others, EU:C:2022:101, paragraph 41 and the case-law cited, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020CJ0160. See also https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/what-rule-law_en

[19] See judgment of 5 March 2024, Public.Resource.Org and Right to Know, ECLI:EU:C:2024:201, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62021CJ0588

[20] See para. 74 of the judgment in Case C-588/21 P.

[21] See para. 85 of the judgment in Case C-588/21 P.

of such standards is in practice required by the relevant supervisory authority, the question arises whether the rule of law principle of legal certainty requires the grant of free access to any such standard.

1.2 Regulatory Security State in a Future Context

So far, we have outlined some of the key features of the regulatory security state (RSS), the compliance, security and tech markets which it has generated and on which it has come to depend in the process, and the key challenges it faces in the current technological, legal, and geopolitical environment. In this section, we present key results from the first round (of two) of the expert survey inspired by the Delphi method and adapted for our purposes of 1) investigating the futures of RSS and 2) exploring its functioning in practice by zooming in on the case of insider risk management (see section 2.). Our aim has been to gather and reflect expert judgments on key dilemmas related to security compliance in contemporary regulatory and geopolitical contexts as we look ahead. The purpose has not been to reach a forced consensus, but to map areas of agreement, disagreement, and uncertainty, and to better understand how experts reason about risk, security, and the future and the role of the RSS ahead. We also attempted to place the RSS into a future context to help us build a contextual future-oriented understanding. In particular, we were interested in identifying any omissions in our own reasoning – what contexts have we ignored, what contexts should be considered? Existing literature on the RSS tends to still be rather narrow and specialized, and hence we wanted to zoom out a bit and place the RSS in a bigger picture and get a new perspective its role in the security futures.

One immediate puzzle that emerges from both the literature reviewed, our own research and further reinforced by the expert judgements presented below, is the widespread consensus about the failures and structural weaknesses of the regulatory security state. Even more puzzling, despite this consensus about the failures and weaknesses, is that it appears extremely difficult to imagine better alternatives and positive futures of security governance. While dystopian futures are easy to imagine, there appears to be a certain resignation and passive acceptance of these systems despite their dysfunctionalities and inability to deliver on the desired goals. This lack of imagination and faith in the possibility of change and agency is particularly troubling in the case of national security.

1.2.1 Expert Future Perspectives – A Note on Delphi-inspired Method

As mentioned above, the surveys used to collect expert opinions for this report were inspired by the Delphi method. This is classified as a ‘consensus method’ or a group facilitation technique ‘(…) designed to explore the level of consensus among a group of experts by synthesizing and clarifying expert opinion’ (Campbell and Cantrill 2001, 5). Although the name ‘Delphi’ traces its roots all the way back to the oracle of Delphi, where the ancient Greeks were said to receive forecasts about the future (Cantrill et al. 1996), the Delphi method originated in the US in the middle of the 20th century (Dalkey and Helmer 1963). In a study by the name of ‘project Delphi’, the RAND Corporation developed the method to obtain a reliable expert consensus with the aim of more accurately estimating key Soviet nuclear targets in the US (Campbell and Cantrill 2001). Since then, however, the method has been used not only in military contexts but also by academics in various disciplines including, but not limited to, resource management, medical education, business, and social policy (Humphrey-Murto and De Wit 2019).

The Delphi method is structured by administering multiple rounds of anonymous surveys to experts (Campbell and Cantrill 2001). Usually, the method comprises two or three rounds. The

respondents should be provided with adequate background information (Humphrey-Murto and De Wit 2019). In addition, the results from each round (e.g. factors considered relevant by other respondents) are analysed and fed back to the experts before they answer more questions in the following round (Campbell and Cantrill 2001; Dalkey and Helmer 1963). There are several strengths associated with this iterative data-collection process. Notably, the method allows the experts to gradually form a more considered opinion, both because they receive feedback throughout the process (Campbell and Cantrill 2001) and because they are shielded from potential social and psychological effects associated with confronting other experts face to face (Dalkey and Helmer 1963; Landeta 2006). Additionally, since the experts do not meet face to face, researchers can use the method to collect expert opinions from geographically dispersed locations (Campbell and Cantrill 2001). In this study, seven of the twenty-one experts who answered the first round of surveys were not Norwegian. Although they were familiar with the Norwegian context, they could also provide valuable insights from other countries and cultures.

The Delphi exercise undertaken to gather expert opinions for this report was comprised of two rounds, which will be described in more detail in the following sections. The figures below provide information about the professional backgrounds of the twenty-one experts that responded to the first survey round. Note, however, that several experts answered that they held more than one professional role. Although some experts from the private sector and consulting were included in the sample, the majority had their background from the public sector or research. In a free-text question asking for specification about the respondents' primary expertise, several researchers provided information about which academic discipline they belonged to. These were, for example, criminology, history, anthropology, sociology, law, political science, international relations, and security studies with research interests focused on such as bureaucracy, audit, sustainability, democracy, defence, security, intelligence and compliance. All experts have had prior knowledge of the research project, can be considered subject-matter experts, having an understanding of both regulation and security, albeit from different disciplinary perspectives, and have been recruited through the networks of the project researchers based on the relevance of their expertise.

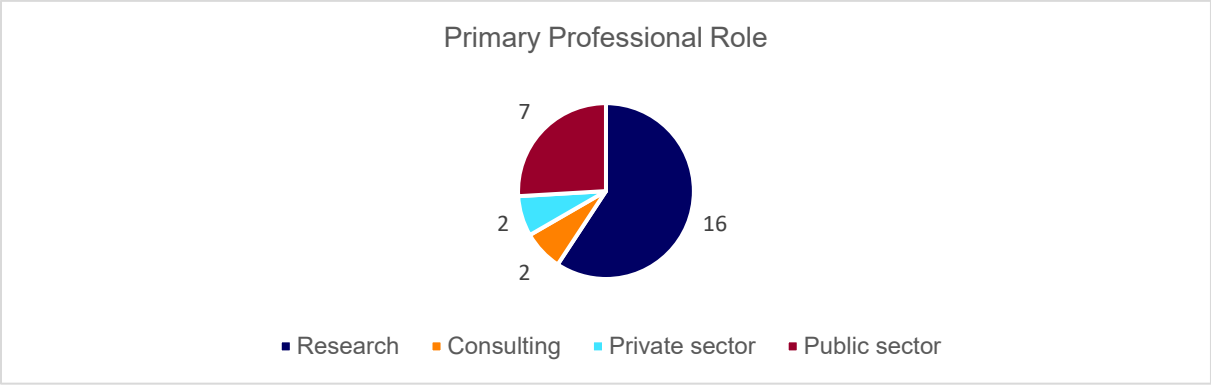

Figure 1-1. Respondents' professional role(s).

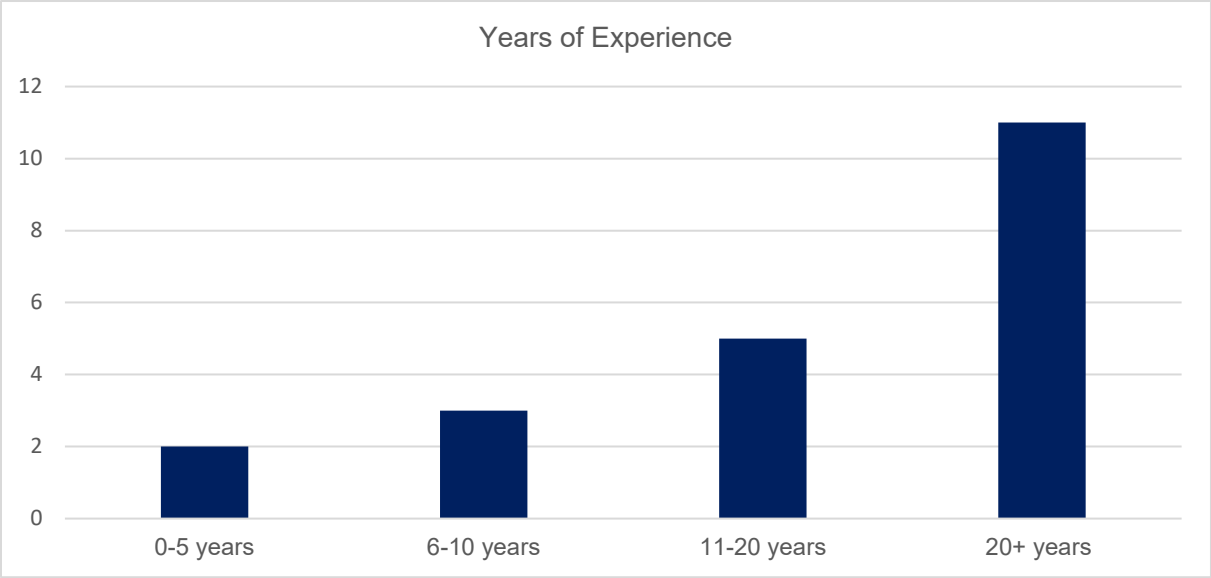

Figure 1-2. Years of experience.

Moreover, the Delphi method has been described as a 'flexible' method that can be modified in several ways (Campbell and Cantrill 2001). First, it can be used to generate both quantitative and qualitative data. In both rounds of surveys in this study, the experts were asked to evaluate statements along different scales (e.g. level of agreement, risk, desirability, likelihood, thinkability), producing quantitative, albeit small-scale, data. However, they were also repeatedly asked to generate qualitative reflections by explaining their reasoning and adding factors or drivers of change that are often unrecognised, ignored or not discussed. This speaks to how the Delphi method can be used not only to ask respondents to evaluate pre-crafted statements based on literature and research results identified by the researchers conducting the survey, but also to generate new ideas, uncover omissions and understand reasoning behind expert assessments (Campbell and Cantrill 2001). The importance of expert imagination was additionally highlighted in the introduction to the first survey:

> '(…) the current geopolitical situation is exposing the inherent limitations of RSS. The goal of our Delphi exercise is to probe deeper into the possible futures – short and long-term – of this form of security governance. One of our aims is also to map a broad range of relevant factors that (could) influence the functioning of the RSS. Our goal is to uncover the underlying assumptions, path dependencies and 'epistemic authority' and lock-in in security regulation, governance and management which have emerged during the period of deep peace. We ask you to think through the following series of statements and dilemmas using your experience, expertise and imagination.' (excerpt from the introduction to the first round of the survey)

It should be noted that emphasizing the identification of a broad range of factors (rather than a narrow consensus) and encouraging imagination was a conscious decision. As previously mentioned, the Delphi method is considered a consensus method. One implication of this is that it is arguably skewed towards analysing the consensus points in the data, often to the point of neglecting to push towards discrepancies or alternatives (Ahlqvist and Rhisiart 2015). One reason for this is that the method is often used in fast-paced assessment exercises where the utilitarian dimension of futures studies takes precedence over its potential emancipatory dimension (Ahlqvist and Rhisiart 2015). The fact that consensus methods can also be useful for identifying and measuring areas of controversy or uncertainty (Campbell and Cantrill 2001) is in other words easily overlooked. In this survey, we also attempted to look ahead, into an uncertain future, and tease out dynamics likely to shape it. According to Ahlqvist and Rhisiart, this bias towards

consensus has both ethical and practical consequences and should therefore be rectified by introducing more critical perspectives into futures studies as a whole:

> 'Criticality can support the generation of alternative frames – and awareness of 'otherness' that are theoretically enriching whilst supporting practical learning for individuals and organisations. (…) Within policy-related work, there may have been a tendency to view foresight as the domain of technical experts unconnected to the political stream. Futures studies – when deployed in policy and other contexts – should introduce critical perspectives (or at least be increasingly mindful of them). In this sense, it should be seen as part of the re-politicisation of (technocratic) policy-making, enabling meaningful critique, encouraging contestability, and revealing assumptions and power interests.' (Ahlqvist and Rhisiart 2015, 103)

This dimension of criticality and re-politicization gains an added layer of importance in the case of our project which targets a subject – the RSS and insider risk management – which can be considered an example of technocratic modes of governance. An important challenge for us is how to transgress technocratic and legalistic modes of reasoning when studying and trying to understand the RSS: how to identify the 'blind spots' in this approach to security governance and challenge the epistemic closure of the RSS and this mode of security thinking. And hence, how to open up possibilities for thinking security governance more productively, given the widespread agreement about the weaknesses of current regulatory approaches.

One way in which this Delphi-inspired exercise sought to be mindful of critical perspectives and encourage contestability, was to explicitly inform the respondents in both rounds of the survey that the purpose was '(…) not to reach a forced consensus, but to map areas of agreement, disagreement, and uncertainty, and to better understand how experts reason about risk, security, and the future' (excerpt from the introduction to round 1 of the survey). Despite this, however, the answers from the first round identified several points where there was indeed a high level of convergence and consensus in the experts' opinions.

1.2.2 Challenges and Expert Consensus Insights about RSS

Before delving into the experts' opinions on the RSS, it should be noted that, as mentioned earlier, a component of the Delphi method is that the experts should receive relevant background information before they answer the questions in the survey. According to Humphrey-Murto and De Wit (2019), this is an important, yet often neglected dimension. Before the experts in this study were asked to answer questions in the first round, they were provided with information about and theoretical background pertaining to the Norwegian RSS.

Although the opinions of the experts in no case converged entirely on the scale, there were several instances where the level of agreement was near total. For instance, a majority of the experts disagreed or strongly disagreed with the notion that there are *no* conflicts of interest between the national security state interests (public interest) and the goals of organisations (see Figure 1.3.). To the contrary, they viewed conflicts of interest between the national security state and organisations as important, and yet often neglected or disavowed. As one expert elaborated in the free-text section of round 1 of the survey[22] on this matter:

> 'The positive security state is national - i.e. its core/heart is founded on the state's interest. The RSS, especially the private sector actors, are not national (may be foreign-owned or have some foreign shareholders or the composition of the board may be eclectic), driven by profit maximization as the primary motive i.e. not national security as the primary aim (as it is for the positive security state).'

[22] All quotes in this section are from free-text part of the form in Round 1.

However, even if the experts broadly agreed that there are relevant conflicts of interest between the state and the private sector organizations, there were instances where some experts pointed out that the state and regulated entities may also have aligned interests, given that organisations depend on political and economic stability. These, however, cannot be understood as a default position of alignment. Even when this shared need for stability was considered, however, one expert noted that this does not automatically imply a shared definition of either risk or security:

> ‘States typically evaluate security in terms of systemic stability and long-term strategic risks, whereas organisations often evaluate risks in terms of operational continuity, financial exposure, and legal liability. These different rationalities can create divergence even where interests broadly align, and this divergence shapes how compliance measures are implemented in practice.’

The focus on organizations’ core assets, as the crux of what is to be secured in the asset-threat-vulnerability risk model, further feeds into to the potential conflict of interest between national and organizational security. This was also remarked upon by the experts, such as in the following statement:

> ‘Defining security around “core assets” at the organisational level can mis-specify what is at stake nationally, such as societal trust or continuity of essential services. These are relational and systemic goods that cannot be secured through internal managerial controls alone.’

In other words, the inward-looking asset-oriented focus of security management, a core feature of security compliance, is seen as preventing us from effectively conceptualizing and thus also addressing systemic security threats. Moreover, it can lend itself to mission-creep as protection of core assets is not necessarily considered in light of national security interests but rather organizational interests and thus becomes detached from national security, while potentially serving other goals.

Furthermore, beyond organisational interests shaping how compliance measures are implemented, there was quite broad agreement among the experts that the state’s regulatory power is adversely affected because corporate actors and technical experts write the rules, leading to a different, more structural form of mission creep and ultimately to the depoliticization of the debate around national security (see Figures 1.3. and 1.4.). One expert for instance highlighted that delegating security authority to experts can mean removing focus from key factors that are important to achieve national security but which, crucially, cannot be secured through compliance:

> ‘I strongly disagree that imposing compliance obligations is an effective way to protect organisations from threats. Compliance regimes tend to prioritise procedural conformity and auditability rather than substantive resilience. (...) Security threats, particularly in the current geopolitical context, are structural and relational rather than primarily organisational. They emerge from interstate tensions, economic dependencies, supply chains, and strategic positioning, none of which can be meaningfully mitigated through internal compliance architectures alone.’

> ‘(…) I strongly agree that delegating authority to experts and organisations removes security from political debate and reframes it as a technical problem. This technocratisation can obscure the fundamentally political nature of national security, including decisions about alliances, foreign policy alignment, industrial capacity, and economic strategy. When security is reframed as a matter of compliance with standards and risk management frameworks, it risks depoliticizing decisions that are in fact geopolitical and strategic. The current international environment demonstrates that national security is heavily shaped by the actions of major powers and alliance dynamics, often beyond the control of individual organisations or regulatory frameworks.’

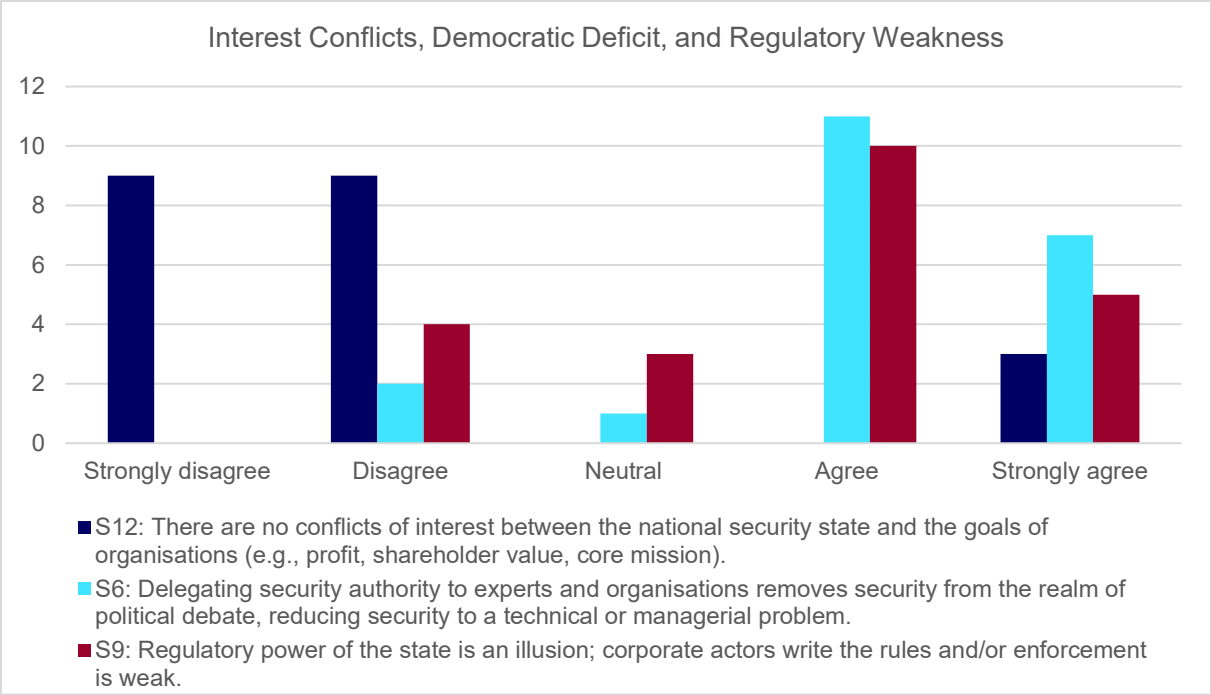

Figure 1-3. Consensus on key challenges related to the regulatory security state.

The expert statements, as well as the answers in the form itself, thus reproduced some of the critiques raised against RSS in the academic literature, discussed in the introduction. In particular, concerns about democratic deficits and depoliticization were prevalent and the perception of (national) security as a mere technical and managerial problem was itself seen as a considerable risk by the experts and potentially counterproductive in that it may reinforce the already existing democratic deficit. Or as an expert put it:

> 'I view the continued delegation of authority to consultants, technical experts, and corporate actors as both highly likely and strongly undesirable. Delegation is often justified on the basis of specialised knowledge and efficiency, but it also redistributes power toward actors who are not directly democratically accountable. This dynamic can narrow the policy imagination by privileging technical or managerial solutions over political or strategic approaches. It may also reinforce path dependencies where expanding compliance infrastructures generate demand for further delegation rather than improving substantive security outcomes.'

Another expert echoing these sentiments, links this to the very loss of state sovereignty:

> 'By delegating power to private organisations (alone or jointly with public organisations) to develop AND enforce standards on matters of national security or critical infrastructure (e.g. through so-called audit checks carried out by the same private entities against payment), the state is abdicating its power/sovereignty.'

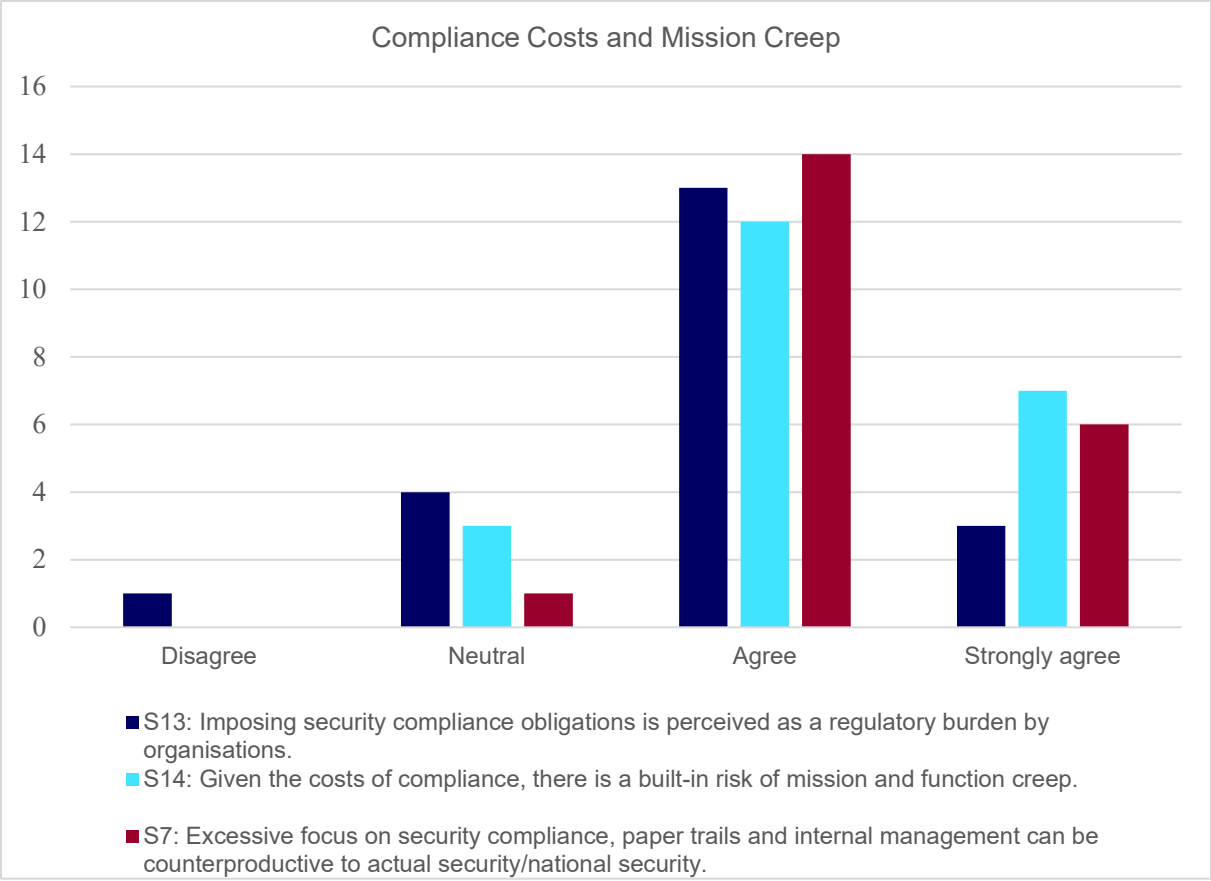

Figure 1-4. Expert consensus on the costs of compliance and its negative consequences for outcomes.

As previously mentioned, a central goal of the Delphi-inspired exercise undertaken in this study was to identify and highlight factors which are relevant to the RSS, but which are often ignored or overlooked. The expert opinion cited above demonstrates an understanding of numerous ways in which the RSS, by relying on certain forms of technocratic epistemic authority (Obendiek and Seidl 2023; Kuldova 2022), can obscure and thus ultimately fail to contend with the threat of 'weaponized interdependence' (Fishman 2025; Farrell and Newman 2019) in the modern world. In other words, there is a concern that this approach is not well-suited to the current challenges. Moreover, the cost of compliance and the widespread understanding of compliance as a 'burden' on organizations has been linked to concerns about unintended consequences and mission and function creep as organizations try to turn this burden into profit and leverage in the market; this, as we shall see in chapter 2 is of particular relevance to the insider risk programmes. One expert for instance remarked upon how the:

> 'Expanding regulations and standards can increase organisational complexity and administrative burden without necessarily improving outcomes. Overly complex compliance environments may divert attention and resources away from practical risk mitigation activities, creating diminishing returns from additional regulatory detail.'

The concern that 'more' regulation and 'more' compliance do not necessarily result in better security outcomes runs as a continuous thread through the material. This relates also to questions of enforcement (or lack thereof), as well as virtualization of compliance – or else, the gap between realities on the ground (terrain) and compliance fictions (map) (see Figure 1.5.). The continuous expansion of regulation can thus rather be seen as a sign of regulatory weakness,

rather than strength. The expansion of compliance regimes has been also linked to organizational path-dependency, rather than their effectiveness, containing also an element of ritualization:

> 'Once compliance systems are established, they create institutional investments, professional specialisation, and organisational routines that are difficult to reverse. This can result in regulatory persistence even when effectiveness is uncertain. Compliance frameworks may therefore continue to expand due to institutional momentum rather than demonstrable security benefits.'

Compliance has also been discussed by the experts in terms of generating blind spots and thus as paradoxically concealing by disclosing. Moreover, as one expert noted, measurements can skew results:

> 'Compliance regimes frequently reward what is legible to auditors (policies, KPIs) rather than what is revealed under stress (trained people, exercised coordination). This can generate a performative assurance cycle that looks like control while leaving core vulnerabilities and interdependencies insufficiently addressed.'

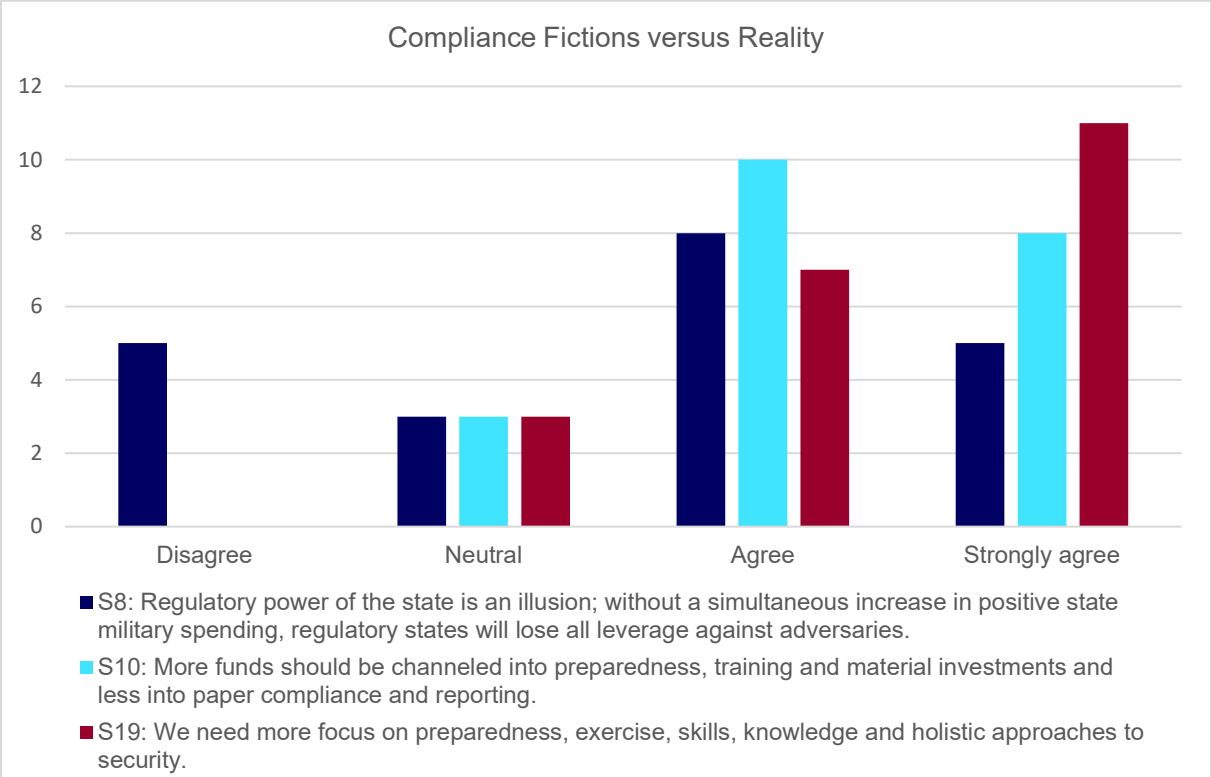

Figure 1-5. Expert consensus on regulatory illusions vs. reality.

However, it is important to highlight that although there was a certain level of disagreement among the experts on whether the regulatory power of the state is a complete 'illusion', there was widespread agreement that there is a need for more *holistic* and *materially grounded* approaches to security, even if this would mean diverting funds away from paper compliance and channelling these into new forms of real and material preparedness (see Figure 1.5.). There was, however, also a dissenting voice arguing that a holistic approach to security could be seen as paternalistic.

As one of the experts noted, the current functioning of the RSS leaves society vulnerable both to traditional and hybrid threats: 'It is utterly naive to assume that a military invasion or hybrid attack

can be deterred or repelled with papers, regulations, and standards.' This echoes the earlier discussion on 'ontological security' and the hypothesis that security compliance delivers more in terms of ontological and less in terms of real security, which also aligns with research on the growth of the security industry as serving ontological security (Krahmann 2018). This reasoning is echoed also in the following expert statement:

> 'An often-overlooked issue is the psychological and political value of security governance frameworks. Expanding technical systems, standards, and compliance mechanisms can create reassurance among policymakers and the public that risks are being managed effectively, even when underlying vulnerabilities remain. This distinction between perceived control and material resilience is important because it may shape policy choices independently of measurable effectiveness.'

In summary, there was a consensus among the experts that an excessive focus on regulations and compliance, neglecting the material and relational factors that impact national security, can be detrimental to both national and organizational security, while potentially undermining societal preparedness – no less as resources flow into compliance. The juxtaposition of compliance fictions with material realities and global interdependence also meant that experts largely agreed that national security cannot be understood separately from preparedness. While this insight may seem intuitive, in practice this would mean a fundamental rethinking of the national security compliance frameworks and their integration (and thus also transformation) with preparedness frameworks and a more serious refocusing on material conditions on the ground.

> 'Preparedness is the binding constraint in crises: capabilities depend on practiced routines and cross-sector coordination (e.g. multi-agency exercises) that cannot be improvised from documentation. A more holistic approach also recognises that security failures propagate through systems and dependencies, so resilience must be built collectively and exercised realistically.'

More meaningful compliance would also require stronger enforcement and the ability of the supervisory bodies to more extensively contrast the compliance maps with the actual terrain. However, increasing enforcement capabilities alone, as the above suggests, would not be sufficient given both the epistemic limitations of the approaches and external and systemic pressures on the RSS. Some drivers of regulatory weakness in the RSS that were discussed in this section were conflicts of interest, delegation of authority to technical experts and ignoring important geopolitical constraints and dependencies. These, however, do not constitute an exhaustive list of factors identified in the material, more of which will be discussed in the following section.

1.2.3 Drivers Behind Regulatory Weakness in Security Compliance

Given the high level of consensus in the first round of the survey regarding the RSS' inherent weaknesses, the first section of the second round of the survey was designed to identify and further explore the experts' thoughts about the biggest drivers behind regulatory weakness today and in the near future (2035).

Before discussing these, a brief digression into the background for the second round of the survey needs to be made. First, in line with the requirements and purpose of the Delphi method discussed above (1.2.1), the experts were provided with a summary of the results of round one – both the areas of agreement and disagreement – before they were asked to evaluate statement batteries and complement these with their reflections. Second, while the first round of the survey obtained twenty-one responses, the number of respondents dropped to sixteen in the second round, making the level of retention 76,2 %. One reason for the drop may be that the second

round focused, in addition to reflecting on the responses in the first round, on the even more specialized subject of insider risk management (as discussed in more detail in section 2.). While some experts reported high confidence in answering our questions on insider risk, others claimed lack of deep knowledge. The challenge regarding attrition could be ascribed to a significant degree to the necessary level of specialization required to confidently answer these questions. While general questions on the regulatory security state were within the experts' domain, the more specialized questions on insider risk were by some seen as beyond their particular expertise. This being said, for some the 'insider risk' perspective was *closer* to their immediate expertise; in this sense, non-attrition did not, in our view, necessarily impact the quality, to the contrary, those with most specialized expertise were retained. Two participants also reported lack of time and the extensive nature of the survey (response time varied between 25–120 minutes for each round depending on how much free text the experts decided to write). While there are no standard guidelines for Delphi, sixteen is still a common number of experts for a Delphi method, where anything from seven to fifteen and fifteen to thirty respondents is common; the retention rate remains within acceptable limits as well, given that 'a dropout rate of 20–30 % can be expected between rounds' (Chalmers and Armour 2019, 731). We are still confident that this serves our purposes of using Delphi as a form of expert-driven 'social diagnosis' in a complex and rapidly evolving social environment (Landeta 2006, 479), offering a perspective on larger drivers that are often left out of more narrow regulatory and disciplinary discussions.

Let us now return to the question of identifying further drivers of regulatory weakness. In the first question of the second round, the experts were asked to select the most important causes/drivers behind the regulatory weakness in security compliance. They were provided with a list of sixteen options identified in previous research as well as round 1 of the survey and could choose multiple responses. In addition, they could add their own or express disagreement with the premise of the statement, in the same way as in round 1[23]. Figure 1.6. illustrates the ranking of drivers that obtained fifty percent or more.

As Figure 1.6. shows, the top five drivers identified as most important are all related to our current economic model, which can lead to both capture by and dependence on corporate actors. Interestingly, the most important driver of regulatory weakness identified was the disproportionate power of Big Tech companies in shaping regulatory compliance (e.g. RegTech). This also speaks to the widespread concerns among the experts about the different dimensions of this power: 1) *political-economic power* (market concentration as regulatory leverage, supply chain control), 2) *infrastructural power* (technical dependence and reliance, too embedded to challenge), 3) *epistemic* (both expert authority and digital systems built on particular epistemologies), 4) *regulatory power* (also in terms of algorithmic governance), agenda-setting and lobbying, and hence the overall power to structure the conditions under which particular regulation and particular understandings of security are thinkable, implementable, legitimate, and defensible. This also speaks to concerns about power and knowledge asymmetry between Big Tech and the State, whether regulatory or positive; the likes of Microsoft, Palantir and OpenAI were flagged by the experts as particularly problematic.

> 'As security governance becomes increasingly technical and data-driven, states may become dependent on private vendors for critical infrastructure, software, and analytical tools. This creates knowledge asymmetries where governments lack full visibility into the systems on which they rely. Such dependencies can introduce strategic vulnerabilities, particularly in geopolitical contexts where supply chains and technological sovereignty are contested.'

[23] The following quotes from experts on drivers are collated from both round 1 and round 2 as they speak to the same subject.

This is echoed in prevalent policy concerns about national control over critical digital infrastructure, but also about regulatory capture, as one expert expressed it:

> ‘capture changes the entire logic of governance: dominant firms can set standards, control information flows, and define compliance in ways that serve their interests. Once normalised, it becomes difficult to distinguish public security goals from market strategies, and the state’s room to manoeuvre narrows sharply.’

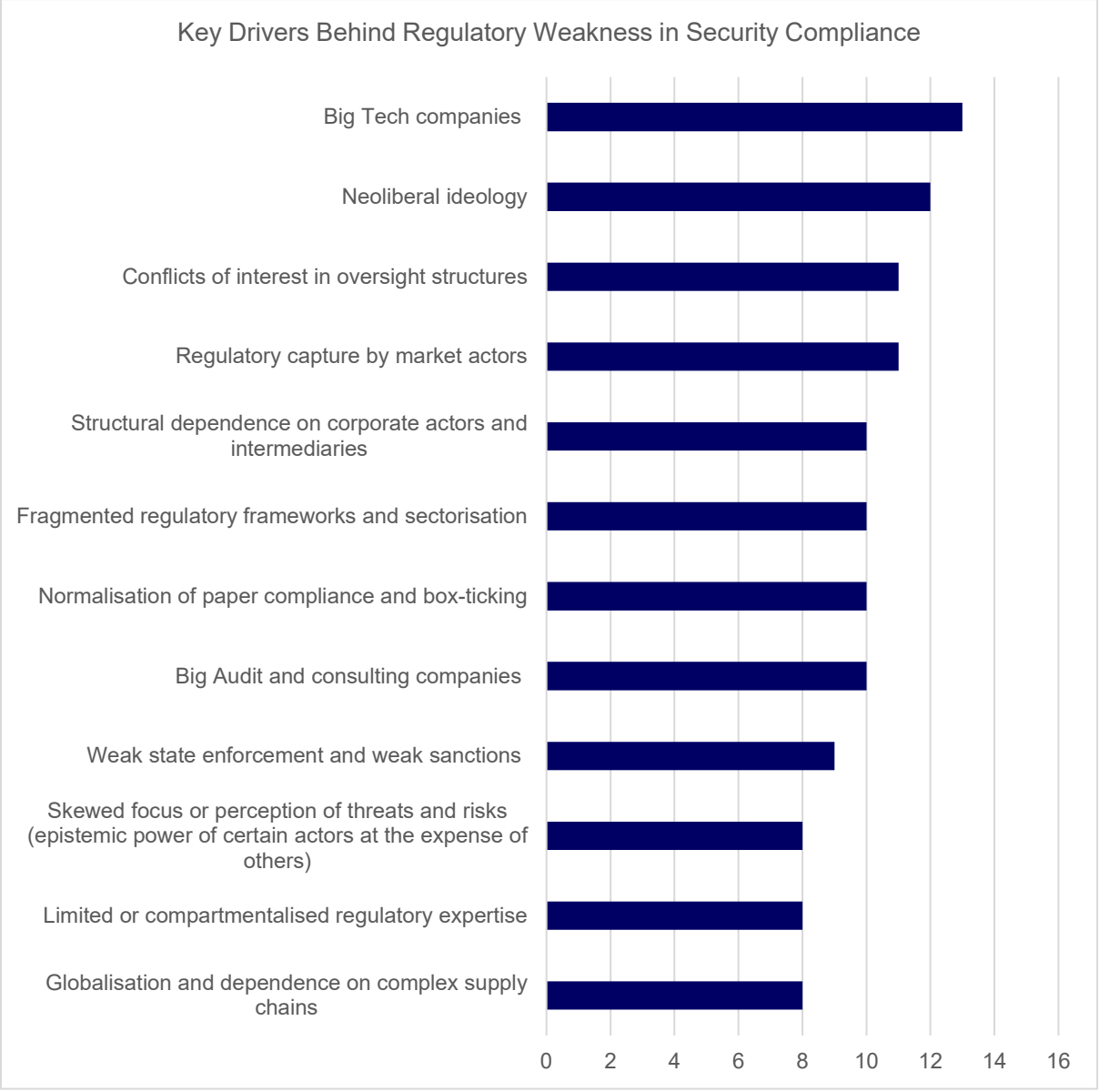

Figure 1-6. Drivers of regulatory weakness.

Another expert argued that a key driver behind the likely near future negative security compliance outcomes would be precisely ‘the technological development (driven of course by commercial interests) and the profound naïveté of politicians as regards technology, seeing it as “good” and “economical”’. While the privileging of compliance solutions has been linked to neoliberal forms of governance in the first place, neoliberal ideology has also been seen as driving their failure. Or as one expert put it:

> ‘Current frameworks are often optimised for cost-effectiveness, and legal defensibility, but high-intensity threat conditions expose their limits, especially where risk is non-linear.’

Another expert echoed the concern about these systems being more about reducing accountability and liability, both for the state and companies, than about security:

> ‘Regulatory structures don't provide security but provide bureaucratic work arounds to reduce accountability of the state towards its citizens. Companies work on the same principle, the idea is not to provide security but to reduce any liability (of the company, in case something happens).’

This is an interesting statement as it also points towards a certain cynicism in regard to security compliance solutions and points us back to the academic discussions about the lack of democratic accountability and legitimacy.

Another concern was related to the role of geopolitics in relation to regulatory power and the power of Big Tech, and how a tense geopolitical climate could reshuffle the cards:

> ‘Cross-border legal and geopolitical constraint: Sanctions regimes, export controls and alliance obligations etc can sharply limit feasible technology choices and supply chains regardless of domestic preferences. This can accelerate both consolidation (toward “trusted” vendors) and fragmentation (toward sovereign preferred vendors), reshaping who holds leverage in security.’

Another expert emphasized that the current regulatory approaches may not be futureproof in respect to the rapidly changing environment:

> ‘Many compliance systems were designed in relatively stable geopolitical contexts and may not be well suited to emerging conditions characterised by heightened interstate tensions, technological disruption, and economic fragmentation (…).’

A more fundamental concern running through both rounds of the survey and invoked by the experts in their reflections, pertained again to epistemology and here more specifically knowledge production itself, impacting governance and power relations at all levels.

> ‘AI fuels disinformation, information warfare and destabilization of knowledge production”: “this targets the epistemic layer that both democracy and techno-bureaucratic governance rely on, namely credible knowledge, expert authority, and shared factual baselines. If information integrity degrades, both public legitimacy and organisational risk management become easier to manipulate and harder to verify.’

Jointly, the identified drivers are both systemic and epistemic. In addition to the drivers identified by the researchers and those ranked by experts, the experts, in both rounds of the survey discussed other forces that should be considered but have been left out. In particular, the role of climate change has been flagged as an important constraint ahead. Climate change forces us to contemplate the actual terrain, or as one expert put it:

> ‘Climate impacts act as threat multipliers that strain infrastructure, supply chains, insurance markets, migration governance, and fiscal capacity, making “business as usual” security models harder to sustain. This driver is structurally different from discretionary policy choices because it imposes physical constraints, pushing societies toward adaptation, rationing, and new collective arrangements.’

Interestingly, throughout both our survey, literature review, and previous research, one word has been conspicuous by its absence: peace (and with it also positive human-centred visions of security). This is interesting in itself, has ‘peace’ become the epistemic blind spot of current

security regulation and governance? Since the end of the Cold War, 'peace and security' appeared as a pair that went hand in hand, as Western countries acted on their so-called enlightened self-interest and spread development, security, good governance, and rule of law across the Global South. Interestingly, peace and related concepts such as reconciliation, de-escalation, mediation, dialogue, diplomacy, or 'human security' (Brach and Sheldon 2025) do not figure in either the language of security regulation or security compliance; this is likely symptomatic of the crisis of liberalism and the shift away from liberal peacebuilding and towards militarization (Iñiguez De Heredia 2021), and the new rhetoric of 'peace through strength' as manifest in recent US national security strategies or rather 'peace through war' as the recent US Operation Fury in Iran has shown.[24]

As a recent report by SIPRI argues:

> 'Non-military conflict management is still relevant, and indeed essential, but the emphasis is increasingly being placed on military answers, as reflected in steeply rising world military expenditure. Despite regional differentiation in motivations, commitment to norms, types of security threats and conflicts, as well as preferred conflict management tools, the commonality shared by almost every corner of the world is increasing militarization, meaning a preference by states to address perceived threats and engage in conflict by military means over other tools. (…) Spending increases reflect the fact that countries perceive a high probability of military conflict in the future, which incentivizes the choice of militarized conflict management approaches and can ultimately become a self-fulfilling prophecy. Without diversified conflict management approaches, the law of the instrument, which states that when one only has a hammer, everything looks like a nail, can lead to widespread securitization and militarization.' (Baldwin 2025, 2–3)

Indeed, liberal universalist and paternalistic peace-making has traditionally been the domain of states, multilateral organizations, NGOs and humanitarian donors; hence it may not come as a surprise that with the increased power of security market actors, including Big Tech, the peace discourse fades into the background and loses its normative power while militarized discourse of security threats and risks leads the charge. Can this glaring omission, the absence of positive goals for security being effectively embedded in regulatory frameworks, drive the long-term weakness of security compliance solutionism?

One expert remarked on this omission and raised the question of 'how to support peace movements?' And indeed, we may wonder how – in a context where the conceptual vocabulary of peace is pushed to the fringes of the security discourse despite peace being fundamental for security and security unthinkable without peace. Or as one of the experts remarked,

> 'Big Tech is getting even more powerful – yet instead of using their billions as a buffer that allows them to stand up for values of fairness, justice & democracy, big tech boards and CEOs are pandering to autocratic leaders. These are the companies that provide platform services, cloud services, etc. to many [security] critical organisations.'

This brings us back to the starting point and the tension between national security and profit interests. And it also brings us back to the question of depoliticization and 'technosolutionism'.

[24] The White House press release from 8. April 2026 titled 'Peace through Strength' is instructive here, concluding with the statement that 'The overwhelming might and fury of the American military gave President Trump maximum leverage. As the Trump Administration enters this next phase of negotiations, it is clear that America stands stronger, our enemies weaker, and the world safer.' https://www.whitehouse.gov/releases/2026/04/peace-through-strength-operation-epic-fury-crushes-iranian-threat-as-ceasefire-takes-hold/

2 Exemplary Case of Security Compliance: Insider Risk Management

Having discussed the regulatory security state (RSS) as a regulatory and governance idea and a new social phenomenon and having placed it within a larger socio-political, technological and geopolitical context, it is now time to consider how it operates in practice. Security compliance is a vast area and there is a wealth of products on the market catering to different regulatory obligations and perceived security threats and risks. In order to study security compliance and management in practice, to the degree that this is even possible given its secretive character and the proprietary nature of technologies involved, we have chosen to zoom in on insider risk management. In 2.1., we will therefore briefly sketch out the relatively recent emergence of 'insider threat' and 'insider risk' as something to be managed by organizations (outside of military, intelligence or handling classified information) in the Norwegian context. We will also discuss some of the key premises upon which these managerial tools are built, and their limitations. In 2.2., we move to a future-oriented expert assessment of the potential risks associated with these managerial tools, which were the subject of the second round of our expert survey.

Insider risk management strikes at the heart of personnel security management and thus implies measures that impact workers and employees across Norwegian society. This is at the core of our expertise of the Work Research Institute, and we view it as imperative to study societal developments impacting on workers' rights, well-being, psychosocial work environment, power shifts in the workplace and the role of trade unions. However, we view this case also as an illustrative example of security compliance at large as it manifests and actualizes the dilemmas of responsibilization of organizations for national security, i.e. the conflicts of interests between national security interests and the interests of organizations, the risks of mission and function creep and the hollowing out of purpose limitations in practice, and it speaks to concerns about legitimacy, accountability, depoliticization and epistemic closure. Insider risk management has gained momentum following the Russian full-scale invasion of Ukraine in light of the renewed concerns about hybrid threats, espionage, sabotage, and influence operations. The war has reignited Cold War fears of spies, traitors, and leaking of classified information – albeit in a radically transformed geopolitical, economic and security environment. The case of the Russian spy Mikhail Mikushin at the University of Tromsø, returned to Russia in August 2024 to a warm welcome from Vladimir Putin, gave a face to the annual threat and risk assessments by the Norwegian intelligence agencies. In 2025, the Norwegian Police Security Service (PST)[25] deemed espionage and sabotage against Norwegian businesses, universities and other organisations as *likely*, while the National Security Authority (NSM) emphasized that: 'Insider risk is for real. Norwegian organizations cannot wait for further warnings from the security services. Preventive measures must be prioritized today.'[26] In response to the security authorities' calls to prioritize personnel security and manage 'insider risk', organizations – both subject to the Security Act and not – are implementing new comprehensive personnel security policies, systems, and practices such as background checks, monitoring, risk flagging, or vulnerability conversations (*sårbarhetssamtaler*) aimed to tackle the 'threat from within' organisations. A plethora of market-based solutions, consulting products, cybersecurity and monitoring software, has emerged. And while these tools promise to manage insider risk - i.e. risk posed *to* organizations by employees and others with legitimate access, the risk these technologies themselves could pose is rarely considered. Another question is how these

[25] *National Threat Assessment* 2025, PST, https://www.pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/_nasjonal-trusselvurdering-2025_uu-engelsk.pdf
26 *Risiko 2025*, NSM, p. 14, https://nsm.no/getfile.php/1314212-1738741587/NSM/Filer/Dokumenter/Rapporter/Risiko%202025.pdf

managerial technologies shape our thinking and understanding of security and security threats – and what is left out.

2.1 Insider Risk and National Security: From Spies to Insiders

In the early Cold War, as the fear of Communist subversion reigned supreme, the 'insider' was primarily conceptualized as an ideological suspect: a person whose political commitments, personal vulnerabilities, private lifestyle or perceived sexual and other deviance might make them unreliable in a security bureaucracy built around secrecy. As the U.S. national security state consolidated after 1947, it became structurally dependent on large numbers of security cleared personnel; what would today be called 'insider management' was conceived, following a series of espionage cases, primarily as a *loyalty* and *reliability* problem which was addressed through screenings, investigations, and institutionalized suspicion about hidden subversion. During the aforementioned McCarthy era – the Second Red Scare and the Lavender Scare – national security vetting and clearance regimes became tied to broader 'confessional' and psychiatric ideas about normality and trustworthiness, reinforcing a concept of the insider as a potential internal enemy whose risk was inferred from identity, character, behaviour, ideology and beliefs, perceived amorality, abnormal sexuality, delinquency, and individual *psychopathology* (Genter 2018; Morgenthau 1955) – ideas embedded into Eisenhower's Executive Order 10450.[27] It is worth reminding ourselves of these origins of contemporary security clearance regimes and insider risk management, for as Genter points out, 'the movement in the first half of the twentieth century of psychiatric discourse into the political arena represented a fundamental rethinking of the relationship between the state, domestic security, and the individual' (Genter 2018, 1069). The legacies and epistemologies of this psychiatric (and psychologizing) discourse permeate contemporary personnel security management, also in Norway. The security clearance regime in Norway dates to the same period of mid-50s, to NATO membership and inspections which led to the establishment of a precursor organization to the NSM in 1953. Security clearances emerged in Norway in response to the NATO requirement from 1955 formalized in *C-M(55)15 (1955), Security within the North Atlantic Treaty Organization*, which outlined rules for classification and personnel with 'unquestioned loyalty' and 'such character, habits, associations and discretion as to cast no doubt upon their trustworthiness in the handling of classified information'[28] (for a detailed history, see: Synstnes 2016). Security clearances and intrusive investigations continue to be central to personnel, to protective security management and to tackling potential 'insiders' under the Security Act. They are also the most immediate expression of the link between insider risk and national security.

During the mid–late Cold War period, personnel security management regimes spread to federal contractors at the same as the 'insider' became more tightly associated with the figure of the 'spy' – a cleared individual acting as an agent for a hostile or rival intelligence service. In this framing, the spy is primarily a counterintelligence (CI) problem, with focus being on recruitment, tradecraft, detection failures, institutional vulnerabilities and access controls. The Cambridge Five can be seen as emblematic of externally tasked and controlled insider threats: embedded over long periods resulting in significant and long-lasting impact on national security, loss of life, compromised intelligence and geopolitical shifts (Gioe and Hatfield 2021a). Insider harm here is

[27] https://www.archives.gov/federal-register/codification/executive-order/10450.html
[28] Security within the North Atlantic Treaty Organization, C-M (55) 15, p. 2 https://www.stjornarradid.is/media/utanrikisraduneyti-media/media/varnarmal/security_regulations_-_c-m_55_15_final.pdf.pdf

episodic, high-impact and driven by adversarial intelligence services, while the solution prioritises counterintelligence tactics and personnel security measures aimed at finding 'the mole'. In the US, the notorious Cold War espionage scandals and high-profile cases of trusted insiders spying on behalf of the Soviet Union, such as Aldrich Ames or Robert Hanssen, which led to deaths of CIA assets, spurred research on the 'insider threat'; in 1986 the US Department of Defense (DoD) established PERSEREC which[29] has for decades now produced applied research and training materials in personnel security. This research has primarily been informed by *behavioural* sciences, *psychology,* and *management,* with the goal of profiling, predicting and pre-empting insiders and remains highly influential in contemporary approaches to insider risk – both in the realm of personnel security management and in cybersecurity. Norway has had its own iconic cases of Cold War espionage, including the political and heavily media-focussed spy case of Arne Treholt. While many have speculated in the motivations of Arne Treholt, the case has not spurred any research akin to that in the US, instead, historical and contextual research took precedence, even if still rather scarce (Gleditsch 2015). Consequently, the understanding of 'insider risk' in relation to national security is predominantly shaped by US defence and intelligence-funded researchers (Kuldova 2024); this research has been taken up by the commercial security industry and built into managerial and digital security products.

From the late Cold War into the post–Cold War era, we can thus observe a key shift towards understanding insiders as heterogeneous actors with diverse motivations and 'critical pathways' to betrayal (Shaw and Sellers 2015). PERSEREC research has tried to understand the 'expanding spectrum' of American espionage – e.g., by analysing individual cases from 1947–2015 – showing that ideological betrayal does not exhaust the motivational space; financial incentives, ego, grievances and disgruntlement, and other mixed motives become increasingly salient (Herbig 2017). There is thus a shift from focus on ideological motivations and external pressure and coercion to behavioural and situational explanations of how individuals' motives interact with privileged access; the psychiatric focus of the McCarthy era becomes refracted through newer psychological and behavioural research. The category 'insider' begins to broaden beyond espionage into a more general designation for any trusted access-holder who can compromise critical assets, a shift reflected in programmatic accounts that trace insider threat from its roots in espionage toward wider organizational harms (Gelles 2021). Espionage in the process becomes just one of many possible insider risks.

The emergence of this broad and general category of insider risk coincides with the digital revolution, the proliferation of cyber threats and cybercrime and the rise of commercial cybersecurity. As both information and infrastructure critical to national security become dependent on digital infrastructures and software, the question of cybersecurity gains top priority in national security circles. Even in the realm of cybersecurity, however, there has been a shift from an early focus on technical barriers to an increasing focus on 'human risk' and 'insiders' (Greitzer 2019) and the merging of cybersecurity with psychology. But other major events played an important role in the expansion of the concept, or as Herbig writes in the appendix to the PERSEREC report, discussing the relation between espionage and insider risk research:

> 'The concept of insider threat has changed significantly since the terrorist attacks of 9/11. The term was being applied during the 1990s to employees and other persons who had insider access to computers and who misused them and the information on them. As computers became standard office equipment and people increasingly stored and accessed sensitive or classified information on them, the threat of information loss or theft, sabotage of information systems, and even cyberespionage by foreign entities became thinkable. Often, early work on

[29] On October 1, 2024 PERSEREC was sunset under the Office of People Analytics, https://www.war.gov/News/Releases/Release/Article/4113076/pentagon-culls-social-science-research-prioritizes-fiscal-responsibility-and-te/

> insider threat focused on systems security, survivable architectures, auditing and monitoring of system users, and the modeling of likely threats and responses to plan effective countermeasures (Anderson et al., 2000).' (Herbig 2017, A-3)
>
> 'Whole new fields of academic study and analysis, consulting services, and conference circuits have grown up around problems of and solutions to insider threat. It is impossible now to think about workplace violence, fraud, domestic or jihadist terrorism, leaking of controlled information, sabotage, and computer misuse and systems hacking without conceiving of it as insider threat.' (Herbig 2017, A-5)

The post-9/11 reforms have added an additional layer to the concept. Intelligence failures and subsequent reforms elevated interagency integration and hence also intelligence and data sharing, increasing the number of people with access to large repositories and cross-domain systems (Jones 2018). These developments, taken together, changed what 'insider' means in practice: it becomes not only an exceptional threat actor potentially undermining national security, but a form of systemic risk produced by how modern national security – and *de facto* all – organizations must operate. When access is broadened to improve coordination, the insider attack surface is seen as growing – and the borderless and interdependent digital systems make control difficult. The solution becomes to subject more and more individuals to different forms of security clearance, security vetting, background checks, perpetual monitoring and surveillance, while expanding security compliance obligations – both within and outside the realm of organizations managing classified information or critical to national security.

The Edward Snowden, Chelsea Manning and WikiLeaks cases introduce the figure of the insider as a self-tasked digital mass leaker and become an iconic example of the new digital era insider threat. These represent a new threat scenario, given the scale (bulk data exfiltration), speed, and detection problems that arise in digital architectures; however, the verdict on the actual damage to national security is still out (Gioe and Hatfield 2021b). In these cases, the national security insider category becomes contested by its proximity to whistleblowing – a troublesome relation perpetuated in contemporary insider risk management systems: some insiders may interpret disclosure as a moral act tied to transparency norms and duty to reveal organizational harm, complicating the loyalty and treason template (Marangione 2019); alternatively, organizations may perceive legitimate whistleblowing as a threat to their reputation and may recast whistleblowers as insider threats, despite existing whistleblower protections. Understanding of the insider threat has primarily been driven by exceptional and spectacular cases: from the spies of the Cold War to the leakers of the digital era. This has, however, coincided with a simultaneous normalization of insider risk, largely driven by cybersecurity concerns, as all-pervasive, and an expansion of the different harms stemming from insiders – well beyond the realm of national security organizations and concerns about the protection of classified information.

In the 2010s–2020s, insider threat was reconceived as enterprise-managed sociotechnical risk and the insider as anyone causing – intentionally or not – harm to the organization. As cybersecurity perspectives come to inform the understanding of insider risk, we also see an expansion of the concept to encompass any thinkable harms to organizations (reputational damage, workplace harassment, violence, fraud, IP theft, compliance breaches, security protocol violations, breeches of ethical codes of conduct and more). There is no longer any automatic link between national security and insider risk, instead, the latter is first and foremost conceived as enterprise risk – the risk stemming from having employees, suppliers, and others with legitimate access. In other words, insider risk becomes a managerial tool that reframes workers as an inherent source of risk and as potential threat actors. The influential CERT's Common Sense Guide to Prevention and Detection of Insider Threats, published since 2005 by Carnegie Mellon University's CyLab, codifies insider threat as an organization-wide mitigation challenge spanning

policy, HR, legal, IT, and security functions, treating insider harm as an ongoing condition to be managed and reduced, not a rare and exceptional anomaly to be hunted (Kuldova 2024). Overall, there has been a shift to the integration of behavioural and technical monitoring with security management and building 'security culture' in organizations. The primary concern however remains with individual behaviour and psychological traits, despite some emphasis on organizational factors (these, however, often boil down to organizational control measures, procedures and guidelines).

Personnel security today is more than mere security vetting originally designed to protect classified information, sites, and infrastructures. While commercial background checks imitate the clearance regime, commercial insider risk programs appropriate the principles of personnel security management as developed in military and intelligence agencies – but, in no small part due to the digital revolution, turned into a form of best practice security management, disconnected from any immediate concerns about national security. Personnel security today has expanded to become a system of continuous personnel management and monitoring of behavioural risk flags, that by default positions the individual as the pre-eminent source of risk to the organization – no longer reserved for national security organizations, but an ordinary part of corporate security and organizational management. This poses a clear challenge – for when the regulatory security state or the Security Act speak of the threat of insiders, they largely think of the threats of espionage and sabotage – but when consultants, security and tech companies and businesses speak of insiders, they think of harms to their organizations that may have nothing at all to do with national security. While the introduction of these security systems is often legitimized with reference to national security and the current geopolitical situation, the risk of mission creep is *de facto* already embedded in most commercial platforms on the market. Therefore, these security compliance solutions have to be understood as primarily originating in the US context. And this also means in a very different working life context – a regulatory context lacking strong worker protections, labour law, or unionization and where intrusive worker surveillance and monitoring is normalized (E. Anderson 2017). These US-developed security compliance solutions are therefore not necessarily compatible either with our legal frameworks or fundamental values which in Norway extend to the workplace – and that we seek to protect, also through the Security Act.

2.1.1 Brief History of 'Insider Threats' and Insider Risk Management in Norway

The concept of the 'insider' is relatively new in the Norwegian context; until recently, we used to speak either of spies (*spion*) or disloyal employees (*utro tjener*); the concept of 'insider' was mostly linked to insider trading (*innsidehandel*). In the Norwegian context, the concept of the 'insider' has been largely imported from the Anglophone context discussed above, or else mostly from the US, UK and Australia and traces its origins to 1) military and intelligence contexts and the threats of espionage, 2) to corporate industrial espionage and threats such as IP theft, and 3) cybersecurity and threats such as social engineering, data theft and sabotage. These different points of origin, historical trajectories, institutional and cultural contexts, and security epistemologies have – over time and as appropriated by consulting companies – merged into a generic category of an 'insider' and 'insider risk' – understood as a risk to organizations stemming from having people with legitimate access. The various uses and evolution of the term in the Norwegian context can be traced across the annual Risk reports by the Norwegian National Security Authority (NSM). The first authoritative mention of 'insider activity' (*innsideraktivitet*) can

be found in NSM's annual report from 201030 in a reference to WikiLeaks, where it is remarked that

> 'insider activity can be committed by current or former employees, consultants, maintenance personnel, or others. An insider does not necessarily have malicious intent themselves but may be vulnerable to outsiders seeking protected information, whether through deception, persuasion, or pressure.[31] (emphasis added)

This speaks directly to the translation of the concern with the leaking of classified information from the US context to the Norwegian one. Other mentions in NSM's annual reports follow; for instance, the 2016 report mentioned the considerable threat posed by insiders, citing instances of foreign agents attempting to penetrate PST. The 2017 NSM Risk report moved away from the predominantly statist context and warned *all* organizations that 'people can constitute a weak point in organizations,'[32] referring to the Russian US election influence operations in 2016, linking insiders to hybrid threats and disinformation. In the same year, a 20-page guidance on security in employment relationships: before, during, and at termination (*Sikkerhet ved ansettelser: før, under og ved avslutning*)[33] written jointly by PST, NSM, Police and The Norwegian Business and Industry Security Council (NSR) [34], provided guidance to public and private organizations on measures to reduce insider risk; this report was aimed at organizations *not* subject to the Security Act. Threats to businesses and organizations and their key assets (and profits) from employees were at the core of the guidance. The only reference cited in the guidance is the Australian Government 2016 *Managing The Insider Threat To Your Business: A personnel security handbook*;[35] this Australian report in turn cites only two documents, a two-pager by the FBI on insider threat[36] and a report by the UK Centre for the Protection of National Infrastructure (CPNI), now National Protective Security Authority (NPSA), on insider incidents;[37] again, Edward Snowden and Chelsea Manning are used as exemplary insiders. This document is interesting as it exemplifies the policy mutations and translations of new concepts across boundaries. But it is also interesting as it seeks – in line with the logic of the regulatory security state – to responsibilize businesses for national security, while at the same time positioning *organizational security* (and not national security) as the primary goal. National security and national threat assessment by the intelligence agencies serve as tools to legitimate new organizational security measures, even if underpinned by the regulatory state's hope that businesses can be made to contribute to national security by self-policing. This enlisting of businesses in the task of policing and intelligence production is largely not problematized but instead viewed as cost-efficient for the state. The fact that it is organizational security and not national security that is the object of securing becomes largely glossed over, as is the conceptual shift from treating employees as a resource to treating them, and others with legitimate access, as organizational risks and as *potential* threat actors. Personnel security management becomes in this sense a pre-emptive *management of the potentiality* of anyone with legitimate access becoming a threat to the organization/business, divorced from any immediate concerns about national security.

---

[30] NSM was established in January 2003.
[31] Rapport om sikkerhetstilstanden 2010, NSM, p. 7, translation ours; https://nsm.no/getfile.php/133768-1592988366/NSM/Filer/Dokumenter/Rapporter/rst_2010.pdf
[32] Risiko 2017, NSM, p. 4 https://nsm.no/getfile.php/133726-1592915950/NSM/Filer/Dokumenter/Rapporter/nsm_risiko_2017_lr_0404_enkelts_v3.pdf
[33] Sikkerhet ved ansettelsesforhold – før, under og ved avvikling, 2017, https://politietstryggingsteneste.no/globalassets/eldre/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf
[34] https://www.nsr-org.no/english
[35] https://www.dmv.com.au/wp-content/uploads/2021/12/DISP_Managing-the-insider-threat-to-business_Mar2016.pdf
[36] https://www.dni.gov/files/NCSC/documents/products/Insider_Threat_Brochure.pdf
[37] *CPNI Insider Data Collection Study: Report of Main Findings* (currently National Protection Security Authority, NPSA), https://www.npsa.gov.uk/resources/insider-data-collection-study-report-main-findings

In 2019, the Norwegian Petroleum Safety Authority commissioned DNV GL to produce recommendations on the management of insider risk in the oil industry – moving from *safety* to *security* management (Jore 2020). The report is informed largely by ISO and NS security and risk management standards, general practices for security management, NSM and PSTs definitions of insiders (themselves recycled from US), CPNI studies, the aforementioned Australian Government personnel security handbook, NATO's Insider Threat Detection Study and documents by the again aforementioned US Defense Personnel and Security Research Center (PERSEREC). Again, we see that in the absence of independent Norwegian and European research and guidelines, frameworks from the Anglophone context dominate.

The white paper 'Meld. St. 5 Societal Security in an Insecure World' (*Samfunnssikkerhet i en usikker verden (2020–2021))*[38] by the Norwegian Ministry of Justice and Public Security called for more research-based knowledge on insider threats. It links insider threat to the increased internationalization of Norwegian society and potential security risk posed by individuals with competing national loyalties, which could make them more vulnerable to exploitation by foreign intelligence; the Ministry's concern remains predominantly with consequences of open society for classified information, objects, infrastructure and personnel management in state security agencies (see p. 78). But it is not until NSM's publication of its Theme report on Insider Risk (*Temarapport innsiderisiko*)[39] in June 2020 and the Basic Principles for Personnel Security (*Grunnprinsipper for personellsikkerhet*) in August 2020 that the concept of the insider becomes well-established and defined in the Norwegian security discourse. The NSM theme report on insider risk defines an insider as follows:

> 'An insider is defined as a current or former employee, consultant or contractor who has, or has had, legitimate access to the organisation's systems, procedures, assets and information, and who misuses this knowledge and access to carry out actions that cause the organisation harm or loss. The insider is familiar with the organisation's routines, processes and vulnerabilities, and can use this knowledge to harm the organisation for the benefit of another organisation, a state, or for their own gain. Insider activity can be carried out directly and independently, or on behalf of an external actor. External actors may be state, non-state or other individuals. These actors may seek to exploit individuals with access to a company's or state's assets to achieve their own objectives.'[40]

This report expanded the relevance of the concept from those managing classified information and infrastructure to virtually any organization. It also utilized the language of intelligence threat assessments to understand the insider: it categorized the potential threat actor in terms of *intent*, *capability* and *opportunity* – be it to steal, commit fraud, sabotage, leak information, influence decisions, or help external threat actors achieve their goals. This threat assessment is also a key part of the NS 5832:14 standard and of the asset-threat-vulnerability risk analysis which is suggested as a recommended procedure for protective security management in compliance with the Security Act, discussed earlier. In addition to infiltrators, and recruits, the report warned also of unwitting or accidental insiders with low security awareness or just plain sloppy security habits, and those vulnerable to manipulation or with exploitable weaknesses. While for PST, the main threat stemmed from foreign actors and organized crime, in NSM's translation of threat assessments into the language of risk management, the insider becomes more of a 'floating signifier' or a strategic label that different actors can fill with meaning and partially fix to serve different governance, technical, and political projects. The report repeats the need to understand

[38] https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf
[39] *Temarapport Innsiderisiko,* NSM, 2020, https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf
[40] *Temarapport Innsiderisiko*, NSM, 2020, p. 9, https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf

and protect one's assets, but it is *human vulnerabilities* that are a key concern: since, as the report states, common to all instances of insiders is the presence of one or more *human vulnerabilities* (p. 23): from ideology, conflicts of loyalty, financial trouble, change of life situation (divorce, etc.). This approach builds on research coming from the US defence establishment, PERSEREC and MITRE[41], which also underpins the conceptualization of security clearances. Only here it expands to a generalized form of threat from anyone on the inside, intentional or not. Case study boxes in the report emphasize the heavily mediated, and all non-Norwegian, cases of Chelsea Manning, Reality Winner, Hermann Simm, and Kevin Mallory. This yet again speaks to how the concept has travelled from abroad and became translated into the Norwegian context by NSM. The *Basic Principles for Personnel Security* further reiterate this systematic risk-based managerial approach to a now generalized and rather empty category of 'insider risk'[42]: having a security management system in place and routines for identifying, following up and managing *individual vulnerabilities*, becomes central. In the process of generalization and expansion of the concept, individual vulnerability and its management becomes core focus of the security management system.

In 2023, two reports on insider risk, based on literature and knowledge summaries, came out, one by SINTEF (Høiby et al. 2023) and commissioned by the Civil Security Clearance Authority, and the other by FFI (Slagnes 2023). Both studies emphasize the lack of Norwegian research in the field, and confirm the hyperfocus on the individual, the merging of cybersecurity concerns about the 'human factor' (Afnan et al. 2024, e.g.,; Colwill 2009; Kraemer et al. 2009) and social engineering with counterintelligence frameworks concerned with espionage and recruitment of insiders, along with the dominance of taxonomical and theoretical 'pracademic' studies (Kuldova 2024). Both studies remark on the general lack of empirical studies in the field and on the lack of Norwegian material. Neither report considers these systems in relation to Norwegian working life, to labour law regulations or other values core to the Norwegian way of life. We refer the reader to these studies for a more detailed literature review on this subject than we can offer here.

While critical research on this subject has been practically non-existent, the security industry has not wasted a moment in appropriating the concept of insider risk. This is not surprising given its conceptual versatility and character as a floating signifier which can be filled with any meaning, depending on context. In the world of consulting, the 'insider' can signify any thinkable threat stemming from having people in organizations. Much like in the context of security compliance in general, discussed in 1.1.2., even here we see a rapid emergence of security consulting and software products designed specifically to tackle the problem of insider risk. While some emerged in response to the concern of the intelligence services, NSM, and security compliance under the Security Act, we find also a plethora of other products sold as 'best practice' for personnel security to prevent any sort of non-compliance or unethical conduct on the part of the employees.

Security consulting, legal and professional firms on the Norwegian market today offer courses, consulting services, background checks, software and other products to *pre-empt* malicious and accidental insiders and manage all sorts of risks posed by individuals with legitimate access *to* the organization and its assets (e.g., infrastructure, IP, profit, reputation, business continuity) – far beyond the risks of espionage, leaking of classified information or terrorism. Indeed, from the point of view of the regulatory security state this could be viewed as a success – after all, the market is responding and delivering solutions to tackle problems identified by the intelligence agencies as pressing. But the question is whether these market-based solutions are appropriate to the actual threats identified by these services and thus fit for purpose, whether they are

[41] MITRE Insider Threat and Research Solutions, https://insiderthreat.mitre.org/
[42] *Grunnprinsipper for personellssikkerhet*, NSM, 2020 https://nsm.no/getfile.php/134159-1598879548/NSM/Filer/Dokumenter/Grunnprinsipper%20for%20personellsikkerhet%20.pdf

proportionate and in line with the values that we seek to defend, or whether they pose new risks. On the website of Holte Consulting we can for instance read that:

> '…the requirements of the Security Act related to preventive security in organizations subject to the Act are not very different from what should be expected from good governance in organizations that are not subject to this legislation.'[43]

We could ask here – is this really the case; is it – or should it be the same?

2.1.2 Epistemic Closure: Key Assumptions and Blind Spots of Insider Risk Management

Insider risk management frameworks, as we have seen, can be traced back to the secretive worlds of intelligence and espionage which eventually merged with concerns about cyberthreats and approaches to cybersecurity informed by the psy-disciplines (from psychiatry, psychology, psychometrics to behaviourism), and managerial concerns about effective management of the workforce, control of the workforce and increases of productivity and efficiency. As such, they go beyond the increasingly publicly debated concerns about the security clearance regime from which they originated. The following thus has relevance for the security clearance regime as well, but we should be conscious of the difference; the security clearance system raises its own questions (Bakke 2019; Graver 2021; Synstnes 2016): for individuals – where the loss of clearance undoes careers, is associated with considerable stigma and can be perceived as unjust or discriminatory. The process itself can also be lengthy and psychologically draining for organizations, who may struggle to access the necessary competence and thus wait for personnel to be cleared. It also poses issues for the labour market and social dynamic at large, where citizens with affiliations to countries deemed a threat to the Norwegian state are excluded from positions of trust and deemed potentially disloyal and untrustworthy. With insider management, we are dealing with a general approach to workforce management, both within and outside of the Security Act and thus with a managerial paradigm which originated from the classified realm but became a form of general enterprise risk management; it replicates some of the issues present in the security clearance regimes but also presents additional risks. Moreover, where the former is regulated and in the hands of the public agencies, the latter has – despite all existing regulated – limited safeguards in actual practice.

Before we proceed to unpack some of the key assumptions and blind spots of insider risk management as it exists today – in theory and on the market, let us consider a fairly representative example from the Norwegian context, which will help us in this exercise. As mentioned earlier, private security companies have become central in translating the Security Act, and other compliance-oriented laws and regulations for that matter, into *guidelines* for the organizations, even in the public sector. A case in point is the *Guidelines for Personnel Security in Power Supply* written for the the Norwegian Water Resources and Energy Directorate (NVE) by the consulting company Advansia; this company has become well-established in the field of insider risk, and is staffed by, among others, former PST employees. The Guidelines simply state that

> 'Personnel security is about implementing measures that reduce the risk of employees posing a security threat—in other words, reducing the risk of insider activity. The guide is intended as a supporting document to help establish a consistent and best practice approach.'[44]

[43] https://holteconsulting.no/2024/04/04/nar-det-blir-alvor-om-forebyggende-sikkerhet-i-din-virksomhet/
[44] NVE Veileder nr. 1/2024, Veileder i personellsikkerhet for kraftforsyningen, p. 5 https://publikasjoner.nve.no/veileder/2024/veileder2024_01.pdf

The guidelines include the typical recommendations for a security governance framework driven by risk management: identifying critical assets, assessing vulnerabilities, and conducting threat assessments; having clear procedures for recruitment and onboarding (such as background checks, OSINT, and suitability assessments), ongoing employee training and awareness on insider threats and cybersecurity. It also emphasizes regular reviews of access controls, integration of insider risk into crisis preparedness, and careful handling of terminations (e.g., NDAs, equipment recovery) and subcontractors through due diligence and risk assessments. In this sense it of course echoes NSMs Basic Principles and the Theme report on Insider Risk discussed above, as well as the NS 5832:14 standard. Insiders are divided into intentional (infiltrators, recruited, self-motivated) and unintentional insiders (ignorant, reckless/negligent): all workers, by default, pose an insider risk – these definitions open up the Pandora's box of perpetual worker monitoring, control, and evaluations in the name of security. A further citation from the guidelines sheds more light on this approach:

> 'People's thoughts, ideas, and attitudes can change both in the short and long term. Personality traits, external stress factors, and organizational weaknesses can all be decisive in whether individuals in this category of insiders actually commit malicious acts. This highlights the need for continuous attention to all employees through daily security management and relevant preventive measures.'[45]

Effectively, what is to be managed are people's thoughts, ideas and attitudes. Theoretically, the guidelines reproduce and translate into Norwegian the Critical Pathway to Insider Risk™ framework developed by Eric D. Shaw, former intelligence officer and clinical psychologist, and Laura Sellers, published first in 2015 in *Studies in Intelligence*, a journal run by the Center for the Study of Intelligence, part of the CIA (Shaw and Sellers 2015). The model has since been expanded into a range of trademarked investigative tools, training programs, certifications, and consulting services.[46] In this approach, monitoring, management, and reporting systems are used to spot dissatisfied employees. Here, performance reviews and security vulnerability conversations (*sårbarhetssamtaler*) with those showing security concerns are key tools. While the focus is mainly on reporting and control, employee well-being can be emphasized, such as in NVE's guidelines, however – not as a goal in itself, but as a way to reduce insider risk. Or as the guidelines put it,

> Disgruntled employees, or former employees who for various reasons hold a grudge against their employer, may seek revenge—for example, through actions that could negatively impact or harm their current or former employer. It is therefore important to identify the factors that contribute to job satisfaction and/or dissatisfaction within the organization...[47]

The concept of 'human vulnerability' and its management emerges as a central concern. To take another example, in the *Personnel Security and Vulnerability – guidelines* from The Immigration Appeals Board (UNE)[48] we can read the following:

> 'The term "vulnerability" or "human vulnerability" can encompass many aspects. At UNE, it may, for example, be related to the risk of being exploited by criminal actors, one's own network, or foreign intelligence services. It may involve a lack of awareness or understanding of rules, guidelines, and UNE's values. It can also include conflicts of loyalty, financial difficulties, or

[45] NVE Veileder nr. 1/2024, Veileder i personellsikkerhet for kraftforsyningen, p. 13 https://publikasjoner.nve.no/veileder/2024/veileder2024_01.pdf
[46] For more, see the Insider Risk Group's website where Eric D. Shaw, former intelligence officer and clinical psychologist is the CEO: https://www.insiderriskgroup.com/approach
[47] NVE Veileder nr. 1/2024, Veileder i personellsikkerhet for kraftforsyningen, p. 7 https://publikasjoner.nve.no/veileder/2024/veileder2024_01.pdf
[48] Personellsikkerhet og sårbarhet – en veileder, acquired under Freedom of Information Act, translated from Norwegian.

> opportunities for personal or others' gain. Curiosity or a strong interest related to conflicts, case types, ethnic groups, or individual cases may, in some contexts, also constitute a form of vulnerability. A vulnerability may trigger unwanted behaviour, whether conscious or unconscious. This may include unauthorized database searches, dissemination of sensitive information, carelessness as regards confidentiality obligations, equipment, or concerning UNE's guidelines and system access. It may also involve failing to act neutrally as a case officer or decision-maker, for example due to conflicts of interest. This may often happen unconsciously.'

In the above we also see the slippage from concerns about national security towards concerns about organizational security and reputation management.

Furthermore, while the management of this individual vulnerability is the primary responsibility of the leadership and security managers, the individual employee is also responsibilized for managing their vulnerability:

> 'Assess their own vulnerability and report to their immediate supervisor if any of the circumstances (…) may negatively affect their work.'
>
> 'Contact their supervisor if they are concerned about a colleague in a vulnerable situation.'[49]

Security threats thus become reinscribed as 'vulnerabilities' and workers recast as a source of risk rather than a resource or asset worth protecting and developing.

The most interesting, however, is the fuzzy and floating concept of the insider itself. Here we may also provide a brief example of how the concept has travelled to Norway and been defined. The 2025 Security Conference in Oslo organized by the National Security Authority (NSM), featured Paul Martin, the former head of the UK Centre for the Protection of National Infrastructure (CPNI, now NPSA) and former Director of Security for the UK Parliament, and currently a Professor of Practice at Coventry University's new London-based Protective Security Lab and a Distinguished Fellow of RUSI. Paul Martin held a talk titled *It's all about people – building trust and resilience.*[50] The talk reflected the key tenets of his recent book *Insider Risk and Personnel Security: An Introduction* (Martin 2023), which falls within a larger field of security pracademic literature on insider threats. Much like the approaches of the security consulting industry, it endorses a broad concept of insider risk which encompasses 'unwitting insiders' who 'cause persistent low-level harm through poor performance and small acts of rebellion' to 'purposeful insiders with malign intentions' who 'have the potential to cause far greater harm' (Martin 2023, 1). While the latter are said to be his prime focus, there is no shortage of advice in the book on how to evaluate and handle employees with 'risk indicators'. As is common in the literature on insider threats, various crime, threat and harm scenarios, from violence to reputational damage, are merged together under the category of the 'insider'. Upon Martin's definition, an insider is simply 'a person who betrays trust by behaving in *potentially* harmful ways' (Martin 2023, 7; emphasis added) and it is up to the organization to define what constitutes harm to itself. Insider risk is then 'the security risk arising from trusting people' (Martin 2023, 7). And hence, 'trust, trustworthiness, deception and betrayal' and their 'management' become 'the core concepts in personnel security' (Martin 2023, 8). Recast as 'insider risk', criminal acts, terrorism, espionage, or sabotage, come to sit next to IPR theft, minor frauds, workplace violence, leaking, violations of ethical codes of conduct, whistleblowing, sexual assault and harassment, corruption, loss of assets, spilling, misuse of sensitive information, blackmail and more. We are told that 'a striking characteristic of insiders is

[49] Personellsikkerhet og sårbarhet – en veileder (2025), p. 3.
[50] https://nsm.no/kurs-og-konferanser/sikkerhetskonferansen/sikkerhetskonferansen-2025/program/it-s-all-about-people-building-trust-and-resilience

the diversity of their harmful actions' – this statement is followed up by a sigh that not all organizations realize this and take it sufficiently seriously, for 'they may not regard these problems as manifestations of the same underlying phenomenon, which is insider risk' (Martin, 2024, p. 14). Of course, any criminologist would doubt such an assertion, for is 'insider risk' really the same underlying phenomenon behind terrorism and whistleblowing? If we were to follow Martin, we could simply dismantle all the research dedicated to terrorism, espionage, whistleblowing or sexual harassment and instead devote ourselves to developing risk indicators. The problem is that this unsound assertion, repeated again and again in managerial literature, by consultants, and recycled into the empty managerial standards has become a managerial truism, widely repeated and accepted as the 'ground truth'. What happens with our understanding of the world and security threats when we reduce complex phenomena such as terrorism, espionage or sexual harassment to a matter of 'insider risk'? Not only is this intellectually lazy, but it results in a profound and dangerous epistemic closure if this is *the* approach we take to threats against national security.

Granted, an organization may want to tackle and pre-empt all thinkable harms to its profits, reputation, business continuity and assets with the same hammer, and it may be most cost-effective to see all these diverse phenomena as a singular insider risk nail, but reducing these diverse security threats and misdemeanours into 'the same underlying phenomenon' is fundamentally unsound. Despite this, the regulator and security establishment fail to pause over the unsoundness of the concept. Would we say that what all external threats have in common is that they are 'external'? Would we just as easily go with all external threats being lumped together and then say things like – we can manage China in the same way as Iran or Taliban or the climate change?

What is under communicated here is that we speak of a security risk to the organization and its assets, for 'personnel security is about protecting organisations from the people who work for them' (Martin 2023, 13). Already this should give us pause; while insider risk programs are pushed on organizations in the name of protecting 'national security' or legitimized with recourse to the Security Act, they are primarily designed to protect organizations from employees – that is a very different matter. The inclusion of whistleblowing among the insider risks listed is a brilliant example of this. One of the exemplary case studies listed by Martin under the heading 'whistleblowing', intended to show that 'insiders may harm their employer by revealing or alleging wrongdoing', is the case of Peiter Zatko, Twitter's head of IT security who 'testified at a US Senate hearing that Twitter had misled customers and regulators about weaknesses in its security and the number of face accounts. The company denied the allegations' (Martin, 2024, p. 21). This is all we are told; the clear impression is that we are to think of Zatko as insider who damaged the reputation of Twitter. The case itself is, however, more paradoxical than this: Zatko used to work in DARPA and ran several Department of Defense (DOD) programs, among them Cyber-insider Threat (CINDER) and his whistleblowing in the Twitter case others raised, among others, the issues of Twitter's inability to protect the organization from insider threats. Zatko further:

> 'alleged that the Indian government had placed an agent inside Twitter. He testified that Twitter struggled to identify potential infiltration by foreign agents and typically was only able to do so when notified by outside agencies. The company was 'unwilling to put the effort in' to hunt down bad actors within its ranks, he said.' [51]

[51] Twitter may have hired a Chinese spy and four other takeaways from the Senate hearing, NPR, September 13, 2022. https://www.npr.org/2022/09/13/1122671582/twitter-whistleblower-mudge-senate-hearing

The paradox here is that while Martin flags Zatko as an example of an insider, his revelations speak to the national security concerns about foreign espionage. This example could not make it clearer that there is no default alignment between the interests of the national security state and that of the organizations implementing insider risk programs; to the contrary, in this case they could not be more divergent.

Another example of an insider provided by Martin is that of Frances Haugen, the well-known Facebook whistleblower, here, too, it is duly noted by Martin that 'the company denied the allegations' (Martin 2023, 21). While from Facebook's perspective or rather Martin's rendering of it, Haugen indeed may be seen as an 'insider', we should maybe remind ourselves that there is still such a thing as 'public interest', however uncomfortable that may be to organizational 'security' practitioners. And as for Frances Haugen, she ended as President Joe Biden's guest at his first State of Union Address where he thanked her for having shown us that 'we must hold social media platforms accountable for the national experiment they're conducting on our children for profit.'[52] Even more peculiarly, the following is listed as an insider case by Martin: 'US regulator the Commodity Futures Trading Commission (CFTC) awarded nearly 200M to a whistleblower who helped them and UK regulators to investigate rigging of financial markets' (Martin 2023, 21). However, this is precisely the point of the whistleblowing regulations and the US award system to whistleblowers – to uncover corporate crime and wrongdoing. Alas, it is by now clear that from an organizational perspective the point is precisely to prevent leaking, whistleblowing and identify individuals who are likely to speak up preferably before they do so. Even if Martin dutifully notes that 'whistleblowing about certain types of wrongdoing is protected by law', he makes a distinction between 'ethical whistleblowers' and other 'self-professed whistleblowers' who 'turn out, on closer inspection, to be complicated and, in some cases largely self-serving' (Martin 2023, 21), thus building in a default suspicion as to the motives of individuals. At the same time, governments across the world pin their hopes on whistleblowers coming forward and helping them uncover crimes and enforce laws, they encourage whistleblowing and produce legislation to protect whistleblowers from retaliation precisely in the hope that they do dare speak up, that they do not let themselves be coerced (or risk managed) into silence; whistleblowers are precisely to speak up from their position *within* organizations, as insiders with knowledge of corporate harm, fraud and crime. Or as the US National Whistleblowing Center, 'a frontline defender of those brave enough to expose corruption, fraud, and abuse' puts it,

> 'Whistleblowers are the first line of defense against corruption, fraud, and wrongdoing and the single most effective source for information about fraud and other illegal activities. Despite the risk to their professional and personal lives, company insiders, government employees, and others with original information about illegal activity regularly come forward to report crimes that would otherwise go undetected.'[53]

Similarly, we can read in the first paragraph of the EU Whistleblower Directive, which springs precisely from this recognition, and with which imposes compliance obligations on the regulated entities, the following:

> 'Persons who work for a public or private organisation or are in contact with such an organisation in the context of their work-related activities are often the first to know about threats or harm to the public interest which arise in that context. By reporting breaches of Union law that are harmful to the public interest, such persons act as 'whistleblowers' and thereby play a key role in exposing and preventing such breaches and in safeguarding the welfare of society.

[52] Biden Calls for New Online Privacy Protections for Children, Wall Street Journal, March 2, 2022, https://www.wsj.com/livecoverage/state-of-the-union-address-latest-news/card/biden-calls-for-new-online-privacy-protections-for-children-CxyC6T58x18Nw6LqNNTI

[53] Why Whistleblowing Works, National Whistleblower Center, https://www.whistleblowers.org/why-whistleblowing-works/

> However, potential whistleblowers are often discouraged from reporting their concerns or suspicions for fear of retaliation. In this context, the importance of providing balanced and effective whistleblower protection is increasingly acknowledged at both Union and international level.'[54]

Similar expectations and whistleblower protections are incorporated into the Norwegian Working Environment Act, under Chapter 2A – Whistleblowing.[55] Much could be said about this burden being placed by the regulator on the shoulders of an individual with limited power and resources who is to battle organizations with their legal teams and resources enough to silence, pathologize, and discredit whistleblowers, for we know well by now that the legal protections rarely function as they should and that whistleblowers rarely succeed if not supported by the power of partnerships and dedicated organizations serving public interest (Kenny 2024). We could also note the drive towards the individualization of responsibility in this (and other) legislation, which increasingly sidelines collective grievance mechanisms and the role of trade unions. Regarding the latter, it should not surprise us that trade union members and representatives often feature in the insider risk management discourse as examples of security risks to be tracked, mitigated and managed, in particular in the US. Here we should be particularly careful about what kind of 'knowledge' we are importing and whether it is at all compatible with our labour regulations and the cherished Norwegian model of workplace democracy, collaboration and trust in the workplace. The excursion into the troubled territory of whistleblower/insider (Joseph et al. 2022) has been made here precisely to exemplify the diverging interests of organizations and the regulator, such as profit versus public interest. This also reveals the possibilities for mission and function creep built into these managerial tools which reduce the understanding of complex security threats and harm scenarios to the problem of risky individuals and 'bad apples'.

And it is precisely these understandings that are being built into technological monitoring platforms that promise to detect 'insiders', raising questions of legitimate degree of surveillance, control and monitoring in the workplace. For an analysis of the digital tools for intrusive employee surveillance and behavioural monitoring available on the European market we recommend the report *Employees as Risks* (Christl 2024); here we can only quote from the concluding remarks of the report:

> 'The cybersecurity, insider risk and communication monitoring systems examined in this study process extensive personal data on employee behavior and communication from many sources. They serve different purposes ranging from the prevention of cyberattacks and the identification of employees who are considered a threat to the organization to the detection of misconduct and otherwise undesirable behavior. As these systems typically share data with each other, they become combined security and risk surveillance systems, which not only promise to detect incidents but to prevent them before they occur. (…) Because of the scale and depth of data collection and their rich capabilities for behavioral profiling over time they can be considered corporate mass surveillance or dragnet surveillance systems. In addition to detecting suspicious behavior, they help organizations automate how to respond to alerts, from notifying managers to automatically blocking employees from performing certain activities. They help them investigate past employee activity and allow them to search for certain kinds of behavior across large amounts of activity data, both in real time and over long periods of time. The systems examined in this case study continuously calculate risk scores for employees and provide profiling mechanisms that make intrusive inferences about employees. Forcepoint offers to assess whether employees are in financial distress, show "decreased productivity" or intend to leave the job, how they communicate with colleagues and whether they access "obscene" content or exhibit "negative sentiment"

[54] DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2019 on the protection of persons who report breaches of Union law, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937

[55] Act relating to the working environment, working hours and employment protection, etc. (Working Environment Act) https://lovdata.no/dokument/NLE/lov/2005-06-17-62/KAPITTEL_3#%C2%A72a-7

> in their conversations. Microsoft's communication monitoring system offers to detect everything from "profanity", "inappropriate" language, harassment and discrimination to corporate sabotage, data leaks, money laundering, bribery, conflicts of interest and "workplace collusion". Microsoft's insider risk system additionally promises to identify "disgruntled employees" and suspicious activities such as visiting "inappropriate or unacceptable" websites. The company's Sentinel cybersecurity system helps organizations understand whether a user whose behavior was identified as suspicious is a "disgruntled employee who just got passed over for a promotion". In addition to the systems' built-in data sources and profiling mechanisms, organizations can create their own risk policies that can detect any type of behavior or communication pattern based on custom data sources, rules, keywords and AI-based classifiers. It is quite easy to set up a policy or "watchlist" that aims to detect, for example, workplace organizing or employees who complain about working conditions. Of course, organizations are required to prevent cyberattacks and protect information security, which represents a legitimate purpose for data collection and analysis. To a varying extent, this also applies to measures against employee misconduct, from violations of regulatory and organizational policies to criminal conduct. Nevertheless, the findings of this case study raise serious concerns about potential misuse by employers, intrusive surveillance, disproportionate data processing, inaccurate risk assessments, arbitrary suspicion and the use of information about employee performance for risk profiling.' (Christl 2024, 68–69)

Today, most security compliance platforms additionally rely on various forms of machine learning and integrated AI tools. Not only is there the aforementioned risk of excessive and intrusive data collection and function creep, as well as divergence between the interests of the regulator and organizational interests of the regulated, but there are also inherent risks of AI-driven hallucinations, false positives, 'dirty data', and more, which can generate very real harms for workers.

The reliance on data and AI technologies to interpret these data also makes these systems profoundly vulnerable to biases in data sets, 'garbage-in garbage-out' problems, incomplete or misleading data, fabricated data and disinformation, which can lead to information integrity failures and undermine security decision-making and skew risk analysis in its own right. The fact that technology is neither neutral nor unbiased is not considered (or is disavowed) by those marketing insider threat programs, despite the potentially grave harms and injustices caused by these increasingly 'black-boxed' systems (Amoore and Piotukh 2015; Pasquale 2015; Ananny and Crawford 2018; Wright 2017). On top of a profoundly reductionist theory and understanding of security threats as stemming from 'insiders', we are faced with an added layer of potential harm and risk to people from these systems. These risks, however, do not figure in the security management risks universe – for, being the tools of management, the risks *from* organizations *to* society, people, nature, or national security, do not figure at all. It appears that the frantic profusion of these systems effectively distracts from this massive blind spot. It also underscores how, in practice, the regulated becomes the *de facto* regulator with disproportionate epistemic power and authority to shape our understandings of security threats and how they are to be managed. The 'solutions' offered on the market take the form of *more* checks, *more* due diligence, *more* risk assessments: we have moved from KYC (know your customer) to KYE (know your employee), KYS (know your supplier) and KYD (know your data) – authentications, screenings, background checks, perpetual monitoring, risk indicators abound. And yet, what is actually done based on this information remains opaque.

2.1.2.1 Hyperfocus on the Individual over Organizational and Contextual Factors

The historical trajectory of the concept, combined with the contemporary data-driven nature of many insider threat programmes (ITPs), has shaped an approach grounded in the intersection of computer science, psychometrics, behavioural sciences, and human resource management. Within this interdisciplinary configuration, the analytical focus is predominantly placed on the individual rather than on organisational or contextual factors (see, for example, Greitzer et al. 2013; Idris and Damilola 2023; Maasberg et al. 2020; De Valk 2020; Hashem et al. 2015). While external factors are often mentioned, they are largely considered only in so far as they impact on

the individual (and evaluated against the individuals' ability to handle different 'stressors'). As we have seen, the core idea becomes to flag high-risk individuals. Despite the fact that organizational culture, performance pressures and larger contextual factors play a central role in most corporate fraud, crime and security breaches – the focus of ITPs is solely on detecting 'bad apples' (Benediktsson 2010). Organizational dimensions, on the other hand, are typically conceived in terms of organizational barriers, technical controls, leadership measures all again directed at detecting, pre-empting, or managing *individuals*. In this sense, they are not truly *organizational* in the sociological sense, nor do they consider the wider social, political, cultural or other *contexts* – they are organizational only in the sense of organizational *procedural* measures and barriers designed to protect the organization against individuals within it. The same goes to a large degree for the talk of 'security culture', which is often reduced to a discussion of individuals internalizing security routines or measures to raise security awareness within an organization. This security culture is primarily concerned with building organizational barriers and controls to prevent unwanted acts – not actively building a desired culture. In other words, individual risk and pathways are a dominant theme in the literature on insider risk, as the aforementioned literature reviews also show (Slagnes 2023; Høiby et al. 2023). Epistemically speaking, we are therefore dealing with a field of threat understanding uniquely divorced over time from any understanding informed by social and political sciences, history, anthropology or the humanities – and even more strikingly, divorced completely from criminology or security studies. There is no attempt to understand sociologically any of the emerging threats – there is no particular theory or understanding of Russia, of terrorism, of fraud, of workplace violence, or of the workplace itself, to name just few – insider risk management effectively reduces all these phenomena to a question of individual psychopathology and risk stemming from individuals. If we fall for this mode of 'understanding' or rather misunderstanding of the social world, and appropriate such approach to security threats – are we not up for a massive intelligence failure ahead? The insider risk management approach is fundamentally disinterested in any *contextual* understanding of security threats – instead, it promises us that if we monitor each and every individual with legitimate access, preferably perpetually, for any thinkable risk flags and signs of disloyalty or treason, we will be safe.

It is important to question how *epistemologies* informed by clinical psychology and the needs and particular professional and organizational cultures of intelligence agencies have come to shape organizational 'best practice' across the globe. There is no doubt that this has profound implications for how we conceptualize workers, for relations in the workplace and for what we consider as legitimate levels of surveillance and control in the workplace. While a culture of secrecy, mistrust, control, compartmentalization, but also deception might be something workers in the intelligence community are ready to endure in the name of exciting and secretive careers, it is questionable whether it is a healthy organizational culture that should be expanded to the whole of society in the name of national security, societal security, resilience, total defence or total preparedness, or for that matter any other security buzzword of the day (for not to question whether it is capable of delivering on these goals). At this point we are well served to recall the concept of 'model power' and 'model monopoly' developed by the Norwegian sociologist Stein Bråten (Bråten 1973), which points to the influence one has by possessing a powerful model of reality which others must accept in the absence, weakness, or fundamental incompatibility of their alternative models. It is, however, not that other models do not exist – there is indeed a lot of nuanced and specialized research on security threats – but rather that they have not won in the long historical battle over meaning-making that informs societal practice. Once model power is established, the underlying premises and the episteme – irrespective of how sloppy, such as in the case of the concept of the 'insider' – become close to impossible to challenge as they become entrenched. In our case, this concept aligns with power, market and managerial interests, rather

than being a 'regulatory burden', as it provides a legitimate ground for worker surveillance and control and locates threats and frauds at the level of the individual employee, deflecting from any potential corporate harms or systemic risks generated by corporate actors. Indeed, the evolving security and risk management practices (as codified in ISO and Norwegian standards) which incorporate and translate models such as CPIRTM into Norwegian workplaces under the various rubrics of evidence- and research-driven managerial practices, while sanctioned and legitimized by laws, regulations and guidelines issued by public bodies, naturally acquire substantial model and epistemic power.

2.1.2.2 Managerial and Organizational Interests over Public and National Security Interest

The influence and epistemic authority of management consulting and cybersecurity firms in this field is pronounced; and knowledge production is accordingly linked to product development. At their core, security compliance tools are *managerial* technologies which the regulatory security state attempts to leverage for its national security and public interest. Within this managerial context, and in the context of the 'preventive security dispositif',

> 'fear is mostly directed against individuals, and the search for structural risks is transformed into a search for deliberate threats, and sometimes into a search for scapegoats. Prevention is no longer about structural change, but about apprehending potential troublemakers.' (Bigo 2025, 9).

Relying on these managerial tools, when the state delegates this responsibility to organizations it also tends to abdicate its own epistemic power to conceptualize the security environment *in light of* the national and public interest. Managerial tools are by default concerned with entrenching and perpetuating the power of the management over workers and with managing that part of reality which is within the perimeter of the organization and redefining threats in light of its own interests (as we have seen for instance in the troubling case of whistleblowing/insider slippage). In practice, it becomes both unrealistic and unclear how the alignment that the regulatory security state seeks to achieve is to unfold in practice. As national security threats become translated into *general* security risk and business risk management frameworks, they are also fundamentally transformed (Petersen 2012). Getting rid of disgruntled employees from *your* organization at best means moving them elsewhere, it does nothing to protect the society from the *potential* risk the organization has identified that they may pose – if we are to first accept the premise of insider risk (of course, in some case these individuals might be reported to the police or intelligence agencies, alas, this just goes to show that the functioning of the system depends on the positive state). If we assume that everyone performs such an exercise, where are the individuals excluded as 'security undesirables' from organizations? Of course, they are still in our *society* – maybe they are being taken care of by the social welfare administration, the risk and cost just being moved – and the longer they find themselves outside of employment, the riskier hire they may be deemed. Seeing organizational security as distinct from the social welfare state may immediately appear rather short-sighted. This is particularly true if we consider the simultaneous mechanisms of excluding workers and the efforts and funds channelled in their inclusion – despite whatever vulnerabilities and pasts they may have – into the labour market or into their social rehabilitation and reintegration. Where security management sees them as inherently risky and suspect, viewing their past behaviour as a predictor of their future, social welfare frameworks try to recast the same individuals as a resource and as capable of change. This being said, there are of course individual perpetrators and threat actors, and it indeed is reasonable to have some organizational measures to account for that possibility. The question is one of proportionality: at what point do seemingly reasonable measures turn into unreason?

An even more pressing question, however, is what these systems prevent us from addressing as they push us towards to individual-oriented security narrative and management framework. What

they systematically unsee, interestingly, are the very drivers of contemporary polycrisis. In this sense, the insider risk management strategies stand in stark contrast to the very character of our contemporary security situation. Corporate harms and crimes of the powerful, regulatory capture, environmental and climate consequences of 'business as usual', etc. (Tombs and Whyte 2015; Glasbeek 2002; Rothe and Kauzlarich 2016) – indeed, these harms are neglected as they are hard to stabilize as discrete 'threat actors' that would fit into the pre-emptive risk governance toolkits. And yet, these harms are also the proper object of *politics* (and ideally, of hard regulation) – not to be resolved by either research or technocratic compliance and self-regulation – they speak to the fundamental question of what kind of a society is desirable and how it is to be organized, and what is security (a harder question to answer than one would imagine) and how it is to be achieved. Already this short discussion of insider risk management shows how fundamentally *normative* and political solutions, reflective of interests of some parties over others, are recast as neutral, technical and merely managerial. The harm *from* organizations *to* workers, which is the very reason behind the Working Environment Act, collective agreements and labour regulations worldwide, is not considered a security threat – but a wide variety of harms to organizations from workers are repeatedly and easily rendered as 'security threats'. This brings us to the discussion of how different public interests and public goods are to be managed at the organizational level and weighed against each other. For, of course, organizations do not only have to comply with one regulation but many at the same time, each having a different 'public good' it seeks to protect. Concern with insiders is also just one, even if exemplary, case of security compliance in practice.

2.1.3 Legal Balancing Acts at the Organizational Level

Public and private actors established or operating in Norway are often faced with having to comply with a plethora of cross-sectoral laws and regulations (*forskrifter*) that require compliance with different security-related requirements such as *information* security (pursuant to the Personal Data Act[56] which incorporates the EU's General Data Protection Regulation),[57] *cyber*security (pursuant inter alia to the Digital Security Act which implements the EU's NIS1-directive) and *national* security (pursuant to the Security Act). These cross-sectoral laws and regulations often apply alongside other sector-specific security requirements e.g. security requirements in the health, banking or finance sector (Weitzenboeck et al. 2025). Whether and the extent to which any such cross-sectoral legislation applies to an organisation depends on the material and territorial scope of such legislation.

Thus, the Personal Data Act applies to organisations established in Norway that process personal data, as well as organisations not established in the EEA that process personal data through the offering of goods or services to persons in Norway or the monitoring of such persons' behaviour insofar as their behaviour takes place in Norway. The objective of the GDPR is twofold: the protection of individuals' fundamental right to data privacy and the facilitation of free movement of such data within the EEA, c.f. article 1 GDPR. A key duty of data controllers (the entity that determines the purposes and means of the processing) is to ensure *and be able to demonstrate* information security, i.e. that personal data is 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational

[56] Act relating to the processing of personal data, LOV-2018-06-15-38 https://lovdata.no/dokument/NL/lov/2018-06-15-38

[57] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, pp. 1–88 https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

measures', c.f. section 5(1)(f) GDPR. The data controller must first identify which personal data the organisation holds and then carry out a risk assessment to determine whether existing security measures are adequate, taking into account 'the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons', c.f. article 32(1) GDPR. Any such technical and organizational measures must be documented as part of the organisation's internal control documentation, c.f. article 5(2) and article 24 GDPR.[58] A personal data breach must be notified to the Data Protection Authority without undue delay, 'unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons', c.f. article 33(1) GDPR.

The Digital Security Act transposes the NIS1-directive into Norwegian law and applies to two categories of organisations: (1) public or private operators of essential services in eight specific sectors (energy, transport, health, drinking water supply and distribution, banking, financial market infrastructures and digital infrastructure) c.f. section 2 Digital Security Act; and (2) digital service providers (i.e. online marketplace, online search engine and cloud computing services) c.f. section 9. The Digital Security Regulations[59] provide further details on which organisations are deemed to be operators of essential services, c.f. section 1. An organisation is an operator of essential services if it: (a) provides a service which is essential for the maintenance of critical societal and/or economic activities, (b) is dependent on network and information systems,[60] and (c) where an incident would have significant disruptive effects on the provision of that service, c.f. section 6 Digital Security Act. The entities covered by the Act have two primary duties: (1) they must carry out a risk assessment and implement security measures that are reasonably proportionate to the risk that the entity faces, cf. sections 7 and 9 of the Digital Security Act and section 17 of the Digital Security Regulations; and (2) they must notify the relevant supervisory authorities (depending on the sector), with a copy to NSM, of incidents that have a significant impact on the delivery of services, within the time limits specified in section 17 of the Digital Security Regulations, cf. sections 8 and 10 of the Digital Security Act. According to section 6 of the regulations, the security management system must be based on recognized standards, a provision which echoes article 19 of NIS1 whereby member states are to 'encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems'. The department responsible for the specific sector designates the relevant supervisory authority, c.f. section 21 of the Digital Security Regulations.

The Security Act lays down different types of security requirements, including requirements relating to information security, physical security, personnel security and classified procurement. It applies to public sector bodies as well as suppliers of goods or services in connection with classified procurements, c.f. section 1-2. The purpose of the Act is to help 'protect Norway's sovereignty, territorial integrity and democratic system of government, and other national security interests', 'prevent, detect and counter activities which present a threat to security" and "ensure that security measures are implemented in accordance with the fundamental legal principles and values of a democratic society', c.f. section 1-1.The Security Act imposes security requirements on so-called 'classified' (*skjermingsverdig*) information systems, objects and infrastructure, c.f. sections 6-1 and 7-1. Information systems are classified if they process 'classified information', i.e. if national security interests may be harmed if information becomes known to unauthorised

[58] See the Data Protection Authority's webpage: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/ (accessed 30 March 2026)
[59] Forskrift om digital sikkerhet, FOR-2025-06-20-1131, https://lovdata.no/dokument/SF/forskrift/2025-06-20-1131
[60] A network and information system is defined as: (a) an electronic communications network within the meaning of section 1-5 nr. 2 of the Electronic Communications Act; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance, c.f. section 4 Digital Security Act.

persons, is lost, is altered or becomes unavailable, c.f. section 5-1. Information systems may also be classified if the system itself is of vital importance to 'fundamental national functions', i.e. activities of such significance that a complete or partial loss of function would affect the state's ability to safeguard national security interests, c.f. section 1-5(2) and section 6-1. Persons who shall have access to classified information or to classified objects or infrastructure must have security clearance, c.f. section 8-1. Each agency or organisation subject to the Security Act is responsible for ensuring that its employees have access to the abovementioned information, information systems, objects and infrastructure have security clearance.

Alongside the abovementioned security legislation are also restrictions on the export of certain dual-use items, including certain technology transfer (e.g. information) and research collaboration (dissemination) pursuant to the Export Control Act[61] and its regulations. Controlled goods or technology transfer falling within any of the three Item Lists (I-III) require a license from the Norwegian Agency for Export Control and Sanctions (DEKSA). The lists of goods and technologies that are regulated by the Export Control Regulations[62] are updated annually through international negotiations.[63] The controls include the hiring or hosting of foreign employees, PhD students or other researchers whose research falls under Item List II or III.

The above restrictions and controls must be applied in light of the Equality and Anti-Discrimination Act which prohibits discrimination based on various factors listed in section 6 first paragraph, including 'ethnicity'. However, differential treatment that: (a) has an objective purpose, (b) is necessary to achieve the purpose and (c) does not have a disproportionate negative impact on the person or persons subject to the differential treatment, is not prohibited, c.f. section 9 Equality and Anti-Discrimination Act. Furthermore, in an employment relationship, direct differential treatment based on ethnicity 'is only permitted if the characteristic in question is of decisive significance for the performance of the work or the pursuit of the occupation' and the abovementioned three conditions (objective purpose, necessary, and not disproportionate) are met, c.f. section 9 second paragraph. These conditions must be interpreted restrictively and must refer to a genuine occupational requirement, as the Anti-Discrimination Tribunal (*Diskrimineringsnemda*) has held.[64]

Although employees have a right to privacy and data protection at their workplace, such rights must be balanced against the employer's legitimate needs to ensure the proper running of the business. Thus, pursuant to the Working Environment Act,[65] the employer has a right to implement control measures in relation to employees when such measures are objectively justified by circumstances relating to the undertaking and do not involve undue strain on the employees, c.f. section 9-1. The term 'control measures' is understood broadly and, according to the preparatory works to the Working Environment Act, may be based on technological, economic, health and safety considerations, as well as psychosocial working environment, and social and organisational factors within the company.[66] Before the control measures are introduced, the employer must hold consultations with employee representatives on the proposed

[61] Act relating to Control of the Export of Strategic Goods, Services, Technology, etc., LOV-1987-12-18-93, https://lovdata.no/dokument/NLE/lov/1987-12-18-93
[62] Forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester, FOR-2013-06-19-718, https://lovdata.no/dokument/SF/forskrift/2013-06-19-718
[63] See https://hkdir.no/en/guidelines-and-tools-for-responsible-international-knowledge-cooperation/international-research-and-innovation-cooperation/export-control-of-technology-transfer-and-international-sanctions (accessed 30 March 2026).
[64] See for example DIN-2023-552.
[65] Act relating to the working environment, working hours and employment protection, etc., LOV-2005-06-17-62, https://lovdata.no/dokument/NLE/lov/2005-06-17-62
[66] See Ot.prp. nr. 49 (2004-2005) chapter 12.1 page 135.

measures and provide them with certain information,[67] such that the representatives and employees have a genuine opportunity to provide input and raise objections to such measures.[68] One challenge we have seen in practice is that security measures are often understood as mere technical measures assumed to be without direct impact on working environment and hence not discussed with employee representatives despite having profound impacts on the working environment in practice. Moreover, there is often a tendency towards secrecy when it comes to security measures, which can also undermine trust, security culture, and the psychosocial working environment in the long run.

The above shows that many organisations, depending on their size and sector, have to carry out various types of risk assessments and balance different and at times competing objectives (e.g. weighing risks to fundamental rights and freedoms of data subjects under the GDPR; preventing, detecting, and counteracting undesirable incidents in network and information systems used to deliver essential services and digital services under the Digital Security Act; protecting working environments, including the psychosocial environment). Furthermore, one and the same breach may need to be notified to different supervisory authorities, with different assessments of the likely consequences of the breach having to be notified, depending on the subject-matter. The type and origin of the legislation may also vary. Some legislation stems from Norway's EEA or international obligations (i.e. it is supranational), requiring that it is interpreted in light of EU or international instruments, while others are wholly national (e.g. Security Act). Furthermore, the rules may span from legally binding laws and regulations (*hard law*) to industry standards and guidelines (*soft law*) which, in turn, are often industry "translations" of legal requirements or "best practice". Furthermore, some of these rules are sector-specific, while others are cross-sectoral. This makes for a complex regulatory framework. The problem quickly becomes how to ensure reasonable balancing of different goals and a holistic approach which takes into account consequences across domains.

2.2 Expert-driven Risk Assessment of Insider Risk Management

So far, we have discussed the origins and epistemologies of insider risk management, and we have also identified some of the potential risks associated with this type of security compliance. In the Round 2 of our Delphi survey, we were interested in how these risks identified in our research into the subject are viewed by other experts familiar with them. In other words, we tried to reverse the risk gaze and assess that which is rarely considered – namely, the potential risks stemming from security risk management. Indeed, these qualitative assessments are based on individual expertise and experience, and hence need to be understood as such; others might view such risks differently. However, the widespread agreement on some risks and in particular their likely impact in the future, provides us with a useful tool to think about insider risk management in new ways and challenge established patterns of thought that – as it turns out – our experts view as largely counterproductive for long-term (national and organizational) security.

Prior to being asked to answer questions about this topic, the experts were provided with background information about insider risk management systems and were explicitly informed

[67] According to section 9-2(2) of the Working Environment Act, the employer must provide the affected employees with 'information concerning: a. the purpose of the control measures, b. practical consequences of the control measures, including how the control measures will be implemented, and c. the assumed duration of the control measures.'
[68] See the preparatory works Ot.prp. nr. 49 (2004-2005) chapter 12.6.3 page 147.

about the study's goal of conducting an expert risk assessment based on pre-identified risks. The expert risk assessment was carried out by asking the experts to rate a series of statements according to their perceived level of risk. The risk factors covered by the statements were informed by previous research, discussed in previous section.

However, we are not the first to raise the question of possible risks associate with these systems. A recent report by InfraCERT (KraftCERT), which is a sector CERT (Computer Emergency Response Team) for the electric power and petroleum sectors in Norway[69], has raised similar questions. Before we proceed to a discussion of how our experts evaluated the identified risks associated with these managerial systems, we briefly review the results from the InfraCERT report. In their report Preventing the exploitation of personnel: Principles and measures (*Forhindre utnytting av personell: Prinsipper og tiltak*)[70] InfraCERT describes how organisations can prevent exploitation of employees by threat actors, or, in other words, how they can prevent both witting and unwitting insider threats (KraftCERT 2025). In addition to providing advice on principles and measures to follow, however, a large part of the report is dedicated to mapping the current state of both perceived and experienced insider risks in their member organisations, as well as measures implemented to counteract these and, finally, risks associated with these measures. InfraCERT obtained this information through a survey and qualitative interviews. All of the respondents were security personnel.

In short, the InfraCERT report found that, both when it came to perceived risks and actual situations in which cybersecurity had been compromised, accidents and human error were a substantially bigger risk than intentional acts of disruption. In the survey (N=47), 72 % answered that their organisation had *not* experienced any incidents involving witting insiders, 3 % had experienced several and 2 % had experienced one. When it came to unwanted incidents due to human error, however, 77 % reported having experienced this. Still, despite the low level of risk associated with witting insiders, a large percentage reported having implemented various countermeasures against insider threats. For instance, 45 % answered yes to using security clearances, and 74 % answered that they carried out background checks. In the qualitative interviews (N=11), employees from some organisations reported conducting background checks of *all* employees, regardless of any legal obligation to do so. However, in the survey, only 9 % reported having implemented insider threat mitigation programs.

Furthermore, the report found that the evolution of the responses to insider risks had been an ongoing and accelerating process in recent years. For instance, it was noted that in many organisations, Russia's full-scale invasion of Ukraine led to the implementation of new security measures or the expansion of ones already in use. The authors of the report also write that many organisations '(…) have established security vulnerability conversations, or *have plans to implement such measures*' (KraftCERT 2025, 15; emphasis added) These security vulnerability conversations usually concern people being considered for certain roles, or people with connections to 'high risk countries', i.e. countries flagged in the reports by the intelligence agencies. Relevant to this, there was consensus in the qualitative interviews that security measures can be taken too far and end up posing legal, ethical and/or practical challenges for the organisations. For instance, most respondents highlighted the importance of avoiding discrimination when implementing measures, seeing as this can have legal ramifications. Excluding potential employees on the basis of their, or their close ones', connections to certain

[69] 'InfraCERT is an independent non-profit corporation, but has alerting responsibilities for the power and petroleum sectors in Norway in the event of serious cyber incidents. InfraCERT also does threat assessments, and gives input to national threat assessments. InfraCERT is part of the Norwegian Sector Response Network, is a full member of Forum of Incident Response and Security Teams (FIRST) and is a certified incident response team in Trusted Introducer.' https://www.kraftcert.no/en/

[70] All translations from Norwegian ours.

countries, was not only seen as a legal challenge, however, but also a practical one. Several respondents expressed that this could hinder both the recruitment of competent personnel, and stand in the way of retaining existing expertise within the organisation:

> ‘Several people expressed concern that new regulatory requirements—such as authorization, assessment of related parties, or security clearance—could result in existing employees no longer being approved. This was seen as particularly challenging, as the requirements could lead to the reassignment of experienced employees, a loss of expertise, and a decline in trust within the organization.’ (KraftCERT 2025, 16).

Moreover, several respondents highlighted that measures such as security vulnerability conversations can become a practical challenge, insofar as implementing these is a resource intensive process. This sentiment is echoed in another point that was brought to the fore, namely that strict and extensive security measures can affect the efficiency with which the employees conduct their work. Another concern was that the sum of different measures can end up being experienced by the employees as too far-reaching or invasive:

> ‘Several participants noted that AI and advanced technology could enable total surveillance of employees—with potentially significant security benefits, but to an extent that likely goes far beyond what employees would accept.’ (KraftCERT 2025, 16).

Even though the InfraCERT report only represented a few sectors in the Norwegian working life, we found this important as it echoed findings in the literature and our own research on this subject (under publication). As noted earlier, we have yet to encounter a risk assessment of these programs, but the InfraCERT report was a valuable first step in explicitly asking the question of whether security measures can go too far. The statements that we asked our experts to evaluate were thus based on our own research, interviews and observations in the field and literature review (under publication), as well as concerns raised in the InfraCERT report.

In the following sections, the findings from our expert risk assessment of insider risk management systems as part of the Round 2 of our Delphi survey will be briefly presented.

2.2.1 Risks Associated with Security Compliance – Near future (2026–2030)

As mentioned, the risk assessment was carried out by asking the experts to assess statements on the 5-point Likert scale rating each statement on from ‘very low risk’ to ‘very high risk’, where the middle point was defined as ‘moderate risk’. In general, the responses tended to cluster around the categories ‘very high risk’ or ‘high risk’. Therefore, when presenting the data visually, we chose to group the category ‘moderate risk’ with the categories for ‘low risk’ and ‘very low risk’ (see Figures 2.1. and 2.2.).

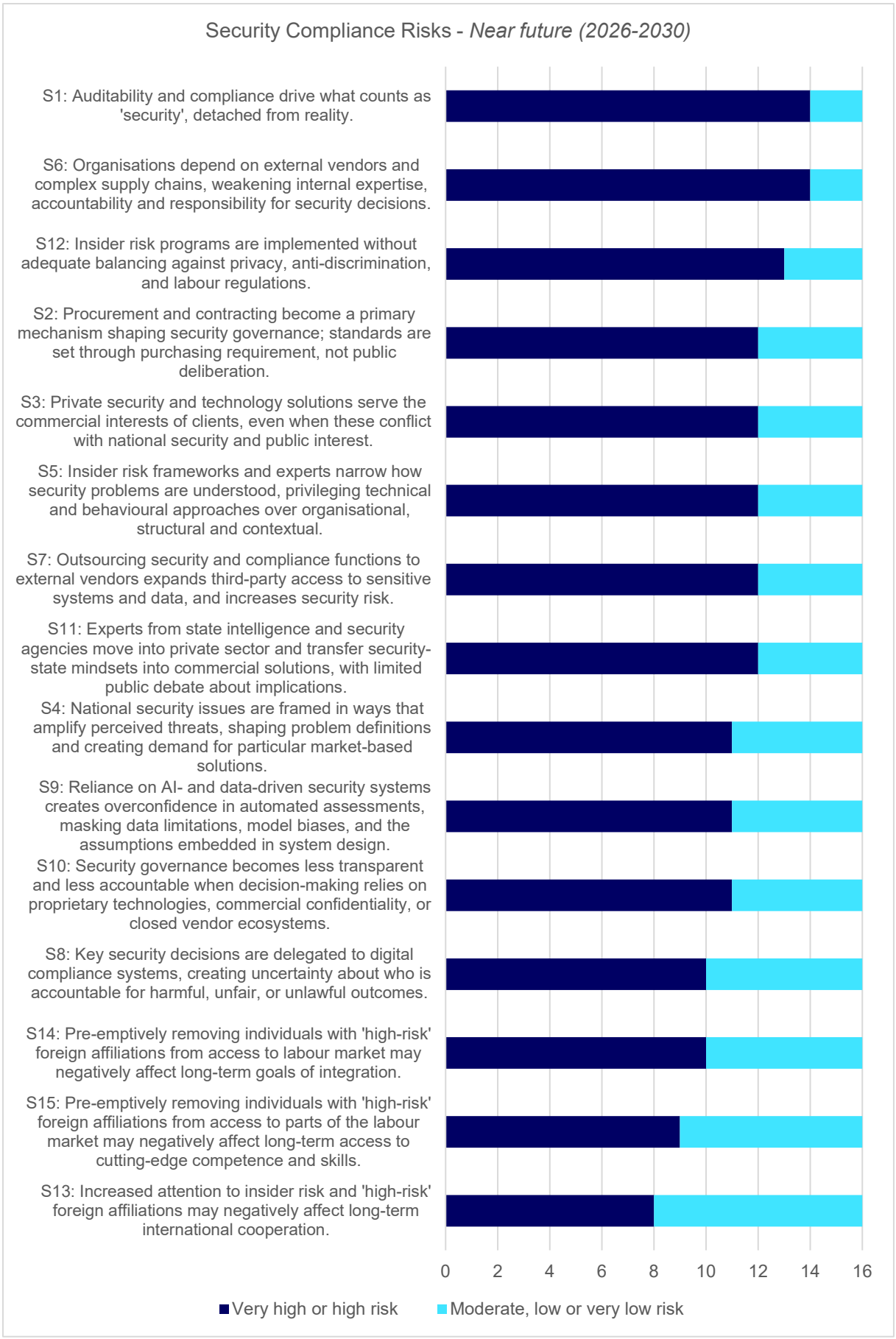

Figure 2-1. Risks Associated with Security Compliance – Near Future (2026–2030).

The first battery of statements sought to tease out expert assessments of near future risks associated with security compliance (2026–2030) based on the trends in security compliance we identified in prior research and discussed earlier in this report and on the results from the first round of the Delphi survey, in particular zooming in on the disproportionate epistemic power of consultants and security market actors in shaping security (compliance) discourses. For full disclosure, the statement battery was introduced to the experts with the following background information:

> 'The regulatory security state has contributed to the boom of private security management consulting and tech firms and other intermediaries who hold considerable epistemic power as experts, filling the 'zone of discretion', i.e. power over how national security related laws, regulations, guidelines and recommendations are translated into concrete organisational practices, technical standards and data-driven management platforms. Already today, security standards, frameworks, and "best practices" are effectively defined by market-leading vendors and technical experts rather than through independent research, public and political debate, or democratic processes. Please assess how significant you consider each of the following potential risks associated with their epistemic power over insider risk management.' (from round 2 of the Delphi survey)

In table 2.1. we have ordered the experts' perceptions of the identified security risks from very high/high to moderate, low and very low. Interestingly, 14 out of 16 experts consider auditability and compliance driving what counts as security, detached from reality as very high/high risk ahead. This speaks to the fundamental concern about the gap between the compliance maps and the actual territory. The same number considers the dependence on external vendors and complex supply chains weakening internal expertise, accountability and responsibility for security decisions as equally high risk. Interestingly, both key risks pertain to *the politics of knowledge* and for that matter also 'non-knowledge' and (strategic) ignorance (Aradau 2017; McGoey 2019), to how we come to know and understand security and to the *epistemic power* and dependence on actors shaping this knowledge. If we read through the other statements which the majority of our experts consider high/very high risk, we see that these too, in some fundamental ways, stem from the issues of epistemic power as it intersects with market power, private interests, or the power to shape regulatory processes and even bypass or undermine political and democratic debate. They can thus be traced back to the tensions between national security and organizational or private interests. They speak to the same democratic and accountability deficits identified in the academic literature on the regulatory security state at large (discussed earlier in 1.1.). Concerns about loss of competence on the side of the regulator were also raised, or as one expert commented in the free text:

> 'There are serious risks associated with outsourcing security decision making and regulation, particularly to for-profit corporations. This also risks hollowing out internal expertise and the capacity of government to conduct meaningful regulation.'

The technocratic rendering of security as an object of risk management and compliance procedures has consequences for the locus of contestation and the limits of possible critique: disagreements become disputes about risk assessment methods, due diligence procedures, assurance thresholds, and documentation sufficiency rather than about underlying security purposes, masking deeper value trade-offs and epistemically closing the field of the thinkable – and hence doable and practicable – approaches to security.

2.2.2 Risks Associated with Insider Risk Management – Near Future (2026–2030)

The second battery of statements sought to tease out expert assessments of near future risks associated with insider risk management, formulated based on insights gained through literature

review and our independent research (Kuldova and Østbø 2026; Kuldova 2024; and under publication), while also integrating concerns identified in the aforementioned reports by InfraCERT (KraftCERT 2025) and Cracked Labs (Christl 2024).

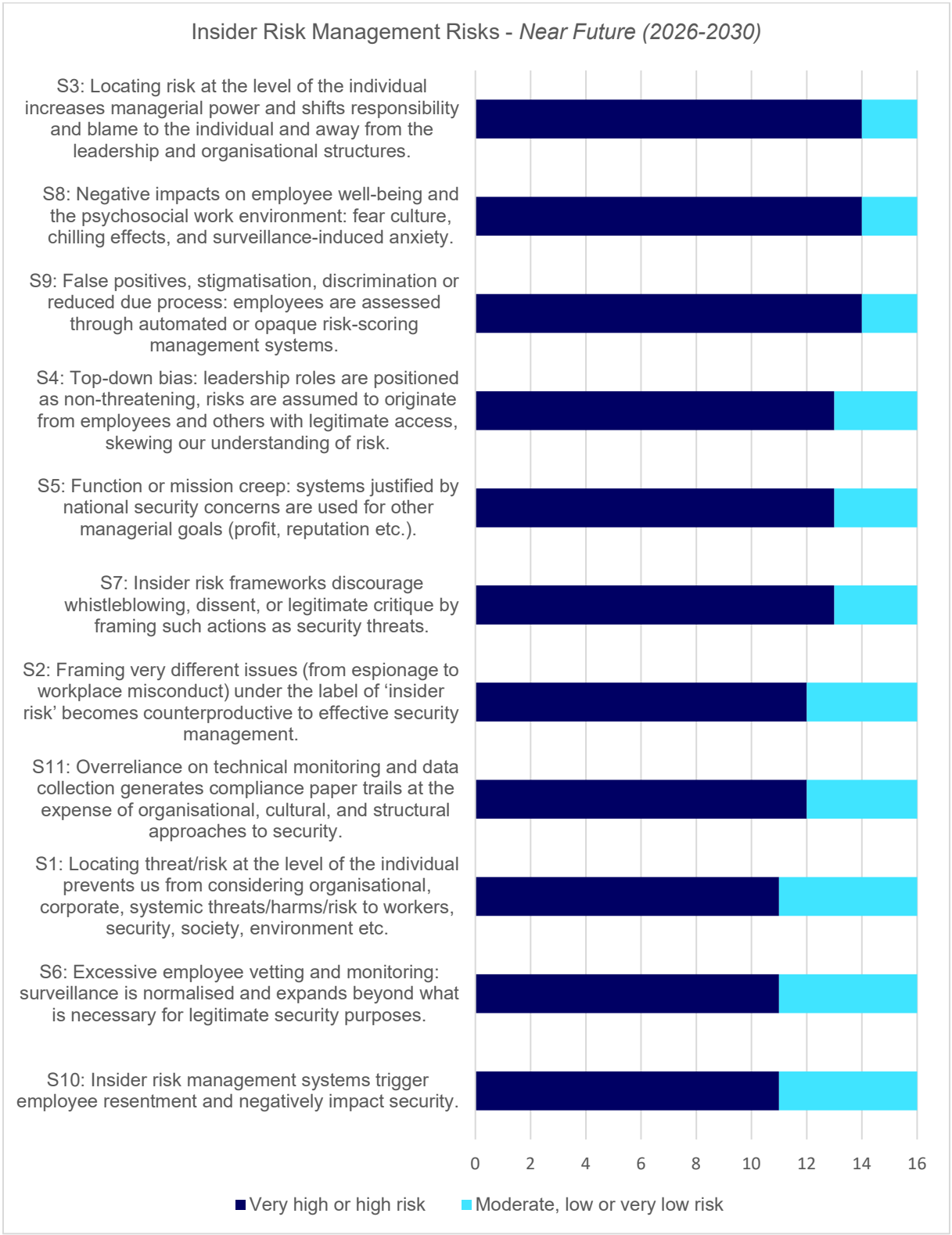

Figure 2-2. Risks Associated with Insider Risk Management – Near Future (2026–2030)

We were keen to understand which of the identified risks were seen as high/very high risks by most of our experts and hence around which concerns the consensus about high levels of risk emerges. We were also interested in what risk dimensions should be considered when implementing these and similar personnel security management practices or crafting alternative paths to security management. Of course, in neither of the risk assessment exercises did we aim or attempt to predict any probabilities. Instead, our goal was to narrow down a long list of possible future risks and understand which ones should be prioritized and theorized as core risks. For full disclosure, prior to assessing these risks, we provided the following background information to the experts:

> 'While national security authorities are concerned with espionage, leaking, sabotage and foreign influence operations, the concept of 'insider risk' as it manifests in today's commercialised managerial practice is being applied to a broad range of 'risks' stemming from people within organisations to these organisations. This goes well beyond concerns related to national security: e.g., sexual harassment, counterproductive workplace behaviour, white-collar crimes, reputational and legal risks, bullying, breach of internal ethical codes, trade secrets and IPR (intellectual property rights) violations. Paul Martin, one of the leading pracademics (practitioner-academic) in the field, argues that insider risk encompasses anyone from 'unwitting insiders' who 'cause persistent low-level harm through poor performance and small acts of rebellion' to 'purposeful insiders with malign intentions' who 'have the potential to cause far greater harm' (Martin, 2024: 1). Insider risk management systems promise to pre-empt and manage all these 'risks' and 'threat scenarios' stemming from individuals with legitimate access to organisations. They rely on automated screening, continuous monitoring, and vendor tools (risk scoring, anomaly detection, behavioural signals) and other intelligence-driven solutions. However, we rarely assess the risks connected to these risk management systems themselves and their consequences. Please assess how significant you consider each of the following potential risks associated with insider risk management.' (from round 2 of the Delphi survey).

The top three risks which 14 out of 16 experts converged upon were around concerns of managerial power in the workplace and the very fundamental premise upon which insider risk management systems are built: 1) the concern about increasing managerial power and shifting responsibility and placing the blame on the individual and, consequently, 2) negative effects on employee well-being and the psychosocial workplace environment, such as chilling effects and surveillance-induced anxiety and 3) the risk of false positives, stigmatization, discrimination as a result of being subject to opaque managerial technologies. Even here, in line with this study's focus on identifying factors which are frequently ignored or overlooked, the experts were asked to provide qualitative responses or elaborate on their assessment of the pre-identified risks. The same top risks were reiterated in the free text:

> 'Like an ouroboros or, in norse mythology, Jörmungandr, the over-focus of organisations on insider threats leads such an organisation to turn onto itself, its head (board of directors, manages) swallowing its tail (employees not high in the managerial hierarchy). Employees are "expendable" – you higher new ones - while the board is "secure/protected" when the focus is (deliberately) misdirected onto the insider.'

> 'The top-down bias is important: leadership roles are positioned as non-threatening while risks are assumed to originate from employees and others with legitimate access to the organisation, skewing our understanding of risk. Research shows that leaders have easier access to overriding internal control and also more to gain. The risk assessment should reflect this.'

As these critical reflections strike at the core premise upon which insider risk management systems are built, we are forced to consider the inherent riskiness of these systems – not a mere 'unintended consequence', but a built-in design feature. This raises the question as to whether these systems need fundamental rethinking – in particular given the broad range of risks of

worker harm associated with them. Here we should remind ourselves that even for those subject to the Security Act, there is a clear requirement under section 1.-1.c of the Act that one is to 'ensure that security measures are implemented in accordance with the fundamental legal principles and values of a democratic society'. Despite this, we see the emergence of problematic security practices and products, which can be experienced as invasive by employees and potentially in conflict with the Equality and Anti-Discrimination Act, DEI policies, data protection legislation, Guidance on Monitoring and Control of Employee's Digital Activities, Collective Agreements or the Working Environment Act. Yet, protecting precisely these the democratic values, enshrined in these laws, is also a key national security interest.

However, the key question is not only whether such systems are legally fit for purpose, as much can be accommodated within existing legal frameworks, but also whether they are epistemically fit for purpose and capable of delivering the security they promise. This requires asking which harms are disavowed, which risks are ignored, and how threats are conceptualised. It also raises the question of whether these systems genuinely serve national security or other objectives, and whose interests they ultimately reflect. All the above, and in particular the top risks point to fundamentally epistemic issues and the question of what forms of knowledge underpins contemporary modes of governance and whose knowledge counts and whose does not. When we speak here of epistemic closure, we go significantly beyond questions of 'bias' or cognition. Often, such as in intelligence studies, discussions circle around tackling 'cognitive closure' and cognitive bias related to individual psychology and psychological mechanisms that are seen as leading to various types of intelligence failure (Hatlebrekke and Smith 2010). Unlike these approaches, we speak of epistemic closure that is linked to socio-political, economic and cultural factors and mechanisms that shape knowledge production within a particular field, creating, over time, insular realities that become difficult to challenge – even despite, such as in the case of security compliance, the widespread consensus on its failures to deliver, and on risks associated with it (in this sense, the 'cognitive closure' literature would be understood as part of this field, privileging a particular understanding of reasons being intelligence failure, at the expense of others). The question that these risk assessments raise is – why, if we agree these risks are high – are we not challenging, but rather perpetuating and tweaking these systems, or even demanding more of the same? Do we lack the future imagination or courage or believe it impossible to break with these established modes of thinking?

Our intention here is not to discredit these approaches, but rather to put them into their proper place and challenge the 'organizational mismeasure' (Hummel 2006) that can emerge when these become (or threaten to become) the dominant mode of thinking about and pre-empting security threats in a society. As mentioned earlier, there are of course individual threat actors, spies and violent individuals capable of both undermining national security and of inflicting serious harm and suffering, but their existence should not overshadow organizational and systemic harms. It should also not overshadow the focus on the causative forces and contextual understandings that could open alternative and more constructive modes of security governance and management. As one expert remarked in round 2 of our Delphi survey:

> 'I believe the security situation in 2035 will be shaped largely by increased Russian activity and further disengagement from the USA. (…) I believe that current and near-future sources of insider threats are likely to remain motivated by individual behaviour than systemic risk. Particularly, I believe that money, coercion and ego are highly likely to remain the motivating factors rather than ideology or systemic pressures. As such, I believe that it is undesirable to move towards systemic solutions to individual issues. This, in my view, is a pattern which has largely remained constant in western security services since the end of the Cold War. I also believe that transparency in workplace security practices is a bad thing, at least in the intelligence context. Knowledge of how a surveillance or monitoring system operates is the key

> enabling factor for an adversary hoping to exploit that system. Secrecy should not be assumed to be negative and transparency always a goal; rather, context is heavily important here.'

The question we raise is rather whether treating everyone as a potential traitor serves security in the long run and what this approach unsees, disavows and ignores when trying to make sense of individuals and/as security threats – i.e. the enormous wealth of contextual knowledge, beyond individual motivations and psychopathology, that becomes defined out of security governance as it becomes translated into managerial practices.

2.3 Implications: Placing Identified Risks into a Future *Context*

Placed in future context, the risks associated with security compliance and insider risk management point toward a broader trajectory in which the regulatory security state seeks to manage uncertainty through intensified monitoring, behavioural analysis and automated classification. Or as one expert put it in the free text form, commenting on the identified risks:

> 'Many of the high risks above are linked to the spread of what is called "audit culture". These trends are amplified in systems that rely on AI and automated mechanisms of regulation.'

We have seen how 'audit culture' (Shore and Wright 2015, 2018) merges with the security discourse, effectively being 'securitized' (Buzan et al. 1998) and this securitization in turn normalized and even banalized (Bigo 2025; Wærp 2024). The likely direction of travel is toward deeper integration of AI into personnel security, anomaly detection and predictive risk scoring (Aradau and Blanke, 2017, Brayne, 2020). In such a context, insider risk programmes are likely to appear increasingly attractive because they promise anticipatory control in environments defined by uncertainty and complexity. Yet this promise rests on a familiar move: recasting irreducible uncertainty as a technical problem to be solved through more data, better models, and more continuous surveillance. The danger is that structural vulnerability is displaced into individual suspicion, while political questions about institutional resilience are reformulated as technical questions of detection, scoring, and intervention.

This trajectory is also likely to deepen the concentration of corporate power within security governance. Generative AI systems are increasingly controlled by a relatively small number of firms that possess not only computational capacity but also significant influence over standards, platforms, and the terms on which digital systems can be accessed and governed. In this setting, dependence on AI is deeply political. In the event that insider risk and compliance architectures become more deeply embedded in privately controlled AI ecosystems, public authorities are likely to find themselves relying on commercial actors not only for tools but for the very data, models, and infrastructures through which security is interpreted and acted upon. This raises the prospect that future security governance becomes more privatised and less open to meaningful public scrutiny, even as it presents itself as more intelligent and more efficient (Aradau and Blanke, 2017, de Goede et al., 2014, Ulbricht, 2018).

The implication is that taking security seriously in the future requires sustained attention to who owns and controls the infrastructures of security knowledge, how platform dependencies shape state capacity, and whether AI-enabled governance strengthens or erodes democratic accountability. Without that wider perspective, the likely result is a more deeply technologised form of dependence, in which public institutions become increasingly reliant on black-boxed systems and concentrated corporate power to govern uncertainty (Zuboff, 2019).

When we asked the experts to evaluate a series of statements on two scales of un/desirable and un/likely in the Round 2 of the Delphi study, an interesting paradox manifested itself very clearly. Namely, there was a systematic mismatch between the future the experts assessed as likely but undesirable and the future they deemed desirable but unlikely. The undesirable but likely future was one where security governance is likely to become even more individualising, intrusive, and compliance-driven, where organisations will increasingly treat people as potential risks, rely on continuous vetting and behavioural monitoring, and delegate judgment to private vendors, consultants, and automated systems. In that likely future, security is defined narrowly around the protection of assets, data, and organisational reputation, while broader structural drivers of harm and insecurity are neglected. The desirable but unlikely future pointed broadly in the opposite direction. They favoured a model of security that is systemic rather than behaviour-centred, participatory rather than top-down, and publicly accountable rather than market-led. In that preferred future, security would address organisational and societal causes and drivers of harm, balance protection with employee rights and autonomy, impose clear limits on monitoring, preserve in-house public expertise, and subject private actors to democratic oversight and substantive accountability. These pointers from the Delphi survey provided an impetus for the next stage of our foresight exercise, during which we built creative future scenarios, intentionally divorced from any concern about their likelihood, but rather conceived as future scenarios good to think with – ideally helping us to break with the aforementioned epistemic closure and re-open a discussion about the very meaning of (national) security.

3 Future Scenarios: The Possibilities and Limits of Security Compliance

Thinking about the future of the regulatory security state (RSS) is no longer a speculative luxury but a strategic imperative. As the preceding analysis has shown, the RSS emerged within a specific historical window – a peace-time characterised by the belief that security could be managed as a matter of market efficiency and governed risk. However, the current situation is defined both by the return of wars and violent conflict and by what has been termed a polycrisis, i.e. a condition where multiple global emergencies are so deeply entangled that the whole is more dangerous and unpredictable than the sum of its parts.

In this context, future scenarios are essential to link the macro and the micro. They allow us to connect the tectonic shifts of global geopolitics and the possibilities of the 'weaponization of interdependence', such as in the case of the Strait of Hormuz (2026), ongoing at the time of writing, where Iran is leveraging its geographical control over this critical maritime chokepoint (the macro) with the granular, techno-bureaucratic compliance rituals and 'insider risk' management systems within individual organisations (the micro). By exploring these scenarios, we seek to break through the 'epistemic closure' that often limits security discourse to technical fixes, forcing a confrontation with the fundamental contradictions of a state that delegates its *raison d'être* to the market.

3.1 Why Build Future Scenarios?

The modern security environment is defined by an unprecedented level of complexity that defies traditional risk-management logic. We are currently navigating a polycrisis that manifests across multiple, overlapping dimensions, where the resurgence of large-scale, inter-state war in Europe re-centres the 'positive state' and military deterrence, directly challenging the RSS's reliance on soft regulatory tools. This shift is further exacerbated by the erosion of the international rules-based order and the rise of geoeconomic confrontation, which has transformed global supply chains into strategic 'chokepoints' and led to the systemic weaponisation of the economy. Simultaneously, the proliferation of hybrid threats, cyber warfare, and AI-driven disinformation campaigns has blurred the lines between war and peace, domestic and foreign, truth and fiction. Finally, environmental and demographic pressures, ranging from climate change to an aging workforce, act as potent threat multipliers that intensify widening inequality and social polarisation. This complexity necessitates a radical expansion of how we conceptualise security. To date, the RSS has functioned primarily through negative visions of security—defined by the avoidance of risk, the mitigation of threats, and the performance of compliance. By exploring the possibilities and limits of security compliance, these scenarios invite us to ask: Is the RSS a durable form of governance, or is it a fragile facade in the face of survival-level threats? Only by imagining these futures now can we hope to steer the state away from an 'illusion of control' and toward a more substantive, legitimate, and holistic model of national and human security.

3.1.1 A Note on Future Scenario Method

The scenarios presented here were developed by the research group during a dedicated full-day workshop following the comprehensive analysis of the two-round Delphi survey. This workshop was underpinned by preparatory analytical work focused on mapping 'weak signals' and identifying a preliminary set of metaphors to serve as catalysts for the group's discussions.

Methodologically, this process is grounded in prospective theorizing – a future-oriented framework dedicated to the active cultivation of desirable futures (Gümüsay and Reinecke 2024). This approach consciously expands the field of inquiry to encompass possible, plausible, and even preposterous eventualities. By moving beyond the traditional research goal of mirroring or illuminating 'what is,' we adopt a generative orientation aimed at 'world-making,' or creating 'what is to become' (Gergen 2015). This perspective recognizes that research is not a neutral observer of a fixed reality but a 'future forming' endeavour that can proactively transform its subject matter. Because the future cannot be captured by mere linear projections from the present, this approach requires the active production of social imaginaries that allow us to exaggerate, explore, and decisively break with established narratives.

The process began with reflections on the synthesised results of the Delphi expert surveys, in particular with an eye to the emerging trends and contradictions that have informed our creative process. Below, in 3.1.2. we summarize some of these emerging issues and drivers of change that we considered when developing these scenarios (Inayatullah, Sohail 2004) (see 3.1.2.). To the future scenarios, we employed metaphors as generative tools for theorising (Boxenbaum and Rouleau 2011; Cornelissen 2005). Metaphors allow for 'conceptual blending,' fusing the realms of lived experience with radical imagination to create semantic innovation, and stimulate the emergence of new perspectives and conceptualizations of the problem at hand. By doing so, 'the resulting image and meaning is creative' (Cornelissen 2005, 751), allowing us to articulate complex systemic shifts – such as in the first scenario we present below, 'Potemkin Village' (3.2.1.) – that might otherwise remain abstract.

All forms of theorising involve a 'conceptual leap' from observed phenomena to theoretical constructs (Cornelissen et al., 2021). Our objective was to reach beyond narrow disciplinary or professional frameworks to explore different forms of knowledge and experience. Rather than presenting these scenarios as authoritative, methodologically vetted models that seek to represent reality as it currently exists, we envision them as generative outputs. They are designed to stimulate discussion, provoke debate, and engage practitioners in imaginative accounts of what the future could be. In this sense, we follow Gümüsay and Reinecke (2024) in recasting science as a useful perspective to 'understand how humans could collectively evolve intelligent yet democratic ways of organising in the face of complexity and uncertainty' (Farjoun et al., 2015, p. 1789). Before we proceed to the scenarios we developed, let us briefly summarize the 'weak signals' we identified across the two-round Delphi survey.

3.1.2 'Let's See Where Clues are Leading'[71]: Trends and Contradictions Toward 2040

In the round 1 of the Delphi survey, we asked our experts to evaluate a series of statements on possible future developments on two scales, on whether they consider them desirable or undesirable and likely or unlikely in the near future (2026–2035). We also asked the experts to evaluate a series of statements concerning possible future shifts in power and agency, assessing whether they considered these developments thinkable or unthinkable by 2040. These evaluations provided useful insights into both widely recognised drivers of change and emerging issues, as well as the boundaries of what is currently considered thinkable. We summarise these findings here, as they informed our scenario development, even where we deliberately sought to move beyond them and challenge those perceived limits. While there was some disagreement about likelihood, there were clear majorities when it came to desirability. Hence, we decided to orient our thinking about the assessment of the un/desirability of certain futures, with likelihood being a secondary consideration.

[71] A line borrowed from the song 'Panopticom' by Peter Gabriel (2023).

The most important finding of this exercise was how *undesirable* the experts found the continuation of the current trends, which they also generally assessed as *likely.* The statements that follow synthesise the collective assessments of the surveyed experts. They are presented in the present tense for analytical clarity but should be understood as reflecting aggregated judgements about likely and desirable future developments rather than definitive claims about the future. Globally and geopolitically, the Fukuyaman end of history has ended (Hochuli 2021). The rules-based international order is replaced by great power rivalry (the expert group was undetermined whether it would be a bipolar world dominated by the US and China). Economic interdependence is weaponized through regulatory tools, sanctions, and tariffs. The disruption of supply chains fosters further deglobalization, derisking and nationalizing of production. As regards the RSS, if we put the statements deemed undesirable and likely together, a self-reinforcing logic emerges. The private security market is expanding, and more private actors are involved in security provision. Public-private partnerships dominate security governance at all levels (organization, state, society, international). Technical and security experts continue to exert epistemic authority and determine the shape of security governance and 'best practice'. This epistemic authority feeds on general geopolitical insecurity as well as AI-fuelled disinformation, information warfare and destabilization of knowledge production.

Accordingly, the RSS continues to rely on delegating security authority to organizations, technical experts, consultants, and market actors (multinational BigTech, security companies, audit firms), expanding their power over citizens, organizations and policy development. The consequence is that technical, managerial and surveillance-, data-, and intelligence-driven solutions are preferred and focused on targeting risks, threats and unwanted future events. Many of the experts even agreed that regulatory capture by monopolistic actors that set the terms of governance will be normalized and distinguishing between the state and the market becomes obsolete.

On the other hand, within the stipulated time frame, the experts generally did not foresee an extension of these undesired tendencies to their logical conclusion. While there was no consensus on the possible fracturing of NATO, its *dissolution* was regarded as unlikely, as was a Russian invasion of European countries other than Ukraine. Most experts disputed the statement that the nation state, after a short period of reassertion, would lose its relevance. Values that at the time of writing were cherished as central to liberal democracy and the 'Norwegian model' were deemed rather resilient. The death of the welfare states, with all services becoming private, was considered unlikely, and concepts such as public interest, privacy, proportionality, legitimacy and accountability, public debate and liberty were not believed to lose their appeal to citizens. Notions such as citizen(ship), public interest, and democratic representation would retain their place in public debate, as per the consensus. On the other hand, while regarding the state's 'monopoly on violence' as desirable, there was disagreement about whether that concept would be relegated to the history books. Also, there was no consensus on whether the state would be outcompeted by corporations and multinationals in security provision.

On the optimistic side, the desirable outcome of a reassertion of the nation state and the formation of new alliances in a multilateral world was seen as a likely one. The question whether that would *replace* the bipolar world order, remained contested. The desirable event of small states reasserting themselves as norm and value-entrepreneurs reshaping global governance in face of polycrises was rejected as unlikely, even if desirable. Some experts regarded the likely emergence of new global coalitions outside of existing structures (e.g. UN) as desirable, but others disagreed. The climate crisis and material limitations of the planet will, according to expert consensus, force alternative modes of organizing society and economy. The experts would welcome such a development and would prefer an alternative to neoliberal governance and a shift of power from RSS to the positive state (military, politics), although the likelihood of these

two outcomes was contested. The same applies to the global emergence of indigenous and popular protest movements amidst climate uncertainty, security threats and collapsing economy.

On the other hand, the increasing replacement of free market policies by resource nationalism and direct national control over industries was seen as likely, but its desirability was contested. The experts would welcome a lively public debate about security politics and how to build secure societies but could not agree on whether that was likely to happen or not. Moreover, while seeing open discussion and social dialogue about security management within organizations (e.g., trade unions and workers involved) as desirable, the expert group was undecided as to whether this was likely. Perhaps most pessimistically, it was not deemed likely that proportionality, privacy, legitimacy and accountability, liberty and other values would become central guiding principles in security governance.

But we also asked the experts what they deem thinkable and unthinkable in respect to shifts in power and agency towards 2040 (see Figure 3.1). When assessing the table in Figure 3.1, it is important to note that 'thinkable' is *not* the same as 'likely'. The terms can appear at first synonyms, but whereas the latter has a close connection to probability, the former has strong connotations of potentiality. In this way, this part of the exercise is more open, uncovering the perceived possibilities of the future – negative as well as positive.

From these responses we can gauge that the experts imagine the potential for the position of the state to be strengthened. According to most of the experts, it remains thinkable that states will reassert control over the economy, resources and production, which will be the main source of power. Military power and deterrence will remain the defining form of power, whereas only a minority of the experts considered it thinkable that the needs of the positive state will diminish as multinational corporations and financial institutions establish their own militaries. Still, a majority of the experts found it thinkable that corporate control over natural resources, manufacturing, and value chains will be a defining form of power. Nevertheless, whether we will see a profound shift of power towards the regulatory state is a contested issue, as is the thinkability of supranational bodies and governance superseding the state. Perhaps most strikingly, there is a strong belief in the mobilizational potential of citizens, against the state, supranational governance, or, most prominently, against corporate power. Put even more briefly and simply, within the horizon of the thinkable the positive state is resurgent, the RSS will not grow perpetually, corporate power is not unlimited, and active citizenship is still alive and thriving.

Departing from what was regarded as desirable in the previous part, there is more optimism here, or at least hope. The thinkability of the most undesirable scenarios is contested. Against this background, the thinkability of popular mobilization is puzzling: why would people mobilize and even self-organize alternative societies if things are not that bad? One expert commented with the following statement in the free text:

> 'One often overlooked factor is the resilience of institutional and ideological frameworks even during periods of crisis. Political and economic systems rarely transform rapidly, even when structural pressures intensify. Instead, existing governance models tend to adapt incrementally, producing changes at the margins rather than systemic transformation in the short term. This path dependency suggests that expectations of rapid alternatives emerging within a decade may be unrealistic. A second factor is the relationship between social instability and perceived legitimacy of governance. Rising inequality, climate pressures, and economic uncertainty may generate protest movements and political mobilisation, but these developments do not necessarily translate into coherent alternative systems. Instability can coexist with institutional continuity, particularly when dominant actors retain economic and political influence.'

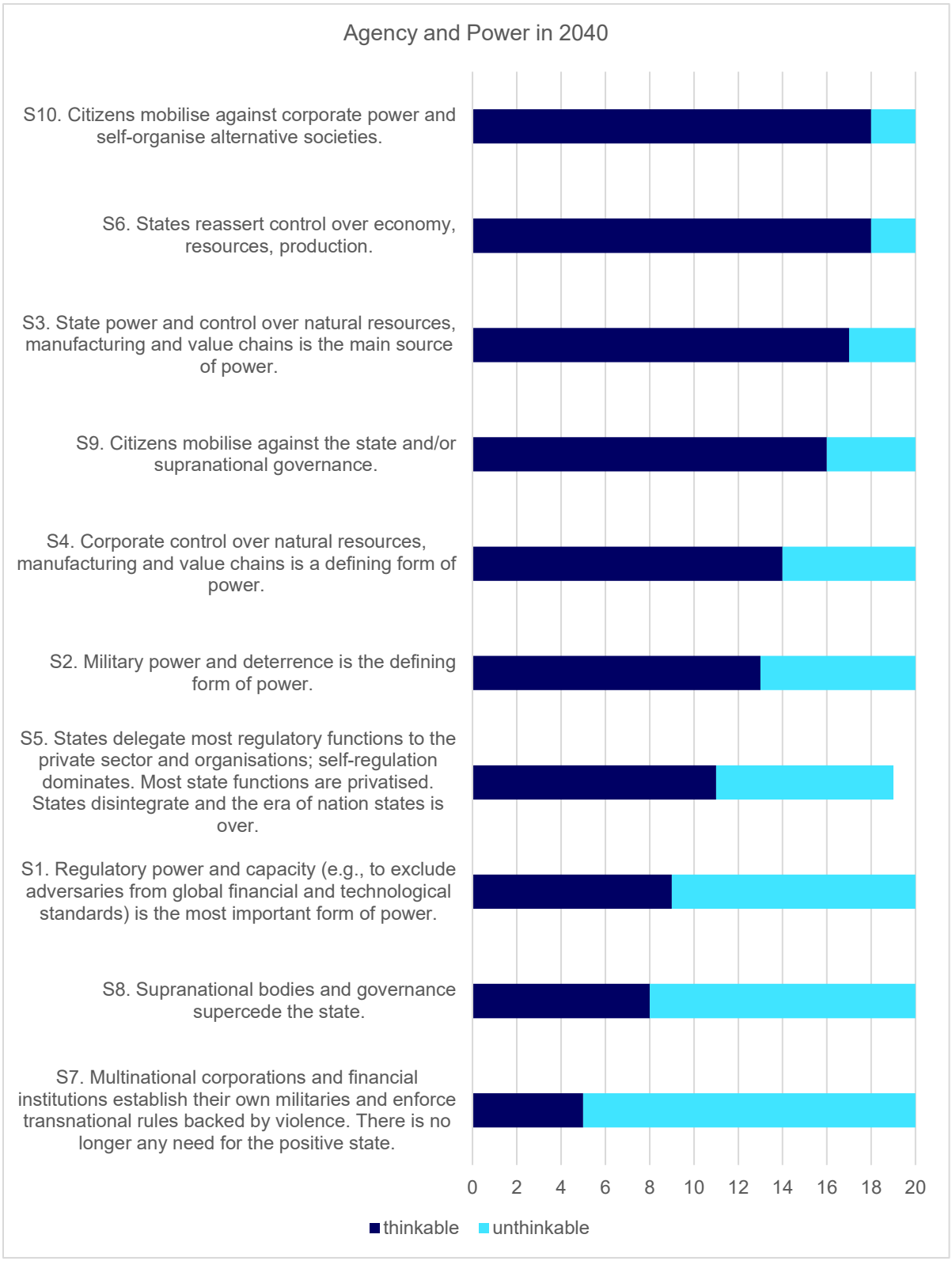

Figure 3-1. Expert opinion on power shifts by 2040, ranked from the most to least thinkable.[72]

[72] 1 respondent was excluded from the original 21 as both categories were ticked simultaneously in all statements, question 5 excluded one additional respondent who also chose both options, hence 19 respondents on question 5

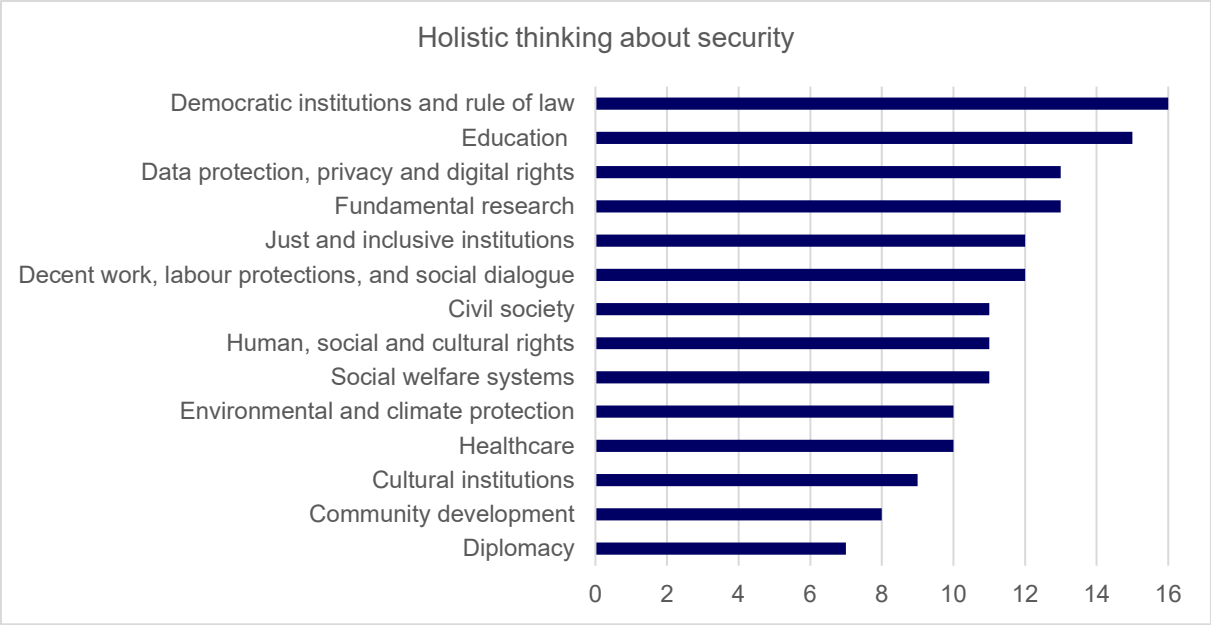

Figure 3-2. Holistic thinking about security: what should be funded and invested in?

In the second round of our Delphi survey, we also asked the experts where funding should be channelled if we were to approach security more holistically. The answers are ranked in Figure 3.2. with democratic institutions and rule of law on top, followed by education, data protection and digital rights, and fundamental research. Again, the top four priorities mirror the fears of the hollowing out of the democratic institutions, the disproportionate power of Big Tech and concerns about knowledge production – these hints are suggestive of the fundamental relation between power and knowledge, and whose ideas and interests are shaping the societies we live in. One expert commented in the free text:

> 'I have ticked all of the above and agree that dominant approaches towards security protection are reactive, threat-centric and technocratic. I also acknowledge that the world is becoming a far more dangerous place; democratic backsliding, the resurgence of far right, the return of imperialist thinking, and the rise of neofascist regimes in many countries means that security is under threat. Some level of reaction is necessary. The key challenge is how to balance those "threats and technocratic solutions" with other, more progressive, inclusive and democratic forms of regulation and accountability.'

This provides a pointer as to what is desired and perceived as necessary if we are to approach security more holistically. The concerns relate to our failure to do so. Moreover, from what we can read across this Delphi study, the most undesirable outcomes consisted simply in the extension of today's negative tendencies to their logical extreme. The next section will do just that. Essentially an exercise in 'forced thinkability', it starts where the Delphi ends.

3.2 Between the Map and the Territory: Speculative Trajectories of the Security State

In the following, we will present four scenarios that serve as conceptual stress tests for the regulatory security state, linking the macro-dynamics of global polycrisis with the micro-realities of organisational compliance. While they employ the language of fiction and metaphor to break through current 'epistemic closure', they are rooted in our Delphi expert surveys, literature on the

regulatory state and our previous and ongoing research. They are not intended as predictions of what *will* happen, but as provocative inquiries designed to expose the logical conclusions of current trends. By framing empirical data within speculative accounts, we invite the reader to look past the 'illusion of control' and engage with the fundamental political and normative questions that will define the security of tomorrow.

3.2.1 Scenario 1: Potemkin World

In the Potemkin World, states seemingly remain the foundational entities of the international system. However, they have been captured by the Regulatory Oligopoly, consisting of huge Tech and Audit companies. In the Regulatory Republic of Norway, domestic political institutions still exist, but they are integrated in the 'regulatory loop', with decisions being made and regulations updated by AI. As a rule, states still have laws and nominal constitutions, but these are said to have been integrated in the regulations, and their original letter and spirit are generally forgotten. Social problems, unrest, and environmental damage are persistent and increasing. These issues are not addressed directly, but through regulations, as direct measures addressing causes are deemed too expensive. There is a 'regulatory divide' between white-collar employees responsible for keeping the regulatory machinery going, and menial workers as well as unemployed residing in favelas outside the regulated zones, as the AI driven background check programme has denied them access due to risks and vulnerabilities such as connections to other countries, difficult family situation, financial problems, health issues, psychological risk factors, or other determinants. The background check programme reaches its conclusions after an all-encompassing analysis of social media, bank accounts, health data, physical locations, culture consumption, and conversational data. Those deemed risky or vulnerable are expelled, left to an existence in the 'regulatory exhaust', i.e. the flow of social and environmental harm from which the regulated ones (known colloquially as the 'regs') are shielded. 'The externals', as the out-regulated ones are called, are discontent with this existence, and social unrest is brewing. The regs, who are by now in a minority, respond by generating more regulations, effectively pushing more people out of white-collar work in the regulated zones and into unemployment in the favelas. The Regulatory Republic of Norway, most notably its data centres, has long been subject to hacker attacks and drone surveillance from the neighbouring Eurasian Regulatory Autocracy (ERA). Not deeming this sufficient for a kinetic response, Norwegian regulators, following global best practice, respond with a new complex of regulations, mappings of critical infrastructure, exclusion of second-generation Eurasian immigrants (first-generation ones have long been expelled) and, by extension, also first-generation immigrants from ERA's neighbouring countries, from the ranks of the regs. The authorities also increase the amount of water and food every reg is required to keep in their house to a two-week supply, as opposed to the previous requirement of ten days.

The Potemkin World is reached by extending and intensifying the tendencies of the current regulatory state, taking them to their logical extreme. This mental exercise is useful not only because it may tell us where we are headed, but also because it highlights where we are. The name derives from accounts that Count Grigory Potemkin allegedly had fake façades built to impress Russian Empress Catherine the Great on her 1787 journey to the newly captured region to the north of the Black Sea, providing an illusion of affluence. Since then, 'Potemkin' has come to denote anything (beautiful) that is hiding an (ugly) reality. In this report, we use it in an even more extreme sense – to illustrate how regulations simply have become 'reality', hiding the physical reality from all sides at once.

In this scenario, Big Tech and Big Audit have merged, having continually sold their allegedly cost-effective solutions ostensibly guaranteeing security to other actors, including the states

themselves, thereby gradually taken over their functions, reshaping them in the process, strangling politics, law, and society as such. The positive state with its rule of law has withered away, and the regulatory state is in this sense complete. Citizen rights are no longer relevant, as people, as far as the regulatory state is concerned, exist only as data to be extracted for profit. Regulations are continually updated, expanded, and perfected by AI, loopholes seemingly closed, digital compliance paper trails generated. Not only are human discretion and agency reduced to a bare minimum, but humans can no longer understand how and why decisions are reached or partake meaningfully in rulemaking. They can ask the systems for an explanation, but the answer they generate will, although plausibly formulated, likely have little or no connection with 'reality'. The total reliance on automated systems has resulted in epistemic capture. Whereas the original Potemkin villages were one-dimensional, with just simple fake façades, the regulatory state is a multi-level, multi-dimensional, and ever-developing Leviathan of illusions and hallucinations. The total dominance of the regulations and the fetishization of digital solutions have led to the negligence of physical reality. What is 'true' or 'actually existing' has become largely irrelevant to the inner logic of the regulatory complex. The worship of the digital, the automatized, the formal, and the procedural has gone so far as to disrupt the connection between representation and reality, resulting in layers of self-referring regulations. Whereas at earlier stages, the regulations might have actually contributed somehow to physical security, at the mature stage, they contribute only to ontological security: they reinforce our notion of being technologically advanced and taken care of. Indeed, we become so preoccupied with closing and patching tiny loopholes in the regulations that we risk falling into the physical crater in the real world. Craters and other dangers are still there, only that we have lost sight of them, as the regulatory map has become more important than the terrain. This logic also pertains to other risks or threats, of course.

On the one hand, Potemkin World is the most likely scenario, but on the other, it is also temporary, since it is not sustainable. First, it inherently implies the concealment of physical realities that are bound to resurface – reality will strike back, whether in the form of war, social unrest, or environmental damage. Second, its inner dynamics lead to accelerated automation and destabilization of knowledge as such, potentially posing a threat to physical reality – humanity and the environment. Third, it relies on highly energy-demanding technologies (computer centres) that are vulnerable to physical shocks (war, natural disasters, sabotage).

3.2.2 Scenario 2: Open Panopticom

In the Open Panopticom, a popular rebellion has turned the Potemkin World upside down. The Potemkin façade had started crumbling after environmental disasters and hybrid attacks revealed that the regulatory oligopoly had built an illusion of security through its AI-driven compliance systems. The regs, who realized that it was all a fiction, aligned with the long resentful externals. Charismatic, anti-establishment, tech-savvy politician-activists in the mould of the late Aleksei Navalny and Volodymyr Zelensky joined forces with regs and specialists defected from Big Tech, Big Audit, and the public bodies of the regulatory state to create a global popular campaign by joining existing 'pirate parties' and anti-corruption movements, using digital platforms for mobilization. After a massive rebellion, the regulatory state still governs, its systems largely intact, churning out regulations, but faced with public discontent, it has succumbed to popular demands of radical transparency. Legal documents such as the Norwegian Security Act have been superseded by the 'Universal Transparency Mandate.' Every procurement contract, every intelligence assessment, and every automated risk-score is reviewed by a global network of citizens and independent analysts. The unelected technocrats and corporate actors of the Potemkin World have lost their epistemic monopoly to meta-national forensic collectives. These borderless actors also monitor the 'chokepoints' of the global economy, ensuring that no state or

corporation can weaponize interdependence. In the beginning, this monitoring was done on a voluntary basis, mostly by externals, as they were seen as most qualified. Later, it became professionalized, taking an enormous amount of resources as a new oligopoly known as Big Transparency took shape, with four huge corporations dividing the forensic market between them. Increasingly, the monitoring work was automatized. As regulation and compliance were already automatized, this put an enormous strain on the computer centres and the energy infrastructure. Externally, the Eurasian Regulatory Autocracy is suspected of spying on Norwegian monitoring in order to map strategic vulnerabilities. Moreover, in order to hide its military manoeuvring, the Eurasians have responded by establishing 'dark zones' – physical territories where all digital signals are jammed, creating a new iron curtain of total data-silence where Panopticom cannot reach.

The Open Panopticom takes its name and conceptual departure from the idea pioneered by musician and activist Peter Gabriel, who envisioned an infinitely expandable and accessible ‘data globe’ designed to allow the world to see itself better and understand ‘what is really going on’. Etymologically, the term references Jeremy Bentham’s eighteenth-century Panopticon – a prison architecture where the few observe the many – but inverts its logic through the suffix ‘com,’ signifying communication.

Technosolutionism is still intact and the tools of the regulatory security state were not abandoned, only seized, deconstructed, and redirected by the governed. Inspired by the investigative methodologies of forensic collectives such as Forensic Architecture and Bellingcat, as well as the human rights work of WITNESS, this scenario imagines a world where surveillance has been turned on its head: a system of ‘sousveillance’ where the many observe the actions of the authorities. Instead of an automated system screening citizens for ‘insider risk,’ the public begins to use the same digital infrastructures to monitor the regulators themselves. In this process, the ‘externals’ are re-integrated as ‘agents of truth’; their lived experience of physical reality becomes the primary source of ‘ground-truth’ verification, countering the state’s official reports that in the mature Potemkin stage lacked any grounding in material reality. However, this order is also unsustainable and creates its own tensions. Privacy has become obsolete, sacrificed at the altar of collective accountability. The Panopticom has become a glass house where secrecy has been replaced by the tyranny of the visible.

3.2.3 Scenario 3: Primordial Oligarchy

Both the Potemkin World and the Open Panopticom rely on ever-increasing processing of data, which depends on highly complex software, vulnerable digital infrastructure and energy-intensive data centres. In the Primordial Oligarchy, either the regulatory complex of the Potemkin World or the forensic complex of the Open Panopticom has collapsed under its own weight, as the result of external shock, or a combination of the two. In the Primordial Oligarchy, the world is essentially a battlefield of the war of all against all. The state system has disintegrated, with armed gangs fighting over spoils, resources, and territory. The Internet as such is down, as the gangs are unable to agree on who is to run the infrastructure, and most computer centres are damaged by hacking, sabotage, and lack of maintenance. Simple and durable technologies are the only ones that function. That also goes for weaponry, as most tanks, missiles, and fighting planes are now useless, since they also relied on digital infrastructure. The former ‘regs’ are diminishing in number, as their managerial peace-time upbringing has left them with practically no skills that are transferable to the primordial oligarchic order. Incompetent food-gatherers and unable to form alliances and even sense physical danger (having relied on risk management systems their entire lives), they struggle to survive physically. They often refuse to drink even pristine spring water, as there are no available records of who have had access to it previously. Sometimes, they stumble

into craters in the ground, insisting that it was not on the map. Moreover, their language and demeanour are largely incomprehensible to the former ‘externals’. Their criticism of the tribe’s lack of risk assessments and their incessant demand of background checks of all tribe members frequently leads to their being excluded from the communities altogether. Violence is endemic, both between and within the gang-based communities. However, as time passes, territory and resources are divided between gang leaders, and a more stable stage is reached. Gang leaders discover that in order to increase their power, popularity, and even their posthumous memory and symbolic immortality, they must provide the population on their territory with security from external threats, basic goods such as housing, food, water, and clothing, and also a sense of belonging and meaning. Some oligarchs, as they are now called, even start supporting culture.

Primordial Oligarchy represents the return of raw physical reality, as the regulatory system of the Potemkin World has been unable to sustain itself. The latter’s rupture between representation and reality can only be temporary. Although people are fed the shiny and clean-looking regulations and assured that everything is fine, physical reality is bound to return with vengeance if or when the discrepancy is too enormous to be ignored. This can to a degree be compared to, for instance, the decaying Soviet Union, where the communist ideology had lost all dynamism and become ossified, with the official discourse formalistic, stiff yet notionally utopian-optimistic, growing completely inadequate to describe the physical reality of consumer shortage, alcoholism, environmental damage, and general despair.

Primordial Oligarchy is the result of civilizational collapse, as we have seen throughout history, the most notable example being the collapse of the Roman Empire, leading to the Dark Ages in Europe. A future analogy here would be sheep grazing in Silicon Valley or Central Park and armed bands pillaging what they can find. A less extreme form of civilizational collapse is the 1991 collapse of the Soviet Union. Like the dissolution of the Communist system, the fall of the Potemkin State will likely result in a primordial state of nature, unleashing a ‘war’ of all against all.

Although we can imagine the fall of a not yet fully developed regulatory state, we depart here from an extreme version of the scenario, i.e. one resulting from the fall of the mature Potemkin World as described above. Whereas traditional laws are at least in principle based on human common sense, the regulations of the Potemkin World are the product of partisan and commercial interests masked as common sense or common good, moreover, they are unknowable for the human mind (and even for its creator, the AI) and of course fundamentally reliant on technology and data centres. With external shock, internal meltdown, or both, the regulatory systems become defunct and unable to pacify the populations. At this stage, law, as it was previously known, is long gone, therefore notional anarchy and widespread violence will likely be the result. Those with access to manpower and weapons will become engaged in the battle for natural resources and territory. In order to gain the loyalty of people, aspiring oligarchs must guarantee them basic goods such as food, water, and shelter, and basic needs such as physical security (protection from attackers), a (more or less) meaningful place in society, and a modicum of hope for the future. An oligarch hoping to rise from the status of criminal ‘authority’ or warlord to a statesman of sorts will need to provide a primitive version of the welfare state. Although Primordial Oligarchy is hardly a model to emulate for liberal democracies, this insight is important to keep in mind, especially as we presently see politicians’ repeated juxtaposition of the welfare state and the ‘warfare state’.

3.2.4 Scenario 4: Pragmatic-Idealistic Naiveté

The Pragmatic-Idealistic Naiveté inverts the relationship between 'the good life' and risks/threats familiar from the Potemkin World. Instead of attaining the goal (an undefined good life) indirectly, by eradicating all evils, in the pragmatic-idealistic naiveté we focus on the good life – sovereignty, meaningful relationships, the common good, community, individual freedom, culture, social and physical security and social and environmental sustainability. The consciousness about what we actually are protecting and defending therefore increases our ability to protect and defend. This scenario represents the resurgence of the positive security state, which has regained its epistemic authority and expanded its horizons of imagination. Democratically elected political institutions make political decisions, which are subsequently implemented by dedicated public servants. The democratic state controls what remains of the private security sector, deciding what it needs from private actors on a basis of political decisions and the advice from public servants, not based on the advice of the private actors themselves. National security is clearly defined as the security of the nation state, not the sum of the self-centred and mercenary interests of commercial and other organisations/institutions. The rule of law is absolute. Security clearances and background checks are reserved for crucial security functions in the military and national security sphere, cf. the strict definition of national security. Immigrants and minorities are included in all spheres of economic and social life, primarily because society and working life are inherently inclusive. The positive security state uses digital technology on a minimalist-utilitarian basis; in all cases, the least technological solution should be considered first, as opposed to the Potemkin World's technology-first maxim. The military is well funded, well organized, and limits the outsourcing of its needs to private actors to a minimum. The police are well funded, well educated, and maintain a public presence and local anchoring in addition to possessing the resources and updated skills to combat modern forms of crime. An adequate welfare state and a strong public sector guarantee free healthcare for all and a social safety net for those who are disabled or unemployed. Education and culture for all are seen together and as goals in themselves, not just means to solve technical problems or entertainment. National and local cultural institutions such as libraries are strengthened. There is a lively but enlightened debate on issues of national security. This is facilitated by the elevation of the quality of education brought about by introducing the Humboldtian enlightenment ideal, replacing the reigning utilitarian approach to education and cultural life. The regs are offered back-to-life rehabilitation programmes in order to reintegrate them into meaningful human activity. Hopeless cases are given digital sandboxes, consisting of gaming areas, that is free-space office landscapes where they are allowed to simulate regulation. Since their working life was completely virtual and unrelated to physical reality anyway, they are expected to deal well with the situation.

This scenario represents an active choice in distinction to the first three scenarios' respective trajectories of total surveillance, total sousveillance, and systemic collapse; it is born from a conscious rupture of the epistemic closure that once limited security to technical fixes. It is triggered by a collective movement that recognizes that the 'illusions of compliance' and Big Tech dominance have failed to provide material safety, leading to a rejection of both the digital hallucinations of the Potemkin World, the total exposure of the Open Panopticom, and avoiding the collapse ushering into Primordial Oligarchy.

On the one hand, this scenario is *pragmatic* because it refrains from catch-all ideological solutions. On the other hand, it is idealistic, because it identifies *positive* visions for the future. Primordial oligarchy is obviously quintessentially realist, but whereas the Potemkin World and the Open Panopticom are rife with utopian statements sold by Big Tech and Big Audit, these 'visions' are all *negative* ones, offering merely the absence of various evils that their technological solutions ostensibly will eradicate. The dearth of positive visions, or else, visions of what we

actually want, leads to the baby being thrown out with the bath water, as we saw in the Potemkin World. The ‘evil-eradicating’ solutions risk attacking the body instead of the ‘disease’, to extend the illness metaphor sometimes used to market these solutions. More to the point, the regulatory solutions might simply reproduce the very causes of the evils. That would at least be in their commercial interest, since it ensures that they are perpetually needed.

Naiveté is a prerequisite for trust. It is a deeply human trait, arguably as important as suspicion, which of course is an important device for humans to stay secure. But to thrive and flourish, humans need trust, and by extension naiveté. In many ways, Primordial Oligarchy is fuelled by suspicion, but aspiring oligarchs need to inspire trust in order to expand their power. The Potemkin World by contrast, has institutionalized and hardwired suspicion in the very fabric of what passes as ‘society’, in the form of surveillance and regulatory systems. Everything is checked, controlled, and transparent, but only in one direction. Paradoxically, the regulatory state demands trust from people and has risen to prominence not least thanks to their naiveté. Panopticom only inverts this with its radical transparency, which makes trust and naiveté meaningless. By contrast, the naiveté of the present scenario presupposes a degree of opacity. In its less extreme form, this scenario marks a fundamental return to the foundations of a positive security state, where the ‘tyranny of regulation’ is dismantled in favour of the rule of law and an inclusive society. While critics may dismiss this vision as ‘utopian’ or detached from the harsh realities of 2035, the true utopia, in the worst sense, or else, a dangerous delusion removed from material reality, is the Big Tech fantasy of algorithmic perfection. By contrast, Pragmatic-Idealistic Naiveté chooses to anchor security in the ‘real world’ of the civic realm, dismissing the juxtaposition of the welfare state and the warfare state. Only a state for the people, by the people, can be a durable defence against the complexities of the polycrisis.

3.3 Towards Critical Futures Thinking and Holistic Approaches in Security Policy

It is time to draw a few conclusions. Reading across this report, a certain paradigm of security which appears to have come to dominate our horizon of imagination emerges – one that is driven by a reductive imaginary of security threats, accompanied by equally reductive market-driven approaches to their ‘management’. The experts largely agreed on the inherent flaws and weaknesses of the regulatory logic, security compliance, and the security epistemologies, exemplified by the case of insider risk management – we have thought these to their logical extreme when engaging in our ‘forced thinkability’ scenario exercise.

If we lift our gaze beyond the logic of the regulatory security state that we took as our starting point, we realize that these approaches are not only reductive in their approaches and understanding – suffering of what we have identified as epistemic closure – but they are also fundamentally oriented around *anticipating, pre-empting, managing and combatting that which we do not want*. Or else, they are oriented around the *negative*. Using a theoretical lens, they can be understood as technologies underpinned by and operationalizing the logic of ‘anti-policies’ (Walters 2008; Kuldova, Østbø, and Raymen 2024; Kuldova, Østbø, and Shore 2024). Anti-policies have proliferated in a number of areas of the governance of the social: from anti-corruption, anti-money laundering, anti-trafficking, anti-terrorism, to anti-harassment or anti-doping. These policies easily create multistakeholder consensus, but the proper question to be asking here is – *what are we for when we are against these phenomena*? That question focuses us on what is being done in the name of combatting these unwanted phenomena; it focuses us on the proposed and implemented solutions, on the power relations and interests they reflect, as

it is here that disagreements would quickly surface. Yet, this central, political, question is often pushed into the background, at the same time as the overall anti-policy framing remains unchallenged. There is a fundamental difference whether a policy is oriented around a negative goal, such as combatting or eliminating threats, or whether it is oriented around a positive goal, such as human security. The latter is typically underpinned by a larger vision of the collective or public good that is to be achieved, and one is forced to think far harder about how such good is to be pursued in practice. Working towards security in this positive sense would open up two discussions: 1) what is security and 2) how to go about achieving it. These are fundamentally political questions, the answers to which are far from given but differ across periods, space, and cultures and have always been historically contingent (Duffield 2013; Folkers 2017b). What anti-policies achieve is taking these questions out from the realm of public debate and politics and placing them (if at all) in the realm of narrow technical expertise, generating 'best practices' and 'standards', which, as we have attempted to show, risk creating serious epistemic closure, blind spots and epistemic capture by actors with vested interests and disproportionate power. To exemplify this, in the negative discourse, security is reduced to a mere *absence* (or at best successful management) of threats, harms and risks; but in the realm of the social, an absence of a negative does not automatically equal a positive. There is a great difference between reproducing 'bare life' (Agamben 1998) and creating 'a life worth living' (Pfaller 2011). As the expert opinion in our Delphi study shows as well, we do expect and should demand more of security than mere absence of the negative.

But you may be wondering, are we not doing that already? We started this report with the desire of the regulatory security state – embodied in visions of 'total defence' – to align and enlist everyone in the service of national security. Within this vision, and given the threats we are facing, we all should, we are told, pull in the *same* direction – state, private sector, academia, non-governmental and other organizations; regulation and security compliance are just cost-effective tools to achieve this goal by adding slight pressure and more direction to those who do not do fall in line voluntarily and/or may be deemed particularly vulnerable. National security appears here at the first sight as a positive goal, spanning from territorial sovereignty to the protection of democratic values and our 'way of life'. However, its uncanny transformation into yet another anti-policy takes place, as we have seen, as it becomes *operationalized* and translated into security compliance and organizational practices. This is precisely why we cannot rest on the laurels of policy and legal analysis but must also turn to the sociology and anthropology of law, security and organizations.

We have seen how 'national security' becomes translated into threat-based risk management – in different shapes and forms and re-oriented around reducing risks to one's *organization*, the nation taking a backseat. As national security trickles down into the organization, it takes the form of 'technological solutionism' (Morozov 2013) where perpetual security innovations are seen as a fix for insecurity (Haddad et al. 2024). And what of the alignment and shared direction? Is it real or a mere fantasy if responsibility is delegated to organizations that do their own assessments, protect their own assets and interests and implement narrow inward-gazing security management practices and technologies?

(National) security becomes translated into the logic of business continuity and an illusion of alignment is created. This is not accidental, but again, a historically contingent development of particular security approaches. The Security Act, to return to our starting point, cares first and foremost about the protection of critical 'assets' and 'vital functions' from threat actors, about minimization of any disruption of business operations and about ensuring continuity of government (people benefit as a by-product, insofar as business continuity is ensured). These approaches to critical infrastructure and vital functions protection, or 'vital systems security' can

be traced back to the Cold War – and, yet again, to the trend-setting US context of security management (Collier and Lakoff 2015). Over time, they have been appropriated into corporate management strategies as well as the offerings of the Big Four consulting and audit firms and their likes with the primary goal of securing profit, rather than (national) security. They have been incorporated into various standards[73] and, after zigzags of translations back and forth, fed into various national laws, regulations and guidelines.[74] Viewing (national) 'security as business continuity' (Folkers 2017a, 2) may have been so naturalized that we have lost sight of the inherent conflicts of interest and power relations between the regulator and the regulated. This discourse we see mirrored also in contemporary approaches to preparedness, which reflects the rationality of business continuity management. Preparedness could open for building redundancies, for transgressing the logic of efficiency, and yet, even that approach to security becomes subject to narrow conceptualization of 'critical' or 'vital systems', of the mere reproduction of 'bare life' and the system as is. The current lack of ambition and political imagination on behalf of 'security' for the people, for human flourishing, for well-being, for peace, is as striking as is the inability to think security in a holistic manner. We have, indeed, created all sorts of labels – human security, environmental security, food security, economic security, political security, health security and so on, but this does not appear to have brought us any closer to a holistic understanding. Instead, the state appears to have shifted its role from a sovereign provider of security in the widest sense to (at best) a guarantor of last resort that intervenes in crisis situations when private provisions and security compliance measures catastrophically fail. There has thus been a shift from ensuring 'good life' to securing 'bare life', prioritizing survival over welfare (Folkers 2017c).

Where is society? Society, and for that matter any notion of the *social*, is conspicuous only by its absence in the prevalent market-led security thinking. Indeed, this can be seen as a historical win for Thatcher's famous dictum: 'there is no such thing as society'[75]. If there is any 'anti-' that captures the essence of these approaches, it is anti-social. The fact that these anti-social security management technologies are increasingly embraced in a country such as Norway – the norm entrepreneur behind the concept of 'human security' (Paris 2001), renowned for a strong social welfare state, for its peacekeeping missions, and for cherishing its social 'trust' (the Nordic gold[76]) – is interesting in its own right. Indeed, the appropriation of these security management technologies which fundamentally challenge both traditional Norwegian security thinking and Norwegian working life regulation, is happening in the context of immense geopolitical and security pressures and the dissolution of the international rules-based order. The return of large-scale interstate war to Europe and the insecurity concerning the future of NATO have naturally spurred unprecedented investments in the military-industrial complex and the 'warfare state', while shifting gears and accelerating the growth of the regulatory security state, expanding its reach and with it also boosting the security compliance market. Emblematically, in March 2025, the Norwegian Broadcasting Corporation (NRK) ran a debate with the following title: 'Cut welfare spending to fund defence?'[77] speaking to this emerging tension between military and welfare expenditure. Later the same year, the Prime Minister Jonas Gahr Støre put it diplomatically, by stating:

[73] See e.g., ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements, https://www.iso.org/obp/ui/en/#iso:std:iso:22301:ed-2:v1:en

[74] The exposition of the history of these translations would deserve a report of its own, here we only have space to remark upon the importance of the very filtering of Cold War national security tropes through corporate governance and its interests – distinct from the interests of the national security state.

[75] https://www.margaretthatcher.org/document/107440

[76] Trust – The Nordic Gold, Nordic Council of Ministers, https://norden.diva-portal.org/smash/get/diva2:1095959/fulltext02.pdf

[77] 'Kutte velferd for å få råd til forsvar?' https://www.nrk.no/norge/kutte-velferd-for-a-fa-rad-til-forsvar_-1.17335629

> 'It is important that everyone in our country now understands that our defence efforts and total preparedness will set a strong direction for our priorities in the years ahead. And just because Norway is in a favourable position, that does not mean we have to cut back on other important areas, such as healthcare, education, and elderly care. But I will use the phrase: It is going to be "less of more." That is how this can be done responsibly.'[78]

The 'less of more', meaning less of more welfare, is an interesting phrase – in particular in light of the areas where there is (practically no discussion about the need of) 'more of more', such as in the realm of regulation and compliance, where 'more of more' is *the* preferred solution: more risk assessments, more screenings, more due diligence, more background checks, more control systems, more monitoring, more threat assessments, more reporting, more standards and so on.

As we have seen across this report, we can conclude that many of the key concerns boiled down to the relation between power and knowledge and the questions of whose interests are shaping the societies we live in and our understanding of security. When considering the relation between power and knowledge, we must also take into account the deepening global inequality and the staggering concentration of wealth: 'about 56,000 people control three times as much wealth as half of humanity' (Holmes et al. 2025). The concentration of power – financial and epistemic – will shape the future: of security, of societies, of the planet. But there is also the power of imagination. In this report, we have seen how certain concepts and epistemologies acquired disproportionate power to shape how we think – not because they were necessarily the best. Even a floating and strikingly empty and all-encompassing concept such as the 'insider' can spread like a wildfire under certain conditions and capture the hearts and minds of security managers. If we pause, take the time to step back and think, and resist the urge to act immediately, we may create a space for exercising critical thought and imagining differently. Our conclusion is, therefore, that we have to create new opening – towards alterative futures, starting by challenging and breaking the epistemic closure, epistemic capture and siloed thinking. We may need to cultivate our ability to imagine alternative, positive futures and regain agency in shaping the world. This may also be the proper place of future studies,

> 'Futures studies – when deployed in policy and other contexts – should introduce critical perspectives (…) In this sense, it should be seen as part of the re-politicisation of (technocratic) policy-making, enabling meaningful critique, encouraging contestability, and revealing assumptions and power interests.' (Ahlqvist and Rhisiart 2015, 103)

There is, today, of course no dearth of anticipatory exercises and attempts to colonize the future and speculate in possible futures. If there is a vogue in the governance circles, it is precisely anticipatory governance (B. Anderson 2010; Kimbell and Vesnić-Alujević 2020; Flyverbom and Garsten 2021). The security discourses discussed across this report are fundamentally oriented around anticipation, prediction, and future potentialities – such as the 'risk indicators' which may suggest a *potentiality* of this or that individual posing a risk in the future. It may therefore sound as somewhat of a paradox that we call for expanding future imaginaries. But what we call for is the need to develop holistic and critical but above all *positive* future imaginaries that consider the possibility of change – both individual and societal. For unlike prediction which assumes that the future is bound by the past – that an individual cannot change, improve, be rehabilitated or that the course of technological development is a given, a matter we have to submit to and at best manage the risks of, such as the assumption of the inevitability of AI shaping all aspects of life on

[78] 'Statsministerens innledning på halvårlig oppsummerende pressekonferanse', 27.06.2026, translated from Norwegian by authors https://www.regjeringen.no/no/aktuelt/statsministerens-innledning-pa-halvarlig-oppsummerende-pressekonferanse/id3113411/#:~:text=Og%20fordi%20at%20Norge%20er%20i%20en,viktige%20oppgaver%2C%20som%20helse%2C%20skole%20og%20eldreomsorg.

the planet in the future, our approach insists that we can imagine differently. The history sides with the latter approach, there is no one path that is pre-determined and given by the past.

It has been very easy to imagine dystopian scenarios, but far harder to address questions of public, social and collective good and how it is to be achieved. It has by now become clear that we need to think harder about the relationship between the state, the private sector and (national) security – and between these and society and culture. If we shift gears and think more in terms of preparedness, we may realize that we need to think far more holistically, and we may reorient security around the concept of the social, around informal capabilities rather than formal compliance fictions. And, it might be, that this is also good security management. That it is possible to think differently about organizational culture and security, even in The Armed Forces, is apparent from their very own Cultural Handbook (*Kulturhåndboken*), in it, we can read the following:

> 'When working on organizational culture, it is important that we keep one thing in particular in mind: Cultural work is not about addressing deviations or "dealing with things we don't want." Nor is actively working on our culture a hobby or a side project. Cultural work is about creating the *conditions* that allow us to carry out our missions, *thrive at work, and build the best possible defence.* If we are to further develop and improve our culture, this naturally also means that along the way we do what we can to reduce the occurrence of what we do not want to see in our culture. Our operational capability is weakened when we have a culture that does not protect our community. The main focus of our cultural work should therefore be on the following: Ensuring that we have a *culture that promotes the fulfilment of our missions while also safeguarding our personnel*.' (Røislien 2024, 12 emphasis and translation ours)

This shows that it is possible to approach security from a positive, collectively oriented cultural angle also at the organizational level. This perspectival shift is fundamental as it reorients us around building what we want: it builds capacities, it builds workforce competencies, it builds team spirit, it creates meaning and security. The Armed Forces naturally have a security clearance regime, the same regime that has inspired the insider risk management, but they also have rituals, routines, and symbols designed to build meaningful organizational culture. While the former have disproportionately shaped security products on the market, the latter, which balances the intrusive practices, has largely been ignored. But it is the latter, culturally informed model built around that which we wish to achieve collectively, that would be of more use to the civil workforce, organizations and society at large. It would also be aligned with the Norwegian labour regulations, democratic values and the ideals of trust. A people-centred, holistic approach to security, which views individuals and their informal networks not as threats but as resources, would likely better serve the goals of preparedness. With approximately 100,000 NEETs (not in education, employment, or training) aged 15–29 in Norway, efforts to promote their inclusion (Frøyland 2020) should be accompanied by careful consideration of the consequences of expanding mechanisms of exclusion. Working life and workers' competencies are imperative in times of crisis and war, and central to the visions of total preparedness – working towards work inclusion serves both long-term preparedness and societal security (Hertzberg 2026). Therefore, we need more strategic and holistic thinking about how national security and preparedness play out in organizations and in the workplace and how different security objectives can most productively be achieved, while not merely respecting but advancing workers' rights, human flourishing and healthy working environment.

Ideas do shape societies and futures; neoliberalism, for one, has been a powerful idea that has restructured societies. In the world increasingly flooded by AI-generated slop, threatening to fundamentally destabilize knowledge production, we must cultivate the power of critical judgement and imagination. This may be the time for the return of the humanities and social sciences to the fore. Without them, we may have compliant workers and brilliant military

engineers, but we may not have a society we wish to live in or a planet to thrive on. And so it might be that the war ahead, might be first and foremost an epistemic one.

4 Recommendations

The report has identified several dilemmas related to the functioning of the regulatory security state: from the challenges of aligning organizations with the national security interest, via the disproportionate epistemic power of private security, BigTech and consulting in shaping security compliance and our understanding of security, to the risks of epistemic closure and mission creep as 'national security' becomes translated into organizational security management. Key concerns were linked to the democracy and legitimacy deficit of security compliance, the blind spots in the understanding of security, the gap between compliance maps and the territory. Taken together, these tendencies impede the emergence of and appear to undermine more holistic and human-centred approaches to security and preparedness. Such approaches were viewed as desirable, but unlikely to emerge due to epistemic and institutional lock-ins that reinforce technocratic and narrow-approaches to security removed from realities on the ground. The key worry expressed throughout this report has been that these approaches are counterproductive to real national and societal security. While compliance rituals may deliver 'ontological security', they may not only fail to deliver in terms of real security but also generate new security risks and unintended consequences. We discussed insider risk management as an exemplary example of security compliance. While it is reasonable for an organization to have personnel security measures, we have shown how insider risk management can turn into unreason – hitting all thinkable risks, harms, and threats in the workplace indiscriminately through the same blunt hammer.

The questions and concerns raised in this report pertained to the fundamental question of who gets to define security, risk, and the future. This report points at systemic issues. It is difficult to provide recommendations to redress these. There is no quick fix. In the following, we offer a few concrete and actionable recommendations – tiny steps towards new security paths. The following recommendations are written based on our understanding of how security compliance is *practiced*, offering suggestions to the regulators, the regulated, organizations not subject to the Security Act and key stakeholders such as trade unions and civil society.

National security interests versus organizational interest

- National security interest should be *clearly* articulated for the purposes of security compliance. National security is neither the same as organizational security nor societal security; where these concepts overlap, the regulator should ensure that a clear line of demarcation is drawn.
- The regulator should explicitly recognize that there is *no default alignment* between national security and organizational interests.
- Risk assessments conducted in the name of national security should be *limited* to and conducted only by those subject to the Security Act.
- Risk assessments in the name of national security should take their starting point from explicitly assessing organizational assets, functions and roles *in relation to* and *critical to national security*, not from organizational assets critical or important to the organizations themselves (while there may be instances where these interests coincide, this is *not* a given).
- Risk assessments under the Security Act should not be reduced to the organizational implementation of ISO/NS risk standards as is often the case today; these standards do *not* contain any specific risk assessment in relation to national security and the section 1-1. of the Security Act.
- At the level of the organization: organizational security measures implemented in national security interest should be clearly separated from general organizational security measures implemented in the organization's interest.

- Clear purpose limitations should be introduced; each organization should have a clear *Purpose limitation statement* regarding security measures implemented in the respective interests of 1) national security and 2) organizational security.
- Intrusive security measures should be *restricted* to the protection of assets and functions *clearly* linked to national security interest (not organizational interest); these should not serve other purposes.
- The regulator should take *responsibility* for *how* national security interest is translated into security compliance and organizational management by market actors and organizations, *enforce* purpose limitations, and ensure that security compliance measures actually serve national security interest.
- The regulator should more clearly specify and guide organizations on section 1.-1.c of the Security Act, which states that one is to 'ensure that security measures are implemented in accordance with the fundamental legal principles and values of a democratic society.'
- Public regulatory bodies and agencies should not issue too broad 'best practice' guidance. If best practice guidance is issued, it must be *specific* enough to prevent mission creep and function creep.
- The regulator should conduct *impact* assessments and *outcomes* evaluations, including analysis of long-term *impacts* of security compliance on national security (interest).

Rationale behind these recommendations: These recommendations stem from our observation of the conceptual stretching of 'national security' and the expansion of security management products on the market *legitimized* by references to national security and current geopolitical situation. The fundamental problem of the regulatory security state, as we have seen, is that it *delegates enormous discretionary power to the regulated entities and to security (compliance) markets*. The key challenge for the regulatory security state is to retain definitional power and achieve its goals as it delegates, outsources and relies on market expertise. One way would be to set and enforce clearer *limitations* and retain definitional power over what is considered national interest. Otherwise, we risk that 'national security' is everywhere but nowhere at the same time and that 'national security interest' becomes reduced to business or organizational interest of any given actor.

Security management in the workplace

- The regulator should consider developing *cross-agency guidelines* on security management in the workplace providing a clear guidance on the balancing of different interests at the organizational level (e.g., national security, security, privacy, anti-discrimination, inclusion, trade union role, etc.). Today, these balancing acts are delegated to each organization; this is problematic given the serious risks for both workers and security.
- Security management cuts across regulatory domains, raising issues of privacy, control in the workplace, democracy, and freedom of speech. But it also promises to deliver on often competing security goals of the regulatory security state, simultaneously: national security, societal security, and preparedness – in addition to its own interest of organizational security. Therefore, the development of cross-agency guidelines should involve representatives of employer and employee organizations, in addition to relevant directorates and regulatory bodies (e.g., Ministry of Labour and Social Inclusion, NSM, Directorate for Civil Protection, the Norwegian Data Protection Authority, The Norwegian Labour Inspection Authority, The Equality and Anti-Discrimination Ombud etc.).
- In the meantime, trade unions should be instructed about their role in security management and should take a more active role in the workplace and in public debate on the proportionality and effectiveness of security management.

- In organizations, employers and trade unions should take the necessary time to discuss what they mean by the concept of 'security' and *jointly* define legitimate organizational security goals and interests. They should also jointly discuss their organization's role in national security (if any), in preparedness, and in societal security in a broad sense. These different security goals should be clearly distinguished from each other and clearly defined. Their impacts on the organization and workplace relations, the organization of work, and workers' rights etc. should be assessed. Organizational interest and *public* interest goals should be clearly separated and the relationship between the two clearly articulated.
- Security measures implemented in the workplace should be subject to social dialogue and should have *clear purpose statements* outlining what concrete risk, harm or security threat is targeted in each case, what *least intrusive* measures were chosen, how their success/failure will be determined; agreement on *prohibited uses* of data gathered through digital security management systems should be considered. Trade unions should take an active role in preventing mission and function creep of security management technologies and measures implemented in the workplace.
- Employers, together with trade unions, should perform annual impact assessments of security measures, evaluating their 1) impact on workers and their 2) actual security *outcomes* held up against their originally stated purposes.
- An active social dialogue about organizational security measures and the intersection of digitalization and security should be a default for *all* Norwegian organizations.
- The employer and trade unions should jointly ensure that security management measures are limited to their stated purpose, that this purpose is legitimate, that data collected in the process is not used for other purposes, that least invasive measures are chosen, that measures are proportionate and that they serve the stated purpose also in terms of their actual *outcomes*. Trade unions should contribute to achieving this goal, while holding the employer accountable; employer should actively facilitate social dialogue in this area.
- In the security discourse, as elsewhere, the principles of the Norwegian model should be upheld: mutual trust between management and workers and the understanding of workers as a *resource*, not primarily as a risk or threat.
- Trade union representatives should be seen as a *resource* in security management, having valuable knowledge and bottom-up understanding that managers and leadership often lack.

Rationale behind the recommendations: Norwegian workplaces are a fundamental democratic arena; the Norwegian model is built on employee representation, trust, and a collaborative culture. Workplace democracy contributes to the legitimacy of and trust in the democratic system, to stability and economic development. Workplace democracy is a core democratic value that we seek to protect, also under the Security Act. In the realm of safety management, we have over the past decades developed strong model founded on the principles of Norwegian working life, and we have learnt from the mistakes of importing American-style managerial systems and developed models such as the Human Organisational Performance (HOP)[79] and moved away from systems which placed blame on individuals towards more constructive, productive and realistic approaches to safety management. The 'security' management field has yet to be aligned with the Norwegian model of workplace relations. At the same time, we see that intrusive measures are increasingly legitimized with vague notions of 'security'. Basic questions such as whose security, or what is meant by security in each instance, remain glossed over. This contributes to overreach and increases the potential worker harm, while potentially undermining

[79] See for instance the practical guide *Safety, Leadership and Learning* by Norsk Industri, https://www.norskindustri.no/siteassets/dokumenter/hms/hop/hop-veileder-engelsk-2024-3005.pdf

actual security. Norway has a solid potential to develop superior approaches to security management informed by sociological and cultural insights[80] that take preserving democratic values, workers' rights and societal values such as inclusive working life seriously. This work will, however, require the state to fund *independent* research and stimulate collaboration between trade unions and businesses on this subject.

Democratic, open and enlightened public debate and futures thinking about security

- Increase funding for independent, open, fundamental research on security and critical futures studies, which can push the state-of-the art and stimulate enlightened public debate, at universities and elsewhere.
- Work to increase academic freedom and openness in security-related research.
- Strengthen and increase funding for investigative and independent journalism.
- Increase funding for cultural institutions, libraries, museums, and art – the very spaces we need to imagine (security) futures differently.
- Increase support for civil society organizations working for the freedom of speech and open public debate.

Rationale behind the recommendations: At present, security is everywhere. It has come to mean many things, it is both expansive – as the national security discourse colonizes more and more organizations, and strikingly narrow – as translates into prime focus on threat actors and management of risk. There is national security on one hand and there are preparedness and societal security on the other, which promise broader visions of security, but often resort to the same techno-bureaucratic compliance tools, elaborate planning, and risk management. There is a fundamental need to *think deeper, broader and more long-term about security*, and to stop reducing security to a matter of techno-bureaucratic security *management*. We need to think more substantially about how to achieve the *collective public* goal of security, peace, and human flourishing within our planetary boundaries. This fundamental thinking about such a human-centred holistic approach to security cannot be done by regulatory bodies and agencies, each concerned with their little share of reality and churning out documents and guidelines that point in different directions. We must transgress this siloed bureaucratized thinking and create spaces where fundamental questions can be raised – from research to strengthening public debate and increasing our ability to imagine and thus also *create* and *shape* futures instead of being preoccupied with predicting them or complaining about our powerlessness vis-à-vis the power of the few. This can be achieved only if we prioritize education, research, and culture. In times of geopolitical and security pressures it is easy to argue that we need to 'prioritize' the essential and to be 'reasonable' and channel funds to where they matter most in terms of self-preservation, such as the Armed Forces. But it may turn out that such a narrow approach is not very reasonable after all, especially if this means that we leave the thinking on security and on the future to self-interested security markets and organizations. Maybe we would be better served if the enormous resources funnelled into and consumed by the production of compliance fictions, were channelled into the productive work of imagining better futures and then actually realizing them. This may strengthen our actual preparedness.

Wilhelm von Humboldt (1767–1835), widely regarded as the father of the modern university, is routinely referred to in celebratory speeches about academic freedom and humanistic learning, ideas that are increasingly seen as irrelevant due to the demands of the deteriorating security situation. But it is often forgotten that Humboldt was a civil servant of his native Prussia. His educational reforms were not intended to increase the enjoyment of bookish members of the

[80] The aforementioned *Cultural Handbook* of the Armed Forces already points towards such a possibility, (Røislien 2024).

privileged classes but to strengthen the resilience of Prussian state and society after devastating losses in the Napoleonic wars.

In these uncertain times, an enlightened approach to security is of paramount importance. Being conscious about security is not the same as securitizing everything, which is tantamount to securitizing nothing. We need to be equally aware of what we need to protect from security threats. Only then will we be able to protect it instead of smashing it with the hammer that makes us mistake everything for nails.

References

Adler, Emanuel, and Steven Bernstein. 2004. 'Knowledge in Power: The Epistemic Construction of Global Governance'. In *Power in Global Governance*, edited by Michael Barnett and Raymond Duvall. Cambridge University Press. https://doi.org/10.1017/CBO9780511491207.013

Afnan, Asasfeh, E. A. Alnawayseh Saif, AbdElkareem Reem, and Salahat Mohammed. 2024. 'Human Factors In Security Management: Understanding And Mitigating Insider Threats'. *2024 2nd International Conference on Cyber Resilience (ICCR)*, 1-10-1–10. https://doi.org/10.1109/ICCR61006.2024.10532956

Agamben, Giorgio. 1998. *Homo Sacer: Sovereign Power and Bare Life*. Stanford University Press.

Ahlqvist, Toni, and Martin Rhisiart. 2015. 'Emerging Pathways for Critical Futures Research: Changing Contexts and Impacts of Social Theory'. *Futures* 71 (August): 91–104. https://doi.org/10.1016/j.futures.2015.07.012

Amoore, Louise. 2013. *The Politics of Possibility: Risk and Security beyond Probability*. Duke University Press.

Amoore, Louise, and Marieke de Goede, eds. 2008. *Risk and the War on Terror*. Routledge. https://doi.org/10.4324/9780203927700

Amoore, Louise, and Volha Piotukh. 2015. 'Life beyond Big Data: Governing with Little Analytics'. *Economy and Society* 44 (3): 341–66. https://doi.org/10.1080/03085147.2015.1043793

Ananny, Mike, and Kate Crawford. 2018. 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability'. *New Media & Society* 20 (3): 973–89. https://doi.org/10.1177/1461444816676645

Anderson, Ben. 2010. 'Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies'. *Progress in Human Geography* 34 (6): 777–98. https://doi.org/10.1177/0309132510362600

Anderson, Elizabeth. 2017. *Private Government: How Employers Rule Our Lives (and Why We Don't Talk about It)*. Princeton University Press.

Aradau, Claudia. 2010. 'The Myth of Preparedness'. *Radical Philosophy* 161: 1–7.

Aradau, Claudia. 2017. 'Assembling (Non)Knowledge: Security, Law, and Surveillance in a Digital World'. *International Political Sociology* 11 (4): 327-342. https://doi.org/10.1093/ips/olx019

Aradau, Claudia, and Tobias Blanke. 2015. 'The (Big) Data-Security Assemblage: Knowledge and Critique'. *Big Data & Society* 2 (2): 1-12. https://doi.org/10.1177/2053951715609066

Aradau, Claudia, and Tobias Blanke. 2017. 'Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data'. *European Journal of Social Theory* 20 (3): 373–91. https://doi.org/10.1177/1368431016667623

Aradau, Claudia, and Tobias Blanke. 2018. 'Governing Others: Anomaly and the Algorithmic Subject of Security'. *European Journal of International Security* 3 (1): 1–21. https://doi.org/10.1017/eis.2017.14

Bakke, Anders. 2019. 'Refleksjoner over sikkerhetsklarering som virkemiddel'. *Lov og Rett* 58 (2): 82–93. https://doi.org/10.18261/issn.1504-3061-2019-02-03

Baldwin, Gretchen. 2025. *Pursuing Peace on a Shoestring: Conflict Management in an Increasingly Complex World*. SIPRI. https://doi.org/http://doi.org/10.55163/RLRA3708

Bellanova, Rocco, and Marieke De Goede. 2022a. 'Co-Producing Security: Platform Content Moderation and European Security Integration'. *JCMS: Journal of Common Market Studies* 60 (5): 1316–34. https://doi.org/10.1111/jcms.13306

Bellanova, Rocco, and Marieke De Goede. 2022b. 'The Algorithmic Regulation of Security: An Infrastructural Perspective'. *Regulation & Governance* 16 (1): 102–18. https://doi.org/10.1111/rego.12338

Ben Jaffel, Hager, and Sebastian Larsson. 2022. *Problematising Intelligence Studies: Towards a New Research Agenda*. 1st edn. Routledge. https://doi.org/10.4324/9781003205463

Benediktsson, Mike Owen. 2010. 'The Deviant Organization and the Bad Apple CEO: Ideology and Accountability in Media Coverage of Corporate Scandals'. *Social Forces* 88 (5): 2189–216. https://doi.org/10.1353/sof.2010.0032

Bergeijk, Peter A. G. van. 2022. *Economic Sanctions and the Russian War on Ukraine: A Critical Comparative Appraisal. I*. ISS working papers. General series No. 699. Institute of Social Studies (ISS). https://pure.eur.nl/ws/portalfiles/portal/51751545/wp699.pdf

Berndtsson, Joakim. 2012. 'Security Professionals for Hire: Exploring the Many Faces of Private Security Expertise'. *Millennium: Journal of International Studies* 40 (2): 303–20. https://doi.org/10.1177/0305829811425635

Berndtsson, Joakim, and Christopher Kinsey, eds. 2016. *The Routledge Research Companion to Security Outsourcing*. Routledge. https://doi.org/10.4324/9781315613376

Berndtsson, Joakim, Anne Roelsgaard Obling, and Åse Gilje Østensen. 2023. 'Business-Military Relations and Collaborative Total Defence in Scandinavia'. In *Total Defence Forces in the Twenty-First Century*, edited by Stéfanie Von Hlatky and Stéfanie Von Hlatky. McGill-Queen's University Press. https://doi.org/10.2307/jj.9992396

Berrefjord, Vivi Ringnes, and Tor Erling Bjørstad. 2025. 'Commercially Sourced Intelligence: Friend or Foe?' *Intelligence and National Security* 40 (3): 391–411. https://doi.org/10.1080/02684527.2024.2437955

Bigo, Didier. 2025. 'The Banalisation of "Suspicion": Politics of Prevention, Digitisation of Prediction, Fate of Travellers'. *International Migration* 63 (4): e70047. https://doi.org/10.1111/imig.70047

Black, Julia, ed. 2002. *Critical Reflections on Regulation*. (CARR Discussion Papers DP 4). ESRC Centre for Analysis of Risk and Regulation. London School of Economics and Political Science. https://researchonline.lse.ac.uk/id/eprint/35985/

Boxenbaum, Eva, and Linda Rouleau. 2011. 'New Knowledge Products as Bricolage: Metaphors and Scripts in Organizational Theory'. *The Academy of Management Review* 36 (2): 272–96. https://doi.org/https://doi.org/10.5465/amr.2009.0213

Brach, Anna, and David Sheldon. 2025. 'History of Human Security'. *Stratos* 2: 4–12. https://www.gcsp.ch/sites/default/files/2026-01/History%20of%20Human%20Security.pdf

Bråten, Stein. 1973. 'Model Monopoly and Communication: Systems Theoretical Notes On Democratization'. *Acta Sociologica* 16 (2): 98–107. https://doi.org/10.1177/000169937301600202

Bures, Oldrich, and Helena Carrapico, eds. 2018. *Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance*. Springer International Publishing. https://doi.org/10.1007/978-3-319-63010-6

Burrell, Jenna. 2016. 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms'. *Big Data & Society* 3 (1): 1-12. https://doi.org/10.1177/2053951715622512

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Campbell, S. M., and J. A. Cantrill. 2001. 'Consensus Methods in Prescribing Research'. *Journal of Clinical Pharmacy and Therapeutics* 26 (1): 5–14. https://doi.org/10.1111/j.1365-2710.2001.00331.x

Cantrill, J. A., B. Sibbald, and S. Buetow. 1996. 'The Delphi and Nominal Group Techniques in Health Services Research'. *International Journal of Pharmacy Practice* 4 (2): 67–74. https://doi.org/10.1111/j.2042-7174.1996.tb00844.x

Carmola, Kateri. 2010. *Private Security Contractors and New Wars*. Routledge. https://doi.org/10.4324/9780203856895

Carr, Madeline. 2016. 'Public-Private Partnerships in National Cyber-Security Strategies'. *International Affairs* 92 (1): 43–62. https://doi.org/10.1111/1468-2346.12504

Carrapico, Helena, and Benjamin Farrand. 2017. '"Dialogue, Partnership and Empowerment for Network and Information Security": The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers'. *Crime, Law and Social Change* 67 (3): 245–63. https://doi.org/10.1007/s10611-016-9652-4

Chalmers, Jane, and Mike Armour. 2019. 'The Delphi Technique'. In *Handbook of Research Methods in Health Social Sciences*, edited by Pranee Liamputtong. Springer Singapore. https://doi.org/10.1007/978-981-10-5251-4_99

Chesterman, S. 2008. '"We Can't Spy ... If We Can't Buy!": The Privatization of Intelligence and the Limits of Outsourcing "Inherently Governmental Functions"'. *European Journal of International Law* 19 (5): 1055–74. https://doi.org/10.1093/ejil/chn055

Christl, Wolfie. 2024. *Employees as Risks: A Case Study on Intrusive Surveillance and Behavioral Profiling for Cybersecurity, Insider Risk Detection and "Compliance"*. Cracked Labs. https://crackedlabs.org/dl/CrackedLabs_Christl_SecurityRiskProfiling.pdf

Collier, Stephen J., and Andrew Lakoff. 2015. 'Vital Systems Security: Reflexive Biopolitics and the Government of Emergency'. *Theory, Culture & Society* 32 (2): 19–51. https://doi.org/10.1177/0263276413510050

Colwill, Carl. 2009. 'Human Factors in Information Security: The Insider Threat - Who Can You Trust These Days?' *Information Security Technical Report.* 14: 186-196. https://doi.org/10.1016/j.istr.2010.04.004

Cornelissen, Joep P. 2005. 'Beyond Compare: Metaphor In Organization Theory'. *Academy of Management Review* 30 (4): 751–64. https://doi.org/10.5465/amr.2005.18378876

Cunliffe, Kyle S. 2021. 'Hard Target Espionage in the Information Era: New Challenges for the Second Oldest Profession'. *Intelligence and National Security* 36 (7): 1018–34. https://doi.org/10.1080/02684527.2021.1947555

Dalkey, Norman, and Olaf Helmer. 1963. 'An Experimental Application of the DELPHI Method to the Use of Experts'. *Management Science* 9 (3): 458–67. https://doi.org/10.1287/mnsc.9.3.458

De Olazábal, Itxaso Domínguez. 2026. 'False Choices: Competitiveness, Deregulation, and the Erosion of GDPR's Regulatory Integrity'. *Computer Law & Security Review* 60 (April): 106237. https://doi.org/10.1016/j.clsr.2025.106237

De Valk, Giliam. 2020. 'On Screening and the Insider Threat – A Methodological Exploration'. *National Security and the Future* 20 (1–2): 35–50. https://doi.org/10.37458/nstf.20.1-2.5

Demarais, Agathe. 2022. *Backfire: How Sanctions Reshape the World Against US*. Columbia University Press.

Diller, Janelle M. 2012. 'Private Standardization in Public International Lawmaking'. *Michigan Journal of International Law* 33: 481–536. https://repository.law.umich.edu/mjil/vol33/iss3/2

Duffield, Mark. 2013. *Development, Security and Unending War: Governing the World of Peoples*. Polity Press.

Dunn Cavelty, Myriam, and Max Smeets. 2023. 'Regulatory Cybersecurity Governance in the Making: The Formation of ENISA and Its Struggle for Epistemic Authority'. *Journal of European Public Policy* 30 (7): 1330–52. https://doi.org/10.1080/13501763.2023.2173274

Eichensehr, Kristen E., and Cathy Hwang. 2023. 'National Security Creep in Corporate Transactions'. *Columbia Law Review* 123 (2). https://columbialawreview.org/content/national-security-creep-in-corporate-transactions/

Ericson, Mathias, and Misse Wester. 2022. 'If I Tell You I Will Have to Kill You: Secrecy in Public Administration in a Time of Securitization and Militarization'. *Critical Studies on Security* 10 (1): 43–54. https://doi.org/10.1080/21624887.2022.2062926

Farrand, Benjamin, and Helena Carrapico. 2018. 'Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism'. In *Security Privatization*, edited by Oldrich Bures and Helena Carrapico. Springer International Publishing. https://doi.org/10.1007/978-3-319-63010-6_9

Farrand, Benjamin, Helena Carrapico, and Aleksei Turobov. 2024. 'The New Geopolitics of EU Cybersecurity: Security, Economy and Sovereignty'. *International Affairs* 100 (6): 2379–97. https://doi.org/10.1093/ia/iiae231

Farrell, Henry, and Abraham L. Newman. 2019. 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion'. *International Security* 44 (1): 42–79. https://doi.org/10.1162/isec_a_00351

Fischer-Lescano, Andreas, and Gunther Teubner. 2019. 'Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law'. In *Critical Theory and Legal Autopoiesis*, by Gunther Teubner. Edited by Diana Göbel. Manchester University Press. https://doi.org/10.7765/9781526139948.00018

Fishman, Edward. 2025. *Chokepoints: American Power in the Age of Economic Warfare*. Portfolio.

Flyverbom, Mikkel, and Christina Garsten. 2021. 'Anticipation and Organization: Seeing, Knowing and Governing Futures'. *Organization Theory* 2 (3): 1-25. https://doi.org/10.1177/26317877211020325

Folkers, Andreas. 2017a. 'Continuity and Catastrophe: Business Continuity Management and the Security of Financial Operations'. *Economy and Society* 46 (1): 103–27. https://doi.org/https://doi.org/10.1080/03085147.2017.1307650

Folkers, Andreas. 2017b. 'Existential Provisions: The Technopolitics of Public Infrastructure'. *Environment and Planning D: Society and Space* 35 (5): 855–74. https://doi.org/https://doi.org/10.1177/0263775817698699

Folkers, Andreas. 2017c. 'Existential Provisions: The Technopolitics of Public Infrastructure'. *Environment and Planning D: Society and Space* 35 (5): 855–74. https://doi.org/10.1177/0263775817698699

Forsberg, Ellen-Marie. 2012. 'Standardisation in the Field of Nanotechnology: Some Issues of Legitimacy'. *Science and Engineering Ethics* 18: 719–39. https://doi.org/10.1007/s11948-011-9268-0

Frøyland, Kjetil. 2020. 'Arbeidsinkludering av utsett ungdom: – kva slags utfordring er det?' *Tidsskrift for velferdsforskning* 23 (3): 187–200. https://doi.org/10.18261/issn.0809-2052-2020-03-03

Fukuyama, Francis. 1992. *The End of History and the Last Man*. Free Press.

Garland, David. 2003. 'The Rise of Risk'. In *Risk and Morality*, edited by Richard Victor Ericson and Aaron Doyle. Toronto University Press.

Gelles, Michael G. 2021. 'Insider Threat Prevention, Detection, and Mitigation: Building an Insider Threat Program'. In *International Handbook of Threat Assessment*, edited by J. Reid Meloy, Jens Hoffmann, J. Reid Meloy, and Jens Hoffmann. Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0037

Genschel, Philipp, and Markus Jachtenfuchs. 2023. 'The Security State in Europe: Regulatory or Positive?' *Journal of European Public Policy* 30 (7): 1447–57. https://doi.org/10.1080/13501763.2023.2174580

Genter, Robert. 2018. 'Removing the Mask of Sanity: McCarthyism and the Psychiatric–Confessional Foundations of the Cold War National Security State'. *Journal of American Studies* 52 (04): 1066–94. https://doi.org/10.1017/S0021875817000950

Gergen, Kenneth J. 2015. 'From Mirroring to World-Making: Research as Future Forming'. *Journal for the Theory of Social Behaviour* 45 (3): 287–310. https://doi.org/10.1111/jtsb.12075

Giddens, Anthony. 1991. *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Wiley.

Gioe, David V., and Joseph M. Hatfield. 2021a. 'A Damage Assessment Framework for Insider Threats to National Security Information: Edward Snowden and the Cambridge Five in Comparative Historical Perspective'. *Cambridge Review of International Affairs* 34 (5): 704–38. https://doi.org/10.1080/09557571.2020.1853053

Gioe, David V., and Joseph M. Hatfield. 2021b. 'A Damage Assessment Framework for Insider Threats to National Security Information: Edward Snowden and the Cambridge Five in Comparative Historical Perspective'. *Cambridge Review of International Affairs* 34 (5): 704–38. https://doi.org/10.1080/09557571.2020.1853053

Giumelli, Francesco, and Michal Onderco. 2021. 'States, Firms, and Security: How Private Actors Implement Sanctions, Lessons Learned from the Netherlands'. *European Journal of International Security* 6 (2): 190–209. https://doi.org/10.1017/eis.2020.21

Gjesvik, Lars. 2023. 'Private Infrastructure in Weaponized Interdependence'. *Review of International Political Economy* 30 (2): 722–46. https://doi.org/10.1080/09692290.2022.2069145

Glasbeek, Harry. 2002. *Wealth by Stealth: Corporate Crime, Corporate Law, and the Perversion of Democracy*. Between the Lines.

Gleditsch, Nils Petter. 2015. 'The Treholt Case'. In *Nils Petter Gleditsch: Pioneer in the Analysis of War and Peace*, by Nils Petter Gleditsch, vol. 29. SpringerBriefs on Pioneers in Science and Practice. Springer International Publishing. https://doi.org/10.1007/978-3-319-03820-9_5

Graver, Hans Petter. 2021. 'Sikkerhetsklarering og rettssikkerhet'. *Lov og rett* 60: 393–412. https://doi.org/https://doi.org/10.18261/issn.1504-3061-2021-07-03

Greitzer, Frank L. 2019. 'Insider Threats: It's the HUMAN, Stupid!' *Proceedings of the Northwest Cybersecurity Symposium*, April 8, 1–8. https://doi.org/10.1145/3332448.3332458

Greitzer, Kangas, Noonan, Brown, and Ferryman. 2013. 'Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis'. *E-Service Journal* 9 (1): 106. https://doi.org/10.2979/eservicej.9.1.106

Gümüsay, Ali Aslan, and Juliane Reinecke. 2024. 'Imagining Desirable Futures: A Call for Prospective Theorizing with Speculative Rigour'. *Organization Theory* 5 (1): 26317877241235939. https://doi.org/10.1177/26317877241235939

Haddad, Christian, Dagmar Vorlíček, and Nina Klimburg-Witjes. 2024. 'The Security-Innovation Nexus in (Geo-)Political Imagination'. *Geopolitics* 29 (3): 741–64. https://doi.org/10.1080/14650045.2024.2329940

Hansen, Flemming Splidsboel. 2016. 'Russia's Relations with the West: Ontological Security through Conflict'. *Contemporary Politics* 22 (3): 359–75. https://doi.org/10.1080/13569775.2016.1201314

Hashem, Yassir, Hassan Takabi, Mohammad GhasemiGol, and Ram Dantu. 2015. 'Towards Insider Threat Detection Using Psychophysiological Signals'. *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*, October 16, 71–74. https://doi.org/10.1145/2808783.2808792

Hatlebrekke, Kjetil Anders, and M. L. R. Smith. 2010. 'Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure'. *Intelligence and National Security* 25 (2): 147–82. https://doi.org/10.1080/02684527.2010.489274

Hellemeier, Lucas F. 2025. 'Europe's Defence Industry More Than Two Years after Russia's Full-Scale Invasion: Plus ca change, plus c'est la même chose?' *European Review of International Studies* 11 (3): 439–69. https://doi.org/10.1163/21967415-11030006

Herbig, Katherine L. 2017. *The Expanding Spectrum of Espionage by Americans, 1947 – 2015*. Technical Report 17-10. PERSEREC. https://irp.fas.org/eprint/spectrum.pdf

Hertzberg, Haakon. 2026. 'Arbeidslivet som beredskapsressurs'. In *Totalberedskap*, edited by Per Martin Norheim-Martinsen. Gyldendal.

Hochuli, Alex. 2021. *The End of the End of History: Politics in the Twenty-First Century Bok*. Simon and Schuster.

Høiby, Marte, Pål Brennhovd, and Anita Øren. 2023. *En metastudie om innsidetrusselen*. 2023:01616. SINTEF.

Holmes, Oliver, Lucy Swan, Ashley Kirk, and Jon Henley. 2025. '"The 0.001%": A Quick Visual Breakdown of the World's Wealthiest People'. News. *The Guardian*, December 10. https://www.theguardian.com/news/2025/dec/10/visual-breakdown-worlds-wealthiest-people

Hummel, Ralph P. 2006. 'The Triumph of Numbers: Knowledges and the Mismeasure of Management'. *Administration & Society* 38 (1): 58–78. https://doi.org/10.1177/0095399705284202

Humphrey-Murto, Susan, and Maarten De Wit. 2019. 'The Delphi Method—More Research Please'. *Journal of Clinical Epidemiology* 106 (February): 136–39. https://doi.org/10.1016/j.jclinepi.2018.10.011

Idris, Ismaila, and Adeleke Nafisa Damilola. 2023. 'Systematic Literature Review and Metadata Analysis of Insider Threat Detection Mechanism'. *International Journal of Computer Science and Mobile Computing* 12 (4): 60–88. https://doi.org/10.47760/ijcsmc.2023.v12i04.007

Inayatullah, Sohail. 2004. *The Causal Layered Analysis (CLA) Reader: Theory and Case Studies of an Integrative and Transformative Methodology*. Tamkang University Press.

Iñiguez De Heredia, Marta. 2021. 'EU Peacebuilding's New Khaki: Exceptionalist Militarism in the Trading of Good Governed for Military-Capable States'. *Politics* 41 (3): 296–315. https://doi.org/10.1177/0263395720947346

Jäger, Thomas, and Gerhard Kümmel, eds. 2007. *Private Military and Security Companies: Chances, Problems, Pitfalls and Prospects*. VS Verlag für Sozialwissenschaften.

Jones, David Martin. 2018. 'Intelligence and the Management of National Security: The Post 9/11 Evolution of an Australian National Security Community'. *Intelligence and National Security* 33 (1): 1–20. https://doi.org/10.1080/02684527.2016.1259796

Jore, Sissel H. 2020. 'Security and Safety Culture—Dual or Distinct Phenomena?' In *The Coupling of Safety and Security*, edited by Corinne Bieder and Kenneth Pettersen Gould. SpringerBriefs in Applied Sciences and Technology. Springer International Publishing. https://doi.org/10.1007/978-3-030-47229-0_5

Joseph, Michael F., Michael Poznansky, and William Spaniel. 2022. 'Shooting the Messenger: The Challenge of National Security Whistleblowing'. *The Journal of Politics* 84 (2): 846–60. https://doi.org/10.1086/715595

Katzenbach, Christian, and Lena Ulbricht. 2019. 'Algorithmic Governance'. *Internet Policy Review* 8 (4). https://doi.org/10.14763/2019.4.1424

Kenneth, W. Abbott, David Levi-Faur, and D. Snidal. 2017. 'Theorizing Regulatory Intermediaries'. *The ANNALS of the American Academy of Political and Social Science* 670: 14-35-14–35. https://doi.org/10.1177/0002716216688272

Kenny, Kate. 2024. *Regulators of Last Resort: Whistleblowers, the Limits of the Law and the Power of Partnerships*. Cambridge University Press. https://doi.org/10.1017/9781009425629

Kimbell, Lucy, and Lucia Vesnić-Alujević. 2020. 'After the Toolkit: Anticipatory Logics and the Future of Government'. *Policy Design and Practice* 3 (2): 95–108. https://doi.org/10.1080/25741292.2020.1763545

Kraemer, S., P. Carayon, and J. Clem. 2009. 'Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities'. *Computers & Security* 28: 509-520-509–20. https://doi.org/10.1016/j.cose.2009.04.006

KraftCERT. 2025. *Forhindre utnytting av personell: Prinsipper og tiltak*. https://www.kraftcert.no/filer/KraftCERT-utnytting-personell.pdf

Krahmann, Elke. 2018. 'The Market for Ontological Security'. *European Security* 27 (3): 356–73. https://doi.org/10.1080/09662839.2018.1497983

Kruck, Andreas, and Moritz Weiss. 2023a. 'The Regulatory Security State in Europe'. *Journal of European Public Policy* 30 (7): 1205–29. https://doi.org/https://doi.org/10.1080/13501763.2023.2172061

Kruck, Andreas, and Moritz Weiss. 2023b. 'The Regulatory Security State in Europe'. *Journal of European Public Policy* 30 (7): 1205–29. https://doi.org/10.1080/13501763.2023.2172061

Kruck, Andreas, and Moritz Weiss. 2025. 'Disentangling *Leviathan* on Its Home Turf: Authority Foundations, Policy Instruments, and the Making of Security'. *Regulation & Governance* 19 (1): 146–60. https://doi.org/10.1111/rego.12594

Kuldova, Tereza Østbø. 2022. *Compliance-Industrial Complex: The Operating System of a Pre-Crime Society*. Palgrave. https://doi.org/10.1007/978-3-031-19224-1

Kuldova, Tereza Østbø. 2024. 'National Security, Insider Threat Programs, and the Compliance-Industrial Complex: Reflections on Platformization in Corporate Policing, Intelligence, and Security'. In *Policing and Intelligence in the Global Big Data Era, Volume I*, edited by Tereza Østbø Kuldova, Helene Oppen Ingebrigtsen Gundhus, and Christin Thea Wathne. Palgrave's Critical Policing Studies, 27-84. Palgrave. https://doi.org/10.1007/978-3-031-68326-8_2

Kuldova, Tereza Østbø, Helene Oppen Ingebrigtsen Gundhus, and Christin Thea Wathne, eds. 2024. *Policing and Intelligence in the Global Big Data Era, Volume I: New Global Perspectives on Algorithmic Governance*. Palgrave's Critical Policing Studies. Palgrave. https://doi.org/10.1007/978-3-031-68326-8

Kuldova, Tereza Østbø, and Jardar Østbø. 2026. 'Privatisering av sikkerhet: Når kartet blir viktigere enn terrenget'. In *Totalberedskap*, 312-331. Gyldendal.

Kuldova, Tereza Østbø, Jardar Østbø, and Thomas Raymen. 2024. *Luxury and Corruption: Challenging the Anti-Corruption Consensus*. Bristol University Press.

Kuldova, Tereza Østbø, Jardar Østbø, and Cris Shore, eds. 2024. *Compliance, Defiance, and 'Dirty' Luxury: New Perspectives on Anti-Corruption in Elite Contexts*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-57140-4

Landeta, Jon. 2006. 'Current Validity of the Delphi Method in Social Sciences'. *Technological Forecasting and Social Change* 73 (5): 467–82. https://doi.org/10.1016/j.techfore.2005.09.002

Levi-Faur, David. 2017. 'Regulatory Capitalism'. In *Regulatory Theory: Foundation and Applications*, edited by P. Drahos. ANU Press.

Levi-Faur, David. 2023. 'The Regulatory Security State as a Risk State'. *Journal of European Public Policy* 30 (7): 1458–71. https://doi.org/10.1080/13501763.2023.2174170

Loader, Ian. 1999. Consumer Culture and the Commodification of Policing and Security. *Sociology* 33 (2): 373–92. https://doi.org/10.1177/S003803859900022X

Lodge, Martin. 2025. 'The Resilience of the Regulatory State in an Age of Polycrisis'. *Revista Del CLAD Reforma y Democracia* Edición Especial 2025-1: 84–105. https://doi.org/https://doi.org/10.69733/clad.ryd.nee1.a477

Maasberg, Michele, Xiao Zhang, Myung Ko, Stewart R. Miller, and Nicole Lang Beebe. 2020. 'An Analysis of Motive and Observable Behavioral Indicators Associated With Insider Cyber-Sabotage and Other Attacks'. *IEEE Engineering Management Review* 48 (2): 151–65. https://doi.org/10.1109/EMR.2020.2989108

Majone, Giandomenico. 1994. 'The Rise of the Regulatory State in Europe'. *West European Politics* 17 (3): 77–101. https://doi.org/10.1080/01402389408425031

Majone, Giandomenico. 1997. 'From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance'. *Journal of Public Policy* 17 (2): 139–67. https://doi.org/10.1017/S0143814X00003524

Marangione, Margaret S. 2019. 'Millennials: Truthtellers or Threats?' *International Journal of Intelligence and CounterIntelligence* 32 (2): 354–78. https://doi.org/10.1080/08850607.2019.1565276

Martin, Paul. 2023. *Insider Risk and Personnel Security: An Introduction*. Routledge. https://doi.org/10.4324/9781003329022

McDonald, Matt. 2002. 'Human Security and the Construction of Security'. *Global Society* 16 (3): 277–95. https://doi.org/10.1080/09537320220148076

McGoey, Linsey. 2019. *Unknowers: How Strategic Ignorance Rules the World*. ZED books.

Mehus, Jacob, Marit Sæter, and Ingvild Næss Stub. 2026. 'Skal vi løse alt selv, eller kan vi lære av andre? Standardisering som virkemiddel i beredskapsarbeid'. In *Totalberedskap*, edited by Per Martin Norheim-Martinsen. Gyldendal.

Meld. St. 9 (2022–2023). 2022. 'Meld. St. 9 (2022–2023): National Control and Cyber Resilience to Safeguard National Security'. White paper. Recommendation of the Ministry of Justice and Public Security 9 December 2022, approved by the Council of State on the same day. https://www.regjeringen.no/en/documents/meld.-st.-9-20222023/id2950130/

Mittelstadt, Brent Daniel, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi. 2016. 'The Ethics of Algorithms: Mapping the Debate'. *Big Data & Society* 3 (2): 1-21. https://doi.org/10.1177/2053951716679679

Mitzen, Jennifer. 2006. 'Ontological Security in World Politics: State Identity and the Security Dilemma'. *European Journal of International Relations* 12 (3): 341–70. https://doi.org/10.1177/1354066106067346

Morgenthau, Hans J. 1955. 'State of Insecurity'. *New Republic*, no. 18. April: 8–14.

Morozov, Evgeny. 2013. *To Save Everything, Click Here*. Public Affairs.

Mügge, Daniel. 2023. 'The Securitization of the EU's Digital Tech Regulation'. *Journal of European Public Policy* 30 (7): 1431–46. https://doi.org/10.1080/13501763.2023.2171090

Norheim-Martinsen, Per Martin, ed. 2019. *Det Nye Totalforsvaret*. Gyldendal.

Norheim-Martinsen, Per Martin, ed. 2026. *Totalberedskap*. Gyldendal.

Notaker, Hallvard. 2023. 'Nasjonal sikkerhet eller økonomisk effektivitet? Norges evne til å avdekke hybride trusler i samtidshistorisk perspektiv'. *Internasjonal Politikk* 81 (1). https://doi.org/10.23865/intpol.v81.5157

Obar, Jonathan A. 2020. 'Sunlight Alone Is Not a Disinfectant: Consent and the Futility of Opening Big Data Black Boxes (without Assistance)'. *Big Data & Society* 7 (1): 205395172093561. https://doi.org/10.1177/2053951720935615

Obendiek, Anke Sophia, and Timo Seidl. 2023. 'The (False) Promise of Solutionism: Ideational Business Power and the Construction of Epistemic Authority in Digital Security Governance'. *Journal of European Public Policy* 30 (7): 1305–29. https://doi.org/10.1080/13501763.2023.2172060

Olsen, Odd Einar, Kirsten Juhl, Preben H. Lindøe, and Ole Andreas Engen. 2019. *Standardization and Risk Governance: A Multi-Disciplinary Approach*. 1st edn. Routledge. https://doi.org/10.4324/9780429290817

O'Reilly, Conor. 2015. 'The Pluralization of High Policing: Convergence and Divergence at the Public–Private Interface': *British Journal of Criminology* 55 (4): 688–710. https://doi.org/10.1093/bjc/azu114

Østbø, Jardar. 2024. 'Utility and Waste, Moralization, and Hybridization: The Inherent Contradictions of Anti-Luxury Sanctions on the Case of Russian-Owned Gigayachts'. In *Compliance, Defiance, and 'Dirty' Luxury*, edited by Tereza Østbø Kuldova, Jardar Østbø, and Cris Shore, 27-62. Palgrave. https://doi.org/10.1007/978-3-031-57140-4_2

Paris, Roland. 2001. 'Human Security: Paradigm Shift or Hot Air?' *International Security* 26 (2): 87–102. https://doi.org/10.1162/016228801753191141

Partiti, Enrico, Stephanie Bijlmakers, and Panagiotis Delimatsis. 2022. 'Evolutionary Dynamics of Transnational Private Regulation'. *Transnational Legal Theory* 13 (4): 431–65. https://doi.org/10.1080/20414005.2023.2178143

Pasquale, Frank. 2015. *The Black Box Society*. Harvard University Press. http://www.jstor.org/stable/j.ctt13x0hch

Petersen, Karen Lund. 2012. *Corporate Risk and National Security Redefined*. Routledge.

Petersen, Karen Lund. 2013. 'The Corporate Security Professional: A Hybrid Agent between Corporate and National Security'. *Security Journal* 26 (3): 222–35. https://doi.org/10.1057/sj.2013.13

Petersen, Karen Lund, and Vibeke Schou Tjalve. 2015. 'En offentlig hemmelighed: Når sikkerhedspolitik går fra statsmandskunst til allemandseje'. *Politik* 18 (3). https://doi.org/10.7146/politik.v18i3.27618

Petersen, Karen Lund, and Vibeke Schou Tjalve. 2018. 'Intelligence Expertise in the Age of Information Sharing: Public–Private "Collection" and Its Challenges to Democratic Control and Accountability'. *Intelligence and National Security* 33 (1): 21–35. https://doi.org/10.1080/02684527.2017.1316956

Pfaller, Robert. 2011. *Wofür es sich zu leben lohnt*: *Elemente materialistischer Philosophie.* FISCHER Taschenbuch.

Pursiainen, Christer. 2021. 'Russia's Critical Infrastructure Policy: What Do We Know About It?' *European Journal for Security Research* 6 (1): 21–38. https://doi.org/10.1007/s41125-020-00070-0

Robson Morrow, Maria A. 2022. 'Private Sector Intelligence: On the Long Path of Professionalization'. *Intelligence and National Security* 37 (3): 402–20. https://doi.org/10.1080/02684527.2022.2029099

Røislien, Hanne Eggen. 2024. *Kulturhåndboken: En innføring i kultur og kulturforståelse for forsvarets ansatte*. Forsvaret.

Rongved, Gjermund Forfang, and Per Martin Norheim-Martinsen, eds. 2022. *Totalforsvaret i Praksis*. Gyldendal.

Rosa, Hartmut. 2020. *The Uncontrollability of the World*. Polity.

Rothe, Dawn L., and David Kauzlarich. 2016. *Crimes of the Powerful: An Introduction*. Routledge.

Sage-Passant, Lewis. 2023. 'The Security Intelligence Services of the Private Sector'. PhD thesis. Loughborough University. https://doi.org/10.26174/THESIS.LBORO.24050421.V1

Schilde, Kaija. 2023. 'Weaponising Europe? Rule-Makers and Rule-Takers in the EU Regulatory Security State'. *Journal of European Public Policy* 30 (7): 1255–80. https://doi.org/10.1080/13501763.2023.2174582

Seddon, Max, and Polina Ivanova. 2022. 'How Putin's Technocrats Saved the Economy to Fight a War They Opposed'. The Big Read. *Financial Times*, December 16. https://www.ft.com/content/fe5fe0ed-e5d4-474e-bb5a-10c9657285d2?syn-25a6b1a6=1

Shaw, Eric, and Laura Sellers. 2015. *Application of the Critical-Path Method to Evaluate Insider Risks*. 59 (2). https://www.cia.gov/resources/csi/static/Application-of-Critical-Path-1.pdf

Shore, Cris, and Susan Wright. 2015. 'Audit Culture Revisited: Rankings, Ratings, and the Reassembling of Society'. *Current Anthropology* 56 (3): 421–44. https://www.jstor.org/stable/10.1086/681534

Shore, Cris, and Susan Wright. 2018. 'How the Big 4 Got Big: Audit Culture and the Metamorphosis of International Accountancy Firms'. *Critique of Anthropology* 38 (3): 303–24. https://doi.org/10.1177/0308275X18775815

Sivan-Sevilla, Ido. 2023. 'Supranational Security States for National Security Problems: Governing by Rules & Capacities in Tech-Driven Security Spaces'. *Journal of European Public Policy* 30 (7): 1353–78. https://doi.org/10.1080/13501763.2023.2172063

Slagnes, Betina. 2023. *Hva vet vi om innsiderisiko?* FFI-rapport. 23/00546

Słowikowski, Michał, and Michał Klonowski. 2025. 'What Does Ontological Security Theory Tell Us about Russia's Decision to Start the War against Ukraine?' *Studia Polityczne* 53 (3): 5–36. https://doi.org/10.35757/STP.2025.53.3.01

Smeets, Max. 2023. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Hurst & Company.

Stavrianakis, Anna. 2020. 'Requiem for Risk: Non-Knowledge and Domination in the Governance of Weapons Circulation'. *International Political Sociology* 14 (3): 233–51. https://doi.org/10.1093/ips/olz030

Steele, Brent J. 2008. *Ontological Security in International Relations*. 0 edn. Routledge. https://doi.org/10.4324/9780203018200

Synstnes, Hans Morten. 2016. *Den innerste sirkel den militære sikkerhetstjenesten 1945-2002*. Dreyer.

Timmermans, Stefan, and Steven Epstein. 2010. 'A World of Standards but Not a Standard World: Toward a Sociology of Standards and Standardization'. *Annual Review of Sociology* 36 (1): 69–89. https://doi.org/10.1146/annurev.soc.012809.102629

Tombs, Steve, and David Whyte. 2015. *The Corporate Criminal: Why Corporations Must Be Abolished*. Routledge.

Tsingou, Eleni. 2018. 'New Governors on the Block: The Rise of Anti-Money Laundering Professionals'. *Crime, Law and Social Change* 69 (2): 191–205. https://doi.org/10.1007/s10611-017-9751-x

Ullman, Harlan. 2022. 'Why Putin Won't Invade Ukraine'. *Atlantic Council*, February 16. https://www.atlanticcouncil.org/blogs/new-atlanticist/why-putin-wont-invade-ukraine/

Veale, Michael, and Irina Brass. 2019. 'Administration by Algorithm? Public Management Meets Public Sector Machine Learning''. In *Algorithmic Regulation*, edited by Karen Yeung and Martin Lodge. Oxford University Press.

Veggeland, Noralv. 2010. *Den Nye Reguleringsstaten: Idébrytninger Og Styringskonflikter*. Gyldendal.

Veggeland, Noralv. 2020. *Democratic Governance in Scandinavia: Developments and Challenges for the Regulatory State*. Springer International Publishing. https://doi.org/10.1007/978-3-030-18270-0

Wærp, Eline. 2024. 'The Age of Frontex: Banal Securitization and Its Normalization in EUropean External(Ized) Border Control'. PhD thesis. Malmö University.

Walters, William. 2008. 'Anti-Policy and Anti-Politics: Critical Reflections on Certain Schemes to Govern Bad Things'. *European Journal of Cultural Studies* 11 (3): 267–88. https://doi.org/10.1177/1367549408091844

Weber, Max. 2012. 'The "Objectivity" of Knowledge in Social Science and Social Policy'. In *Max Weber: Collected Methodological Writings*, edited by Hans Henrik Bruun and Sam Whimster. Routledge.

Weitzenboeck, Emily M., Rebecca Schmidt, and Diego Praino. 2025. 'Rettslig regulering av samarbeid mellom offentlige og private aktører – digital sikkerhet i helsesektoren'. In *Offentlige eller private velferdstjenester?* edited by Ann-Helén Bay and Asbjørn Røiseland. Cappelen Damm Forskning/NOASP. https://doi.org/10.23865/cdf.243.ch5

Wrange, Jana, Rikard Bengtsson, and Douglas Brommesson. 2024. 'Resilience through Total Defence: Towards a Shared Security Culture in the Nordic–Baltic Region?' *European Journal of International Security* 9 (4): 511–32. https://doi.org/10.1017/eis.2024.15

Wright, Lance. 2017. *People, Risk, and Security*. Palgrave Macmillan UK. https://doi.org/10.1057/978-1-349-95093-5

Yang, Songling. 2025. 'China's Approach to the Anti-Foreign Sanctions Mechanism and Its International Legality'. *Vanderbilt Journal of Transnational Law* 58: 157–96.

Yeung, Karen, and Martin Lodge, eds. 2019. *Algorithmic Regulation*. First Edition. Oxford University Press.

Yilmaz, Harun. 2022. 'No, Russia Will Not Invade Ukraine'. Al Jazeera. https://www.aljazeera.com/opinions/2022/2/9/no-russia-will-not-invade-ukraine

Work Research Institute AFI, OsloMet
AFI report ISSN 2703-836X
www.oslomet.no/om/afi