Planning for (Not) Taking Risk

The Creation of a Security Risk Assessment Standard in Norway

Anne Heyerdahl

Thesis submitted for the degree of Philosophiae Doctor (PhD) in Sociology
Department of Sociology and Human Geography
University of Oslo
2022

Series of dissertations submitted to the
Faculty of Social Sciences, University of Oslo
No. 955

ISSN 1504-3991

Cover: UiO.
Print production: Graphic Center, University of Oslo.

Table of Contents

The papers

Paper 1:
Heyerdahl, Anne. 2022. "Standardizing policy in a non-standard way – a public/private standardization process in Norway." Under review at Journal of Public Policy after revise and resubmit.

Paper 2:
Heyerdahl, Anne. 2022. "Risk Assessment without the Risk? A Controversy about Security and Risk in Norway." *Journal of Risk Research* 25(2): 252–67.

Paper 3:
Heyerdahl, Anne. 2022. "From Prescriptive Rules to Responsible Organisations – Making Sense of Risk in Protective Security Management – a Study from Norway." *European Security* 0(0): 1–23.

List of Figures and Tables

Acknowledgements

In 2013, I applied for a job in the Norwegian Ministry of Justice and Public Security in the division responsible for societal security. Less than two years had gone by since the gruesome attack on 22 July 2011. The Ministry had been hit hard - people had died and offices had been bombed. In addition, the Ministry was responsible for the coordination of societal security measures and was criticized and held accountable.

Why did I apply for the job? At the time, it seemed like a "window of opportunity." The Ministry needed to change, and I could be part of the journey. Part of the reason also lies in my fascination with the field of security and risk, raising questions of who we are as human beings and as a society.

In a ministry, you work with major issues, with little time to think and reflect. When the National Research Council announced a new grant, a public sector PhD, I knew this could be the opportunity I had longed for. I started as a PhD fellow in December 2017.

First, I want to thank the Ministry of Justice and Public Security for supporting the PhD project, taking the role as project owner, and financing the project together with the Research Council. I especially want to thank Hege Johansen, my always enthusiastic boss, who has trusted me fully and has given me time and space. I also want to thank Jon Fixdal for taking on the role as project manager. An acute pandemic is more important than a PhD project and you wisely prioritized accordingly. I do cherish the conversations we have had and your good advice in this regard. I would also like to thank my colleague May-Kristin Ensrud for interesting discussions and for your knowledgeable feedback.

I am eternally grateful for my supervisors' active participation in - and enthusiasm for - my project. Cathrine Holst, Sissel Haugdal Jore and Monica Endregard - you have nicely supplemented each other in knowledge and perspectives. I feel so lucky to have had the three of you as my supervisors.

A special thanks to Cathrine. When I first applied for the grant, I did so at the Department of Political Science. When I moved to Sociology (ISS), the main reason was to be supervised by you. You have a unique combination of sound professional knowledge across several fields, wisdom, and curiosity. Your agenda has been for my project to be successful, and you have gently guided me on the way. I have always felt lucky and thankful after our numerable conversations. Thank you!

Thank you, Sissel, for sharing your many insights on security and risk, for reflecting together with me, and for our fun discussions. My design and analysis have become a lot better thanks to your critical questions.

Monica, your analytical mind, knowledge of the field, and your enthusiasm for the project have been a great asset to me and to the thesis. I am very thankful for your friendly feedback and involvement.

A lot of gratitude goes to my family – to Lars, Nora, and Oscar. When I spend evenings, weekends, and holidays writing, I take time away from us. Thank you for generously accepting and supporting me on this journey, and for being the nice haven you are. A special thanks to Oscar, who was 10 when I started and is 15 years old now. Especially the last year, I have worked too much. I look forward to you setting the priorities for our time together more than my work.

A warm thanks to Lars, who has endured and supported the project, not questioned progress or priorities as the years have gone by. We share the interest in – and experience from - both academia and public sector, and I cherish our many discussions and shared reflections. Key insights have come not least because of you. Thank you!

The project would not have existed without the interviewees. Many thanks to all of you for your engagement, reflections, and for the conversations. The interviews display self-reflection, knowledge, and awareness of dilemmas that is seldom made public or acknowledged, and I am thankful for the rich dialogue you have had with me. Thank you also to several people who have discussed with me more informally in various parts of the "system," who have given me tips and feedback. I do not know who wants to be publicly acknowledged and who does not, and I will thus only say – you know who you are. Thank you!

Thank you also to scholars who have engaged. I really enjoyed the community of PhD fellows at ISS before the pandemic ruined the social and professional bonding. Laura Maria Führer should be mentioned especially, for your good judgements, for supporting me in the process, and for cheering and helping all the way to the finishing line. Thanks also to Inga Sæther and Uzair Ahmed, and to the old gang at room 421 for making me feel welcomed.

Thank you to Per Magnus Mæhle and Maja Flåto for the academically fruitful and enjoyable public sector PhD network. Going into academia after several years of work experience has triggered reflections in all of us on the curious worlds of both academia and public sector; thank you for sharing and engaging. Thank you to professor Per Lægreid at UiB, who has given me valuable feedback at an early stage, and to professor Jostein Askim at Department of Political Science for supporting the project initially. Thank you to Tonje Grunnan for our lunches with PhD pep-talk.

Thank you to ISS for accepting my application and the public sector PhD set-up, the first at the institute. A special thanks to Inger-Lise and staff for all the extra support, given the new set-up.

Thank you to the Norwegian Defense Research Establishment for inviting me as guest researcher for a year, giving me valuable insights and support.

A special thank you to my dear parents. My mother took her PhD at 54 years old, and I am 54 years old now – it’s about to become a family tradition! I am proud to follow in your footsteps.

Lastly, a warm thanks to my larger family and friends – the nice “village” I look forward to spending more time with.

Takk!

Summary

This thesis investigates risk assessment and standardization by standard-setting organizations (SSOs), key governing practices in many societies today. It does so by studying the development of a security risk assessment approach into a Norwegian standard by the SSO Standards Norway (SN 5832:14). The first part investigates the institutionalisation of the standard as a policy process, while the second part investigates sensemaking by security professionals on questions of security risk assessment. The thesis asks how the establishment of the security risk assessment approach as a Norwegian standard can be accounted for.

The study is exploratory, and takes an abductive, puzzle-driven approach. It combines data from 40 interviews with document analysis and fieldwork on five courses in risk assessment, security management, and standardization.

The first part of the study investigates the standardization process as a policy process, as presented in article 1. The security risk assessment approach (labelled the three-factor approach or 3FA) is seen as a policy, and the study follows the 3FA's "journey" from one institutional context to the next, utilizing a within-case, longitudinal, comparative case study design. The process had three phases – it started within government agencies, moved to the jurisdiction of the SSO, and lastly consisted of the 3FA being debated by security and risk professionals.

The investigation of the standardization process utilises, but also develops, the multiple streams approach (MSA) originally developed by Kingdon. It contributes theoretically, by incorporating two sets of institutions – formal rules and knowledge – into the MSA. Both policy entrepreneurs and the institutional context are important for the institutionalization of the 3FA. Special attention is given to the characteristics of SSO standardization and its many ambiguities. The concept of "institutional deficit" is introduced, describing a potential mismatch between SSOs producing policy in a government-like institution, but where SSOs are not structured such that they manage to take responsibility for policies in a government-like way.

The second part investigates security professionals' sensemaking on risk assessment in a security context, utilizing methods from qualitative interpretive traditions. Article 2

investigates understandings of probability's role, and article 3 the role of risk assessment in protective security management.

This part of the thesis draws on Michael Power's risk governance theory as well as security theory. It builds on a little-utilized part of Power's theory, namely his development of three ideal models of risk management logics. The thesis develops these logics into four: risk management as anticipation, optimization, governance, and protection. The theorizing makes it possible to highlight three findings from the second part of the study.

First, there is a perceived tension between risk management's aim at optimization and the goal of protection. Probability plays a key role in the former but is a potential "threat" to the latter and vice versa; precautionary practices embedded in protection are at odds with optimizing resources.

Second, probability has two roles in the expression of risk, that is, anticipating the future and moderating the risk. Those arguing against expressing security risks through probability pay attention to the former (epistemic uncertainty). Those arguing against the 3FA pay attention to probability's moderating role, concerned that downplaying probability leads to overinvestment in low-probability risks.

Third, the thesis finds a perceived inconsistency across time between what is expected before and after an incident. Before, there is an expectation of analytical conduct and optimization, whereas afterwards, they expect a judgement of failure to protect, with blame as a potential outcome.

In summary, both the characteristics of the policy process and security professionals' sensemaking must be taken into account. Conceived of exclusively as a policy process, ideas and sensemaking play a modest role. However, investigating sensemaking by security professionals provides nuance to this conclusion. The 3FA reflects security professionals' sensemaking, where the tension between protection and risk optimization becomes evident. Probability makes risk "risky," and downplaying probability moves risk assessment in the direction of precaution and security. Hence, although the policy process was pivotal for the development of the standard, the 3FA also reflects struggles to combine contradictory risk logics in protective security management.

List of Abbreviations

2FA	Two-factor approach – risk as a combination of consequence and probability/likelihood
3FA	Three-factor approach – risk as a combination of value (asset), threat and vulnerability
CEN	European Committee for Standardization
CIP	Critical infrastructure protection
DSB	Norwegian Directorate for Civil Protection
FB	Norwegian Defense Estates Agency
FFI	Norwegian Defense Research Establishment
IR	International relations
ISO	International Organization for Standardization
MJ	Norwegian Ministry of Justice and Public Security (from 2011) Norwegian Ministry of Justice and the Police (until 2011)
MSA	Multiple Streams Approach
NSM	Norwegian National Security Authority
NS 5814	Norwegian Standard presenting risk as 2FA
NS 5832	Norwegian Standard presenting risk as 3FA
PE	Policy entrepreneur
POD	The National Police Directorate
PSM	Protective security management
PST	Norwegian Police Security Agency
SRA	Security risk assessment
SSO	Standard–Setting Organization
SN	Standards Norway

1. Introduction

Bad things can happen, whether intentionally or not. The Russian war on Ukraine and the recent pandemic have made this abundantly clear. Societies such as the Norwegian do not simply hope for the best or pray for God's mercy. They try to anticipate and mitigate what might come, seeing the future in terms of risk. Societies of today are – however it may be interpreted and whatever it may imply – "risk societies."

My curiosity which led to this thesis started with an empirical puzzle. As a civil servant in the Ministry of Justice and Public Security (hereafter MJ), I was the surprised recipient of criticism at a meeting that the MJ should not let risk assessments in the security area include probability. This was *wrong,* I was told. I became aware that a debate was going on among security professionals on risk assessments when the risk stems from intentional, malicious acts (i.e., criminal activity, armed conflict, and espionage), so–called "security risks." Fascinatingly, the idea that probability should play a role in risk assessments was being questioned by many security professionals.

Having a background in the sociology of risk, albeit 25 years ago, this raised my interest. If the history of risk has to be summarized in one word, it would be exactly "probability." Probability calculation has been viewed as "the underlying essence of risk" (Bernstein 1996; Burgess 2016, 3). Notably, "once risk is detached from probabilities it ceases to be a risk" (Furedi 2009, 205).

Given the centrality of probability,[1] why was it singled out and resisted in these security milieus, and why did other milieus object to it? What "happens" to risk estimates when probability is either removed or downplayed? The arguments were related to a dichotomy, namely the difference between security risks (intentional, malicious acts) and safety risks

[1] I do not differentiate between mathematical or qualitative expressions of probability or likelihood. See below.

(accidents, natural disasters). Security risks, the argument went, should be analyzed using a risk assessment approach tailormade for the special characteristics of security, and this approach should not include probability, as many security risks are unfit for probability judgements.

No-one would argue that war and a hurricane are “the same.” The concept of “security” is linked to conscious humans, with several relevant implications (potentially strategic actors, etc). The debate was, however, about the expression of *risk.* A key question was whether risk should be expressed as a combination of probability/likelihood and consequence (traditionally and well-known), what I label the two-factor approach (2FA), since it refers to two dimensions, or whether it should be expressed as a combination of values (assets), threats and vulnerabilities, labeled the three-factor approach (3FA), a supposedly better alternative for most security risks. The latter approach does not include, at least not explicitly, an expression of probability or likelihood.

From a classical risk-calculating perspective, taking probability out of an expression of risk makes a distinct difference: If alternative A is a risk with a potential consequence of 100 deaths (X) and a probability of 0,0005% that X will happen in the next 50 years, and in alternative B the probability of X is 50%, the risk, in a traditional risk calculation, would be much lower in alternative A than in alternative B. Probability turns unlikely futures into lower risks than likely futures, everything else being equal. A low-probability risk “becomes” a much higher risk without probability, the difference being far less for a high-probability risk. The implication from this perspective is that probability is essential for the expression of risk.

But what if one cannot estimate the probability because one simply lacks reliable data? The probability could be dynamic, moving from 0,0005% to 80% in a second if the “enemy’s” perspectives and priorities changes. Should one try to estimate probability given such uncertainties? The type of consequence of a risk could also be perceived differently. What if alternative A is a terrorist attack on the prime minister's office, making it difficult to govern, whereas alternative B is a traffic accident, something we all accept, since we still drive cars?

The question, at least as seen from the perspective of many security professionals, is how risks should be expressed if they do not fulfill, or are at odds with, key assumptions in a traditional risk assessment approach.

Implicitly and explicitly, in the debate among the risk and security professionals lies, I was convinced, questions of significance for society. If terrorism, flooding, and a pandemic are viewed as high or low risks, this might influence how we allocate resources, and what we do to prevent them. As the pandemic has shown, it also may influence what governments are held accountable for: "Why didn't the government stock masks when a pandemic was considered a high risk in the national risk picture?" In a "risk society," how we evaluate risk matters.

Consequently, the first puzzle that drew my attention was the idea that security risks should be expressed without a reference to probability, contrary to traditional understandings of risk.

Key to the development of my study was a report by the Norwegian Defense Research Establishment (FFI), commissioned by the Norwegian Defense Estates Agency (FB), comparing the two Norwegian risk assessment standards of relevance – seeing risk as either 2FA or 3FA (Busmundrud et al. 2015; NS 5814:2008, NS 5832:2014). The FFI report included an annex with verified interview summaries with nine risk and security professionals. The summaries represented a treasure chest for a sociologist, displaying fascinating perspectives and a diversity of reasoning and sensemaking on questions of risk in a security context. New questions arose, such as why risk assessment approaches should be divided along the dichotomy of "safety" and "security." My interest evolved into a larger curiosity as to how risk and security professionals (hereafter security professionals) reason and make sense of risk assessment, especially linked to security management practices.

The 3FA, presenting risk without probability as described above was published as a Norwegian Standard (SN 5832) by Standards Norway (SN), the main standard-setting organization (SSO) in Norway (see below).

The second puzzle arose in connection to a seminar held by the FFI, where the merits of the 3FA and the new standard (SN 5832) were discussed (2015). In the seminar, people from government organizations had active roles, but there was a curious absence of people representing and defending the standard. This raised several questions. What is a standard? How are standards made? Who are responsible for the content of a standard? Something that seemed very similar to a government product, and with people from government actively involved, was produced by another type of organization (an SSO), which seemed not to be involved in debating its own product.

In summary, the first puzzle driving this study is linked to the idea that security professionals saw the need for a separate approach to risk assessment for security risks, and that such risks should not be expressed through probability. This evolved into a larger question of how security professionals reason on risk assessment in a security context. The second puzzle is linked to the way the approach was developed, into a Norwegian standard.

The thesis will follow both paths, and along the way seek to unravel both puzzles.

1.1. Research Questions and Investigations

The thesis is built on a study of the development of a Norwegian standard for security risk assessment (2006–2014), and the debate that took place primarily after the standard was published in 2014 (2014–2018). Policies can be shaped, we may assume, by the characteristics of the *policy-making process* or by the *ideas and meanings* policies have for those involved (Fischer and Forester 1993; Schmidt 2008; Winkel and Leipold 2016). This study follows both paths. The overall aim of the thesis is to investigate why policies turn out in a certain way, and more narrowly, how the characteristics of standardization by SSOs, and understandings of risk management in a security context, may influence policy processes and outcomes.

With the puzzles described above in mind, the main research question (RQ) is as follows: *How can the establishment of the Norwegian standard on security risk assessment be accounted for?*

By the term "account for" and not "explain" the qualitative and interpretative character of the study is underscored. The study is exploratory, and utilizes an abductive, puzzle-driven approach. Such approaches take surprising or potentially contradictory observations as a starting point for the investigation. Abduction can be fruitful when sufficient explanations are lacking, driving an exploration for a "situational fit" between theory and empirical findings (Alvesson and Sköldberg 2018; Ashworth, McDermott, and Currie 2019; Timmermans and Tavory 2012).

The first part of the study investigates the policy process that led to the standard. The 3FA is viewed as a policy, and the process is viewed as a policy-making process, consisting of three distinct, historical phases. The first phase was when the 3FA was developed by the government (2004–2010), presented in a guideline on terrorism protection from three government agencies (Norwegian National Security Authority, Norwegian Police Security Agency, and National Police Directorate 2010) – hereafter NSM, PST and POD. The second phase (2009–2014) was when it was moved to a committee within SN and ended up as a Norwegian Standard (SN 5832). Lastly, after the standard was published, the content of the standard was debated in a somewhat larger group of risk and security professionals (2014–2018).

A policy process perspective (Weible and Sabatier 2018) investigates how public policies come about, that is, decisions – actions and nonactions – of governments or equivalent authorities regarding specific objectives (Weible 2018). The 3FA is regarded as a policy, developed in part by the government and in part by the "equivalent authority" of SN. The process perspective enables an investigation not limited by organizational boundaries. The study follows the 3FA's "journey" from one institutional context to the next. The historical timeline, combined with the distinctly different institutional phases, enables a case study approach with a within-case, longitudinal comparative design (Gerring 2007). In this part of the thesis, I ask the sub–question:

RQ1: Which elements of the policy process were influential to the institutionalization of the security risk assessment standard?

By the institutionalization of the security risk assessment standard (3FA), I refer to both the construction and publishing of the 3FA first in the governmental guideline, then in the Norwegian standard (SN 5832), and that it was maintained despite criticism afterwards. This part of the study utilizes, but also further develops, Kingdon's multiple streams approach (MSA) (Béland 2016; Kingdon 2013; Zahariadis 2016). Key to the MSA is the analytical assumption of three independent policy streams, namely problems, policy, and politics, but also policy entrepreneurs (PEs) and timing, utilising "policy windows." The abductive approach is open to theorizing, and the MSA is developed to incorporate institutional factors both as formal rules (Zohlnhöfer, Herweg, and Huß 2016) and as knowledge background and ideas (Béland 2016; Winkel and Leipold 2016). The three streams are also understood as logics, where problems refer to *what needs to be changed*, policies *how it should be changed*, and politics *who decides* (see article 1). This adjustment makes the MSA suitable for investigating a small-scale policy process.

This research study is particularly focused on the standardization process and the institutional context of committee-based SSO standardization (Wiegmann, de Vries, and Blind 2017). It draws on theories on standardization by SSOs, mainly from organizational studies (Brunsson, Rasche, and Seidl 2012; Djelic and Sahlin-Andersson 2006a; Gustafsson 2020; Higgins and Hallström 2007; Jacobsson and Brunsson 2000; Timmermans and Epstein 2010). This part of the study is presented in article 1, and I refer to it as the investigation of standardization.

In the second part of the study, I investigate how security professionals make sense of risk assessment in a security setting. Here, differences in sensemaking (Weick, Sutcliffe, and Obstfeld 2005), are investigated as a potential answer to the RQ. I ask the following sub–question:

RQ2: How do security professionals make sense of risk assessment in a security setting?

Articles 2 and 3 build on this part of the study. Article 2 investigates how the question of the probability of incidents is problematized and addressed by security professionals and discusses what this might tell us about security and risk. Article 3 investigates the sensemaking by security professionals of risk assessment in the context of security and protective security management (PSM). The main theoretical perspective is Michael Power's theory on risk governance (2004, 2007, 2016b, 2021) and his three ideal models of risk management logics, that is, risk management as *anticipation*, *resilience* and *auditability* (2014). The ideal models are not well known or utilised, but are here seen as heuristic tools of a sensitizing kind (Blumer 1954; Schwalbe 2020; Swedberg 2018). Power's risk governance theory is chosen because he sees risk as not only linked to anticipation and technical-scientific developments, but also as a management technique. Risk assessment thus becomes part of a larger context of governing, linked to phenomena such as internal control and auditing (Power 2007). I refer to this part of the study as the investigation of sensemaking.

The 3FA is within the sphere of security – intentional, malicious acts (Jore 2019). The study incorporates theoretical perspectives from security studies (Amoore 2013; Aradau and Van Munster 2007; Berling et al. 2021; Bigo 2009; Dunn Cavelty and Søby Kristensen 2008b). Both articles aim at cross-fertilization between insights from risk studies and security studies, academic traditions that have not "spoken" to one another until rather recently (Petersen 2012b).

A secondary aim of the study is also theorizing, especially linked to risk and security, taking the sensemaking by security professionals into account. In Chapter 7, I further theorize the risk logics and create a model of these logics and discuss the findings in light of the model.

The thesis takes it as a given that a controversy existed. Controversies and disagreements are embedded in much social activity when something of value is at stake. Consequently, what is of interest is not the controversy itself, but what it represented and how it played out.

The investigation utilises a combination of qualitative data from 40 interviews with primarily security professionals, fieldwork in 5 courses for practitioners in risk assessment, PSM and standardization, and lastly, an analysis of documents (see Chapter 6).

In summary, the study undertakes research in four areas:

- The standardization process:
    - policy process theory; and
    - the literature on standardization by SSOs; and
- The sensemaking process:
    - risk governance, linked to the sociology of risk; and
    - security studies.

The number of perspectives is a result of the empirical and puzzle-driven starting point. The theories were chosen because they resonate with and sensitize the investigation. The benefit of investigating both the policy process and sensemaking is that it provides a potentially richer understanding and cross-fertilization between the two parts. At the same time, it is at a certain cost, given the framework of a PhD thesis. The breadth of theoretical perspectives, the two parts of the study, the number of data sources, the qualitative research approach, etc., mean that each part is less elaborated upon. This also makes the thesis rather dense. I hope the reader will bear with me, and that the invested time will be worth the effort in the end.

1.2. Motivations and Contributions

The establishment of the 3FA in a Norwegian standard has not been part of a larger societal discourse. The process has raised little to no public attention, almost exclusively taking place among professionals. It is also a comparatively speaking small case by any matrix (number of participants, attention, length of policy debate).

Still, I have chosen to study this case because I see it as raising questions of more general interest. It becomes a lens for investigating standardization by SSOs and risk management, both governing trends characteristic of societies today (Ansell and Baur 2018). Both trends have been described as “boring” (Dunn Cavelty and Søby Kristensen 2008a; Lampland and Star 2009). They are “sinking below the level of social visibility, eventually becoming part of the taken-for-granted technical and moral infrastructure of modern life” (Timmermans and Epstein 2010, 71). Both are abstract phenomena, seldom part of political turmoil. As this thesis attempts to show, they are not trivial, have important implications, and should be investigated.

Protective Security Management in the Aftermath of a 2011 Terrorist Attack

The 3FA standard was developed during a period of extensive changes, both to the perceptions and management of security, in Norway and other countries. The US terrorist attack of 9/11 2001 placed terrorism firmly on the political agenda, also in the Norwegian context (Jore 2012). The process investigated in this study started with a coordination of guidelines on protection against terrorism that was initiated in the aftermath of 9/11.

In 2011, a right-wing terrorist bombed the Norwegian governmental quarters killing eight people, then shot 69 people at a youth camp. Prime Minster Jens Stoltenberg stated on the day of the attack that "the answer to violence is even more democracy, even more humanity, but never naivety" (Prime Minister's office 2011).[2] The immediate political and societal response after the July 22, 2011 terrorist attack has been noted for how it differed from responses after attacks in countries such as the US (Bjørgo and Jupskås 2021; Friedman 2011).

The 2011 terrorist bombed key government buildings, including the prime minister's office. A key question in the aftermath was that Grubbegata, the street of the government quarter, had not been cordoned off. This made it possible to drive a minivan close to the buildings. Security authorities had warned against this possibility, and a decision had been made to close the street, but the decision was not implemented. In the aftermath, it was considered a sign of the naivety of Norwegian society (Bjørgo and Jupskås 2021) and criticized by an enquiry commission (NOU 2012:14). One of the commission's main conclusions was that "[t]he attack at the governmental quarter 22/7 could have been prevented through efficient implementations of protective security measures that had already been decided upon" (NOU 2012:14, 15). The lessons learned "have more to do with leadership, interaction, culture and attitudes – than lack of resources, need for new regulations, organizational matters or larger questions of ethical significance [*verdivalg*]" (NOU 2012:14, 16).

The attack became a watershed moment in Norway's approach to protective security. A key question became the government's ability, or lack thereof, to protect critical assets and infrastructures. Audits, enquiry commissions, parliamentary hearings, and a new Security Act

[2] The Norwegian citations were all translated into English by the author.

all testify to the fact that protective security planning has, for the better part of the past 10 years, been high politics in Norway.

The 3FA standard investigated in this thesis is not directly linked to the 2011 terrorist attack. The attack is, however, relevant as a context for the debate under scrutiny. It also makes it interesting to investigate questions about security risk assessment and PSM in a Norwegian context. On the one hand, Norway, being a small, open Nordic European country, reacted somewhat differently to terrorism compared to countries with stronger securitizing traditions (Bjørgo and Jupskås 2021). On the other hand, PSM has featured high on the political agenda in the aftermath of the 2011 terrorist attack. The study is thus an investigation into how risk and security practices play out – become translated into (Berling et al. 2021) – a Norwegian context, in a situation where protective security goes from low to high politics. The high stakes that PSM has acquired in Norway may make the study especially valuable as a case for exploring more general trends in risk and security, see section 6.5 on questions of transferability (Schwartz-Shea 2014).

Positioning the Study in Relevant Literature

The aim here is to position the research in the relevant literature; see also Chapter 5. The first part of the study utilizes a policy process perspective. The policy process literature is mainly centered on government processes (Weible 2014), although such processes often take place across jurisdictions (Frankel and Højbjerg 2007) – something this case is an example of. Overview articles on the MSA do not even consider processes outside the government or public sphere (Cairney and Jones 2016; Jones et al. 2016; Shephard et al. 2021). A few studies have utilised the MSA on standardization by SSOs (Harcourt, Christou, and Simpson 2020; Rashid and Simpson 2019; Tang and Lima 2019). However, these have referred to transnational and international standardization, and not to a national SSO process. I have not found studies comparing policymaking within government and by an SSO.

Generally, SSO standardization is under-investigated within the social sciences (Brunsson 2000), within sociology (Timmermans and Epstein 2010), and from a policy process perspective (Botzem and Dobusch 2012). This thesis thus aims to contribute to both the standardization and policy process literature.

When it comes to the investigation of sensemaking, this belongs at the intersection between questions of risk- and security management. The risk-security nexus has primarily, although not exclusively (i.e., Battistelli and Galantino 2019; M. Boholm, Möller, and Hansson 2016; Jore 2019), been investigated in security studies and criminology (i.e., Aradau and Van Munster 2007; Corry 2012; Petersen 2012b; Wardman and Mythen 2016). Few of these studies have dealt with security professionals' practices, knowledge, or sensemaking about risk, although there are some exceptions (i.e., Jore and Egeli 2015; Nielsen 2020; Petersen 2013). When security professionals are studied, it is often within the realm of international relations (Adler and Pouliot 2011; Berling and Bueger 2015). Scholars have investigated how security professionals develop transnational networks (Bigo, Bonditti, and Olsson 2016; Hoffmann 2021), the development of privatized security expertise (Berndtsson 2012; Krahmann 2011; White 2015), and how security professionals negotiate their different roles within corporate security (Petersen 2013). A Belgian study has investigated security managers' and law enforcement agencies' thinking about risk in crime assessment (Klima, Dorn, and Vander Beken 2011), and identified two ways of reasoning, one being classical risk calculation and the other framed as "precautionary uncertainty" (2011), resonating with the current study.

Similar controversies are investigated from what I will later label a "first level" perspective, the perspectives and understandings of the risk and security professionals (see section 1.3 below). The US Department of Homeland Security has been criticized for not having implemented a rigorous enough risk assessment approach (Committee to Review the

Department of Homeland Security's Approach to Risk Analysis 2010; Doty 2015), probability neglect, worst-case thinking, and excessive spending on terrorism measures (Mueller and Stewart 2011, 2014; Stewart and Mueller 2020). From another perspective, Brown and Cox have criticised the Homeland Security for utilizing a traditional probabilistic risk assessment approach pertaining to terrorist threats after 9/11 (2011), modelling terrorism in essentially the same way as industrial accidents and natural disasters (G. G. Brown and Cox 2011; Eller and Wandt 2020). A probabilistic approach is not adequate for security risks, it has been argued, due to the lack of knowledge, and the strategic and calculating character of threat agents (Aven 2014; G. G. Brown and Cox 2011; Cox 2008).

In the Norwegian context, some relevant contributions exist. Jore and Egeli took the same controversy as I do as a starting point, and explore how different stakeholders within the petroleum sector regard probabilities when expressing security risks (2015). They found that specialists coming from safety regard subjective probabilities as adequate and necessary in security risk assessment, whereas security professionals with a "security" (malicious acts) background argue against probability estimates (2015). Other scholars have discussed in more general terms how risk assessment should be conducted in a security context (Abrahamsen et al. 2017; Amundrud, Aven, and Flage 2017; Askeland, Flage, and Aven 2017) and whether a best practice exists (Maal, Busmundrud, and Endregard 2016). Differences between safety and security (Jore 2019; Pettersen Gould and Bieder 2020) and corresponding challenges for management (Pettersen Gould and Bjørnskau 2015) are also relevant for this study.

Most social science research conducted on security or safety management in Norway has focused on civil preparedness and crisis management (i.e. Bye et al. 2019; Engen and Lindøe 2017; Fimreite et al. 2013; Jensen, Lægreid, and Rykkja 2019; Renå and Christensen 2020), on societal security (Lango and Lægreid 2011; Olsen, Kruke, and Hovden 2007) and within the "safety" area, as described above. Little research has been conducted on Norwegian security management (Norheim-Martinsen 2016), although some have investigated developments in the Ministry of Defense or the defense sector from a historical perspective (Bjerga 2014; Bogen and Håkenstad 2017; Norheim-Martinsen 2016; Synstnes 2016)

Research on civil-military questions exist both in the civil and defense research milieus (Bjerga and Håkenstad 2013; Endregard et al. 2016; Grunnan et al. 2020; Gustavsen and Haaland 2019; Hjelum and Lægreid 2019; Morsut 2021; Norheim-Martinsen 2019a), but mostly these studies have focused on preparedness and crisis management, and are thus of less relevance to the thesis.

In summary, although relevant contributions exist, I have not found similar studies in neither the policy process, standardization, risk, or security literature, and the study thus fills a gap in the literature.

Finally, this study contributes through its research approach and empirical "richness" in an under-investigated area assumed to be hard to access (Salter and Mutlu 2018). Sociologist Marte Mangset has rightly called for more use of qualitative or "soft" analysis on "hard" topics (2017). According to Wæver and Buzan, critical scholars tend to leave military security to the traditionalists in security studies (2016). This thesis contributes with new insights utilizing "soft" analysis on the seemingly "hard" world of security professionals.

The gap in the academic literature means that there are few studies to go into direct dialog with or to build upon, as pointed out also by Nielsen (2020). The extensiveness of this gap is a challenge, as a great deal must be defined, developed, interpreted, etc. in the investigation. This may complicate the reading, but also speaks to the novelty of what I am trying to accomplish.

1.3. Some Specifications, Limitations and Paths Not Taken

The 3FA is a specific way of judging risk and it has a history before the process investigated in this thesis; it is not only presented in the standard. The 3FA and the standard (NS 5832) are thus not the same (see Chapter 3). The investigation is, however, narrowed down to the process and debate of the standard.

For purposes of simplicity, I label the larger group of risk and security professionals and public servants investigated in this thesis as “security professionals.” They work on domestic issues, either developing risk or protective security management policies, conducting or receiving security risk assessments (see section 6.2). The discourse is directed towards malicious acts with societal – and often national – impact.

Several concepts are used in the investigation, such as “risk”, “security”, “risk assessment,” etc. I distinguish between first and second level perspectives. The first level perspective pertains to how risk and security professionals themselves use such concepts, including researchers engaged in questions of solving risk and security issues. This refers to what Brubaker and Cooper labeled “categories of practice” (2000). In Chapters 2 and 3, the concepts will be explained and contextualized at this first level. The second level is the level of the study where the first-level understandings of the security professionals are investigated and where the theoretical foundation presented in Chapter 4 lies, that is, what Brubaker and Cooper labeled the “categories of analysis” (Brubaker and Cooper 2000).

The distinction between first and second-level perspectives helps identify what this study is not. It is *not* an investigation of the 3FA and the standard NS 5832 to assist professionals or improve implementation (first level). It does not answer the question of the debate, that is, what constitutes a good security risk assessment. The aim is also not to understand what was “really” meant when the standard was created, but what the debate has “stirred up.”

The study investigates a Norwegian case, and translation into English is thus required, consequently altering meanings. The Norwegian term *sannsynlighet* refers to both qualitative and quantitative expressions of probability/likelihood. I use the term "probability" for both, sometimes referring to likelihood to underscore the qualitative character.

The term *sikringsrisikoanalyse* is used in the standard SN 5832 to describe the security-risk assessment approach investigated in this thesis. This literally means "securing-risk-analysis." Everyone agrees that it is a somewhat odd expression. In article 2 and in the introduction, I label it the 3FA. In article 1 and 3, the definition of risk was not the topic of the investigation, and I thus labeled it the "security risk assessment" (SRA) approach in these articles.

In some translations, I have stayed as close to the Norwegian meaning as possible. The word *verdi* is translated as "value," which is basically the same word. The term used in English in security management is usually "asset." As the term *verdi* – "value" – has a wider connotation than asset, it is better translated as "value". Lastly, English words are sometimes used in the Norwegian dialog, such as with the dichotomy between "safety" and "security."

Social science scholars should heed a caution: when terms such as "risk management" and "probabilistic risk assessment" are used, they are often assumed to imply a number of things, such as calculative cultures (Mikes 2009), where the future is seen as predictable, sometimes described as an economic, instrumental, or neoliberal logic (i.e., Aradau 2010; Hagmann and Cavelty 2012; O'Malley 2008; Petersen 2013). Such interpretations should not be assumed, however, as the meanings of these terms are "at play" in what is investigated. I would especially like to draw attention to the term "probability." To be sensitive to the sensemaking, I keep it open if probability has a quantitative meaning, if it is a judgement of likelihood, negotiated guestimate, based on intelligence or something else. For the same reason, I do not try to define key terms, such as "risk", "security," "risk management" etc.

Although the meaning of concepts, and to some extent the historical development of such meanings are key to the study, my aim is not conceptual history (Koselleck 2004). Probability theory within risk studies and mathematics (Aven 2014) is relevant, but not utilized.

Practices have programmatic (normative) and technological (operational) elements (Power 1997; Rose and Miller 1992). The programmatic elements of risk assessment are ideas and concepts about it, whereas technologies are the operations and tasks that practitioners perform when conducting such assessments. The two elements are intimately linked (Power 2007). In this study, I have studied the programmatic part, that is, the ideas about what risk assessments are and should be.

The 3FA standard (SN 5832) is for threats of different magnitude, from theft to war. The thesis deals mostly with sensemaking on the higher end of the threat spectrum, pertaining to national security. When applicable, it is also narrowed down to the question of *forebyggende sikkerhet*, which can mean "protective" or "preventive" security, here translated as the former (see Chapter 7).[3]

Much research on security practices investigates the tension between security and liberty (Bigo 2010; L. Zedner and Ashworth 2019). This is not the topic of this thesis, although it has potential implications both for this and other normative issues, such as prioritization and resource allocation. My priority has been to dwell on the sensemaking of professionals and to unpack meaning, as this is where I see the largest potential for new insights. In Chapter 7 I discuss lessons learned, and some normative implications of the study will be touched upon.

The thesis does not utilise psychological research, but much research on cognitive reasoning discusses matters of relevance to this thesis, such as availability heuristics and "probability

[3] In article 2, the concept "preventive security" was used, but when working with article 3 on protective security, I realised "protection" was a better translation than "prevention."

neglect" (Kahneman 2011; Slovic 1987; Sunstein 2005). The study investigates at a social, not psychological, level. I thus leave questions of rational decision-making and risk behind (Zinn 2016).

Lastly, although the study is about professional judgement, it does not go into theories of professions and professionalization.

1.4. Structure of the Thesis

Chapter 2 gives a very short introduction to risk assessment and PSM, seen from a first level perspective. Chapter 3 presents the Norwegian background and context. Chapter 4 gives a summary of the three articles. The reader is recommended to read the articles at the latest before Chapter 5 (theory), as chapter 5 cannot repeat in full the theory presentations in the articles yet builds in part on these presentations. Chapter 5 provides the theoretical discussion preparing for the findings and contributions presented in Chapter 7. At the end of Chapter 7, I reflect on the philosophy of science implications of an abductive approach and discuss if the theoretical perspectives are inconsistent from such a perspective.

Chapter 6 presents the research process, data and data collection methods as well as analytical approaches. It also presents some key concepts; ideal models, sensemaking, sensitizing concepts and logics. Section 6.4 presents my civil servant background – formal arrangements, methodological and ethical implications. This is supplemented by Appendix 1, where I reflect on my background and the research process. In section 6.5, I utilize Schwartz-Shea's six criteria to evaluate the trustworthiness of interpretive research, before I end with discussing questions of transferability of the findings.

2. Short Introduction to Risk Assessment and Protective Security Management

To understand and contextualize the study, a very short overview of risk assessment, risk management, and protective security management is needed. This chapter is primarily directed at those not familiar with risk management or protective security management.

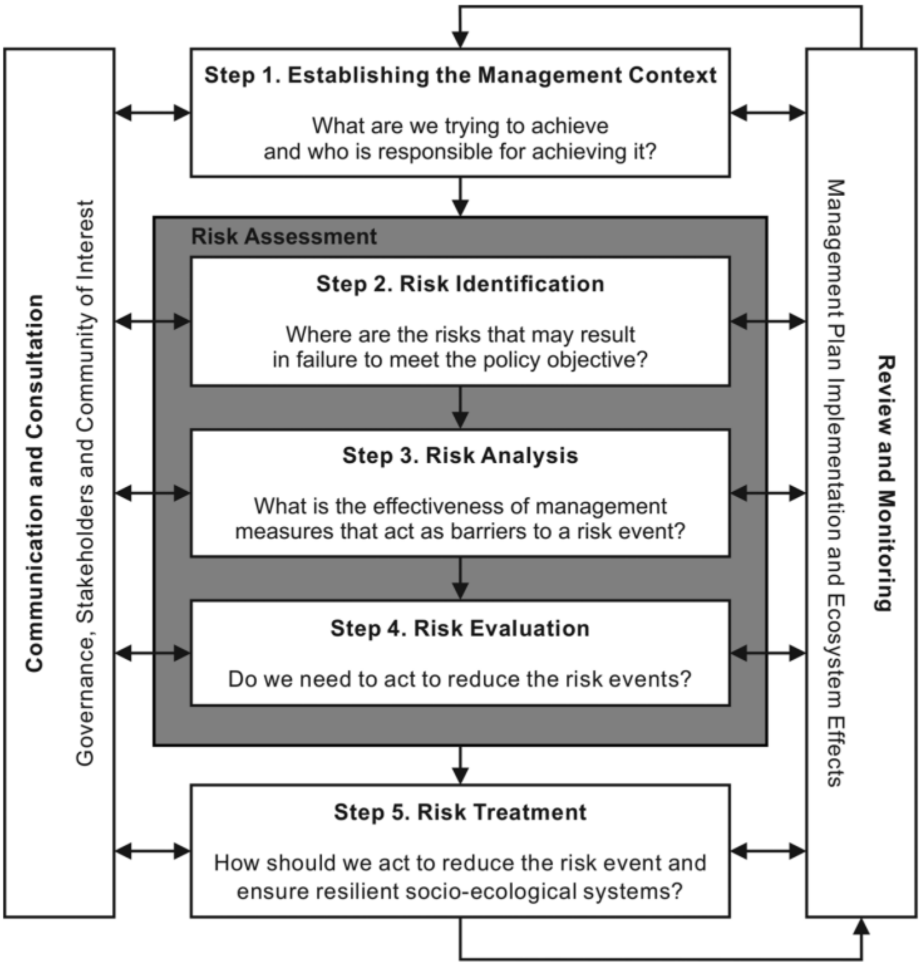
The topics under scrutiny are abstract and intangible. To make them more concrete and "material," I present visual representations when applicable (this and next chapter). As the intent is primarily the visualization, I do not give detailed descriptions of each figure.

2.1. Risk Management and Assessment

Since about the 1980s, risk assessment and risk management have been separated, where risk assessment is understood as the systematic, analytical process of trying to identify and understand risks (Demortain 2016), and risk management refers to all the activities carried out to manage and govern risk (Society for Risk Analysis 2018). The terms "risk analysis" and "risk assessment" are sometimes interchangeable, sometimes not. In the much-utilized risk management framework ISO 31 000, risk assessment is one element in the risk management system, and risk analysis is a sub-section of risk assessment – see Figure 1 (Creed et al. 2019, modifying Cormier et al 2013; see also NS 5814:2008). As this is not always the case,[4] and in line with Aven and Renn, I use the term "risk assessment" and avoid the term "risk analysis" unless in a quotation (2010; see also Thompson, Deisler Jr., and Schwing 2005). What the discussions in this thesis is about is not on the evaluative part (step 4 in Figure 1), it is about the identification and anticipation of risks.

Figure 1 Risk Management Framework –Modified Version of ISO 31 000

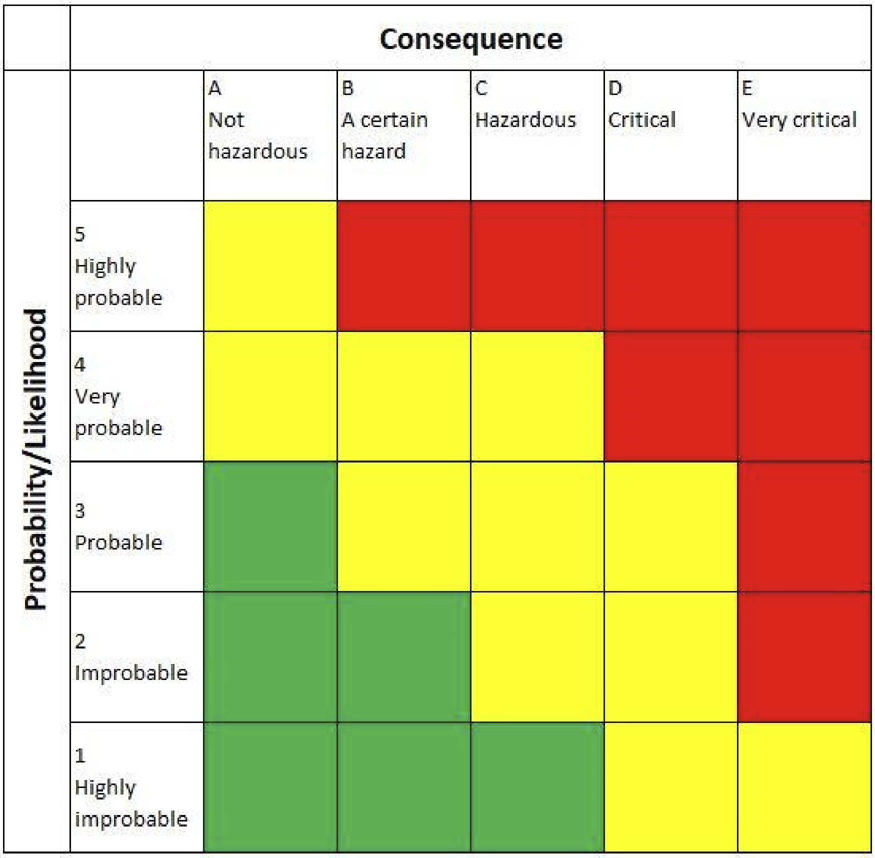
[4] In the standard investigated (NS 5832), it is the opposite; the broader concept is "risk analysis" and the more narrow concept is "risk assessment."


Step 1. Establishing the Management Context
What are we trying to achieve and who is responsible for achieving it?
Risk Assessment
Step 2. Risk Identification
Where are the risks that may result in failure to meet the policy objective?
Step 3. Risk Analysis
What is the effectiveness of management measures that act as barriers to a risk event?
Step 4. Risk Evaluation
Do we need to act to reduce the risk events?
Step 5. Risk Treatment
How should we act to reduce the risk event and ensure resilient socio-ecological systems?
Communication and Consultation
Governance, Stakeholders and Community of Interest
Review and Monitoring
Management Plan Implementation and Ecosystem Effects

One key distinction of relevance to this thesis is between quantitative and qualitative expressions of risk. Quantitative expressions are often seen as requiring sufficient amounts of historical data (Aven and Renn 2010).

A common tool utilized in risk management of relevance to this thesis is the so-called risk matrix, where different risks are mapped pertaining to the two axis, probability/likelihood and consequence. Such risk mapping is an instrument for setting risk appetite, assessing and ranking different types of risks (Jørgensen and Jordan 2016). There are several different versions of this, with varying levels of precision – see Figure 2.

Figure 2: Example of a Risk Matrix



		Consequence				
Probability/Likelihood		A Not hazardous	B A certain hazard	C Hazardous	D Critical	E Very critical
	5 Highly probable	🟨	🟥	🟥	🟥	🟥
	4 Very probable	🟨	🟨	🟨	🟥	🟥
	3 Probable	🟩	🟨	🟨	🟨	🟥
	2 Improbable	🟩	🟩	🟨	🟨	🟥
	1 Highly improbable	🟩	🟩	🟩	🟨	🟨

Many security professionals use a critical judgement of the risk matrix as part of their reasoning in favor of the 3FA.

The dichotomy of this thesis – risk as either 2FA and 3FA – is by no means the only possible expressions of risk, and it also somewhat simplifies the discussion that took place. One perspective of relevance is Aven and Renn's discussion of how characteristics of the risk problem should influence risk judgements and -governance (2020). They categorise risks pertaining to interpretative ambiguity, complexity, uncertainty, and normative ambiguity, and see probability as most relevant when risks are simple, that is, with well-known, "objective," probabilities available (2020). If not, more weight should be "placed on knowledge characterisations than on just the probabilities" (2020, 1128).

2.2. Protective Security Management

Security management is linked to the overall management system in an organization and pays special attention to the protection of the organization's assets (Smith and Brooks 2012).[5] Although there have been efforts to make security management into a science (Manunta 1997; Smith and Brooks 2012), the literature in this field is far less developed than the corresponding literature pertaining to areas such as industrial safety (Bieder and Pettersen Gould 2020; Blokland and Reniers 2019). However, a technical and practically oriented literature exist (i.e., Blokland and Reniers 2019; Martin 2019; Sennewald and Baillie 2020; Stranden 2019).

Protective security is linked to measures supposed to hinder or reduce the effect of unwanted actions (NSM, PST, and POD 2015). Martin has defined protective security as "the means of mitigating risks that arise directly from the potentially harmful actions of people such as criminals, terrorists, hostile foreign states, and malicious insiders" (2019, 4). Examples of protective security measures are military fortification and securing of critical objects (such as harbours, military camps), digital security cryptology, communication security, and personnel security (NSM 2022). Protective security also includes overall security management systems (Security Act 2019).

To demark the area investigated in this thesis from other types of security management, I use the term *protective security management* (PSM). It is not an established term, but is in line with the ideas of protection policies (Huysmans, Dobson, and Prokhovnik 2009; Kirchner and Sperling 2018), such as critical infrastructure protection (Argomaniz 2015; Dunn Cavelty

[5] Its (modern) roots can be traced to the industrial security programs of the World War II, with significant growth after September 11, 2001 (Collier and Lakoff 2008; Metscher 2015).

2008) Martin and the NSM use the term “protective security” (2019; 2020), but I regard it as important to link it to management (a guard may produce protective security, but not PSM).[6]

[6] “Asset protection” is an established term, but it includes both accidents and intentional acts (Davies, Hertig, and Gilbride 2015). In addition, the term “asset” has a narrower connotation, as described above.

3. The Norwegian Background and Context

This chapter gives the historical background and necessary context of Norway. The conceptual landscape presented in this chapter is anything but “neat.” When the concept of security is used alone, it mostly refers to intentional, malicious acts, as in the dichotomy of “security” versus “safety.” When the concept is used with a prefix, the meaning changes, such as with “societal security” – where the term “security” does not refer to malicious acts. Even more confusing, it changes depending on the perspective or policy field. As we will see, the meaning of “societal security” depends on if it is seen from the societal security side or from the national security/military side.

I use the term “national security” when the state is the referent object, that is, the goal is the security of the state (Wæver 1995).

This chapter presents the development of risk management and assessment in Norway. It starts with how these governing tools develops within what is often described as “safety,” not least linked to the offshore oil and gas industry. I will present the two different Norwegian risk assessment standards of relevance, and give a historical background for security governance, with special attention to PSM. I will show how the understanding of security has changed since the Cold War period, when national security was “everything” to the catch–all concept of “societal security,” and eventually how two versions of security conceptualisations exist in parallel. Finally, I will also briefly describe Standards Norway and the standardization process.

3.1. Introducing Risk Management in a Norwegian Context

The development of the offshore oil and gas industry in the 1970s and 1980s is often seen as the start of the development of risk management in Norway (Ryggvik 2008). This was a technically challenging and dangerous industry, experiencing severe accidents, most notably the *Alexander Kielland* accident, when an offshore platform tipped in 1980 and 123 people died.

In 1991, a requirement for an internal control system pertaining to health and security was implemented for all entities above a certain size (Ryggvik 2008). The first Norwegian standard on risk assessment, NS 5814, was developed the same year (SN 5814:1991). The standard took a technical-instrumental systems approach to risk assessment (see Rausand 1991), stating that risk "is expressed through the probability/likelihood for, and the consequences of, an undesirable event" (1991, 4). This standard, revised in 2008,[7] was of key importance to the controversy investigated in this thesis. It represented, or was at least perceived as, the technical way of understanding risk, developed with accidents and natural disasters in mind and with a 2FA understanding of risk.

Larssen and Rhinard have described the overall governing of security in Norway and Sweden as building on Nordic functionalist security studies (Hovden 2004; 2021; Sundelius 2005a). A functional approach emerged in the oil and gas industry. According to Lindøe, Baram and Braut, there was a striking differences between the US and Norwegian offshore oil and gas regulations: "At the beginning of the 1980s the Norwegian government replaced prescriptive…regulation with a unified system of enforced self–regulation […] with functional requirements and performance-based rules" (2017, 71). This is contrasted with the US system, where agencies have "been directed by law to carry out a prescriptive, technically detailed regulatory programme." (2017, 71). Functional rules are in line with the general Norwegian legislative tradition, where laws are short, general and vague, emphasising preparatory works (Fløysvik Nordrum 2020) and seen as expressing respect for expert knowledge and changing professional standards and norms (Molven 2009; Skotnes and Engen

[7] And also in 2021.

2015). Engen and Lindøe have argued that the Norwegian safety regime has traditionally balanced power and trust between regulators and the regulated, resulting in a hybrid system of limited prescriptive rules in combination with voluntary, professional standards and performance–based rules (2017).

To conclude, the Norwegian risk management regime that developed from the "safety" side built mainly on functionally based rules, utilizing indirect management tools such as risk management, internal control, and standards.

3.2. The Development of National– and Societal Security Policy Fields

We now turn to the two relevant policy fields, namely national/state security and societal security. This context is needed, to understand the policy process presented in article 1, but also to contextualize the differences in sensemaking by security professionals coming from different policy fields.

Norway is a member of the NATO, the only founding member with a border with the then USSR, giving it a strategic but exposed position during the Cold War. NATO has been vital in Norway's protective security work, such as through NATO's security directive of 1955 (Ot.prp.nr. 49 (1996–1997)). After the Cold War, it became important for security management to be regulated by law, not only internal directives. A Security Act was proposed by the Ministry of Defense, and enacted in 2001 (Ot.prp.nr. 49 (1996–1997)).

In the Act, the Ministry of Defense proposed a "National Security Authority" (eventually the NSM), with defensive and "protective" responsibilities (Ot.prp.nr. 49 (1996–1997), Security Act, 2001). The NSM now has the cross-sectorial responsibility for PSM pertaining to national security in Norway (NSM 2022). Its historical roots are from the defense side, but with dual governing by the MJ and the Ministry of Defense. The NSM is responsible for policy development, guidelines, educational measures, and audits based on the Security Act.

A key development of a risk-based approach to national security came through the first Security Act. According to the preparatory works to the Act, both NATO and Norway attempted in this period to go from a detailed, rule-based system, to a more risk- and cost/benefit-based system (Ot.prp.nr. 49 (1996–1997)). Notably, the challenges of a risk-based approach were raised already during the preparatory works, such as the difficulties of taking probability into account under high-consequence circumstances (Ot.prp.nr. 49 (1996–1997)). Key arguments in the debate under scrutiny were thus already displayed here, indicating that the perceived challenge of a risk-based approach to PSM is not new and, given the reference to NATO, not limited to the Norwegian context.

The Act gave the security authority (NSM from 2003)[8] a role pertaining to risk judgements (Ot.prp.nr. 49 (1996–1997)). To fulfil this role, NSM initiated cooperation with the technical university in Trondheim to develop methods for security risk assessment (Evensen 2000; Idsø and Jakobsen 2000; NSM 2006; Øksne and Furuseth 2004). These works defined risk traditionally, as a combination of probability/likelihood and consequence (2FA). There were, however, reactions to this interpretation of risk among some security professionals (Stranden 2019).[9] It was also contrary to how it had been described, albeit somewhat unclear, in the preparatory works to the Security Act: “the overall judgement of threat, vulnerability and value give the weighing of risk” (Ot.prp.nr. 49 (1996–1997), underline by author). This description is very close to how risk is defined in the 3FA discussed in this thesis, where risk is defined as “an expression of the relationship between the threat against a given value and this value’s vulnerability” (SN 5830:2012, underline by author). In both cases, risk is not

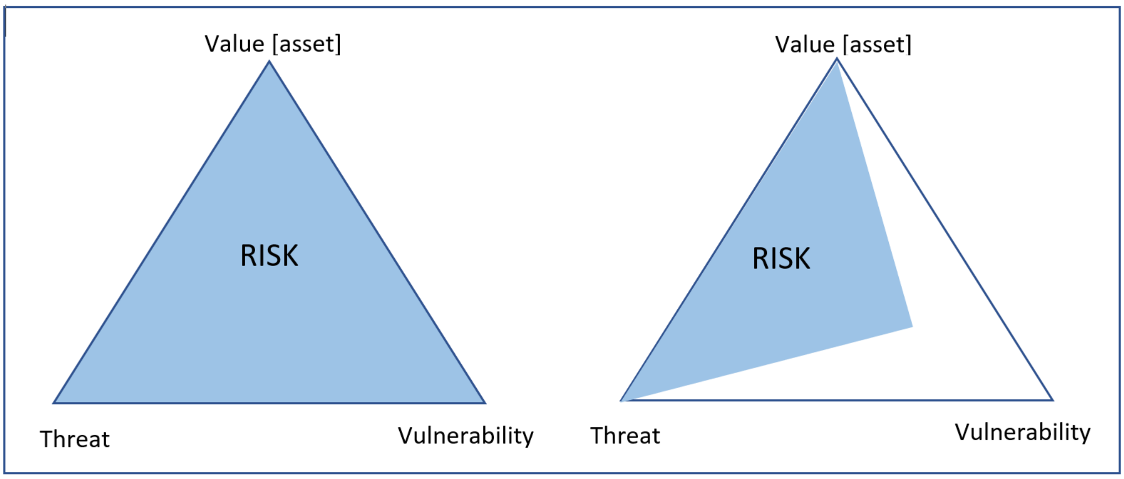
[8] At that time, it was the Security Unit at the Norwegian Joint Headquarters (FO/S).

[9] A handbook developed by Standards Australia on security risk management (HB 167 -2006) has been referred to as influential, with one of its definitions of risk being a combination of consequence, threat, and vulnerability, and another a combination of threat, vulnerability, and criticality.

expressed through an (explicit) reference to probability or likelihood. The NSM has visualized the 3FA as in Figure 3 (NSM 2015).[10]

One could argue that two understandings of risk developed in parallel in the national security milieus. Some milieus built on the traditionally based 2FA described above, while others promoted the alternative 3FA. Some have also argued for combining the two.

Figure 3 Risk – the three–factor model



Source: NSM 2015, 10

Although the preparatory work for the first Security Act described risk in a way similar to the 3FA, it was not until the process investigated in this thesis that it was extensively and more broadly discussed as an alternative approach to risk.

A revised Security Act was proposed in 2017 and enacted in 2019 (Prop 153 L (2016–2017); Security Act 2019; NOU 2016). The Act introduced a functional systems approach, where Ministries are responsible for identifying and having an overview over "fundamental national functions." The MJ and the NSM are given coordinating and auditing roles (Security Act 2019). A new concept of "sound security" [*forsvarlig sikkerhet*] was introduced: Risk judgements should be "the basis for measures that will secure a sound level of security in the

[10] The figure is translated and made by the author, to resemble the original Norwegian figure.

entity" (Prop.153 L (2016–2017, p. 8). In article 3, the sensemaking of the requirement of "sound security" is investigated. In addition to the functional requirements, there are several specific (prescriptive) requirements in the Act.

Summing up, we may conclude that PSM in Norway has been influenced both by risk approaches from the safety side and by requirements from NATO. An important development was the introduction of risk judgement requirements in the first Security Act. Two different conceptualizations of risk emerged, one defining risk similar to within the safety field, and the other as a combination of three factors, namely value, threat, and vulnerability. In the second Security Act, the concept of "sound security" was introduced as a requirement.

The Catch–all Concept of Societal Security

We now turn our attention to the development on the *samfunnssikkerhet* or "societal security" side.[11] Before presenting the societal security governing system, we need to take a step back and present the development of societal security as idea.

The concept of societal security has a civil and risk governance orientation, paying attention to regulation, contingency planning, and crisis management (Engen et al. 2016).[12] There are two historical paths of relevance to the development of societal security in Norway. One is described above, the development of a risk-based approach within "safety," not least in the oil and gas industry. The other comes from military planning during the Cold War. After World War II, Norway, similar to Sweden, introduced a strategy of "total defense" (Larsson and Rhinard 2020; Norheim-Martinsen 2019b), a civil-military cooperation, where large parts of societies' resources could be mobilized in the case of war (Norheim-Martinsen 2019b). It built on the social democratic values of communal mobilization (Håkenstad 2019), with a

[11] Also translated as "societal safety" (Olsen, Kruke, and Hovden 2007), "societal safety and security" (Høyland 2018), "public security" (Meld.St. 10 (2016-2017b), "homeland security" (Lægreid and Serigstad 2006) and "internal security" (Lango, Rykkja, and Lægreid 2011).

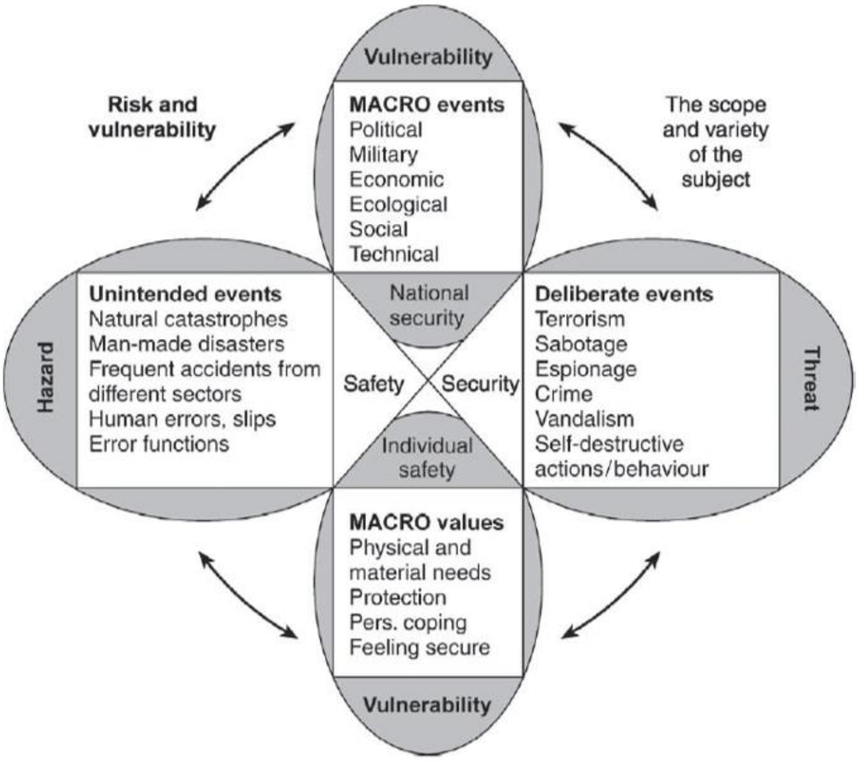
[12] This understanding is distinctly different from the Copenhagen school, where societal security is linked to society's collective identity (Roe 2016).

high level of civilian support (Børresen 2004; Haaland 2020). There is a path from "total defense" to "societal security," as both are conceptualizations of broad cooperation between civil and military security (Sundelius 2005b). During the Cold War this cooperation was on military terms (Norheim-Martinsen 2019). Subsequently, it developed into a system aimed at mutual support and cooperation between the civil and military sides (Endregard 2019).

As the Cold War ended, a need for change in security planning and priorities was identified. Several commissions and white papers were initiated by the MJ (i.e., St.meld.nr 24 (1992–1993; NOU 1995:31). In 1999, the Norwegian government appointed a public commission headed by a former prime minister, "the Willoch commission" (NOU 2000:24). The report, "A vulnerable society," introduced a new perspective on security, that of *samfunnssikkerhet* or societal security (NOU 2000:24). Under the heading of "societal security," a wide range of issues were presented, from food supply and transport, to organized crime and nuclear weapons, illustrated by Hovden, a member of the commission, see Figure 4 (2004, 632; Morsut 2021).

Societal security includes in this conceptualization both unintended (safety) and intended (security) events, from the individual to the national security level. Internationally, similar thinking resulted in recommendations of an "all-hazards approach" to safety and security (OECD 2010). The analysis was inspired by President Clinton's commission on critical infrastructure protection (Hovden 2004; 1997).

Figure 4 Societal Security as Understood by the Willoch Commission



Governing Societal Security

We now turn to the governing system of societal security. Norway has a system of strong ministerial responsibility. Whereas there is a single ministry responsible for military matters (Ministry of Defense), responsibilities for societal security issues are dispersed among various ministries and many subordinate agencies and inspectorates (Meld.St.5 (2020-2021)).

The MJ was assigned a coordinating role for emergency preparedness in 1994, strengthened by an internal control resolution (Kgl.res. 3. November 2000). The role was eventually broadened to societal security coordination. All civil ministries are required to establish an internal control system and conduct risk- and vulnerability assessments within their area of responsibility, regarding both intended and unintended incidents (Norwegian Ministry of Justice and Public Security 2017a).

The Norwegian Directorate for Civil Protection (DSB) was established in 2003, with a broad portfolio of responsibilities, one being to support the MJ in its coordinating role in the area of societal security (Kgl.res. 24. June 2005). One of the DSB's key responsibilities was to have an overview of vulnerabilities in society and initiate preventive efforts, and to develop a national vulnerability and civil preparedness report. I will get back to this when discussing the national risk picture.

Lægreid and Serigstad have described two policy fields within security; societal security (they label it "homeland security") with the MJ as responsible, and national security with the Ministry of Defense in charge (2006). There is however another distinction key to this thesis, between milieus working with intentional, malicious acts (police, the NSM) on the one hand and with societal security/civil preparedness (such as the DSB) on the other. All are under the jurisdiction of the MJ.[13] The first phase of the policy process investigated in article 1 pertains to a disagreement following these lines.

Somewhat simplistically, one may summarize that, during the Cold War area, "security" was understood through the lens of military needs and defense, closely linked to notions of national security (Åtland 2008). After the Cold War period, and especially after the Willoch report, Norway, along with especially Sweden, moved towards a holistic societal security approach (Larsson and Rhinard 2021). In this conceptualization, military threats and crime were just two among many security issues, and the most pressing needs were those on the civil side (NOU 2000:24).

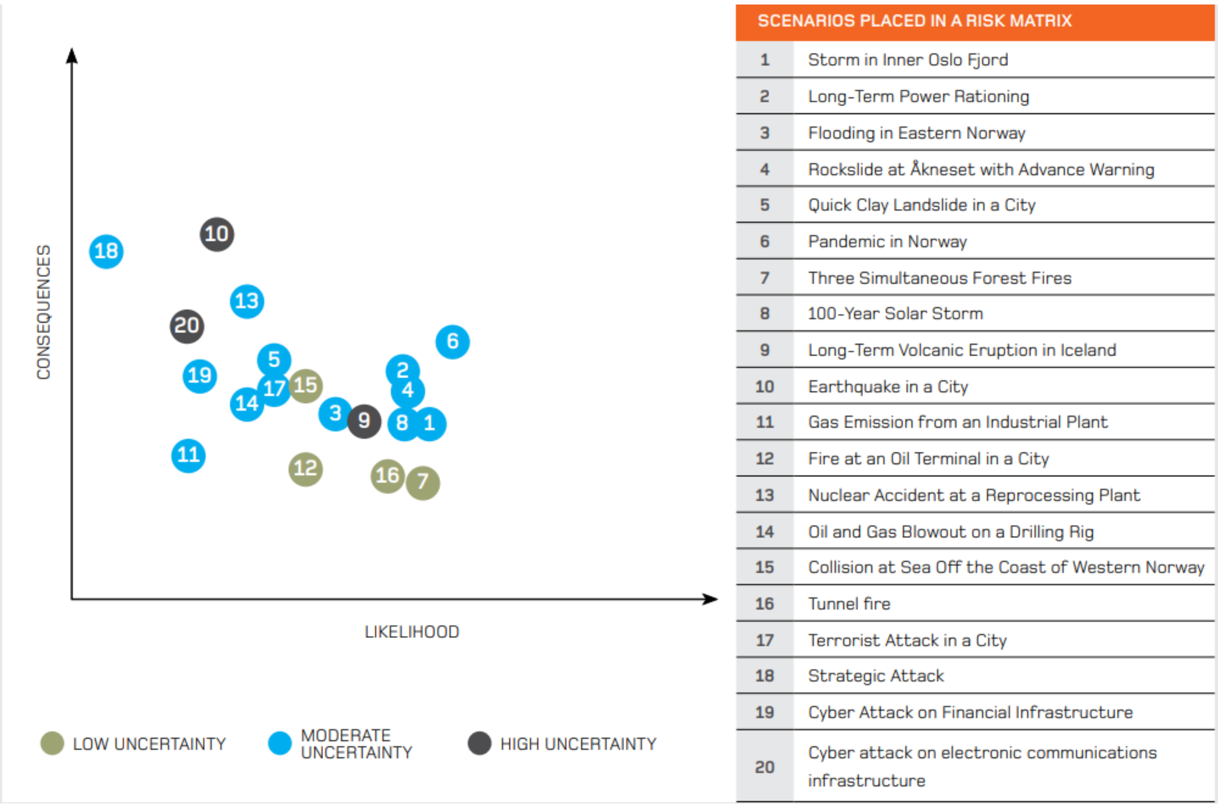
3.3. Should Safety and Security Risks be Compared?

I now turn to questions about whether "security risks" and "safety risks" should be presented and compared in a national risk picture, as the arguments raised represent a key context of the

[13] NSM has a dual mandate from both the MJ and the Ministry of Defense.

study. The DSB started to develop annual reports on national vulnerabilities and civil protection, and in 2011 they developed the first national risk picture (2011). The risk picture was developed based on similar work in Great Britain and the Netherlands (DSB 2011; Vlek 2013). The risks were grouped into three areas, natural incidents, major accidents, and intentional malicious acts. The risk picture was not meant to describe the most important risks at a national level, but to represent risks associated with a variety of realistic worst-case scenarios, analyzed for planning purposes (DSB 2011) - see Figure 5 (DSB 2014, 9).

Figure 5 National Risk Picture



SCENARIOS PLACED IN A RISK MATRIX	
1	Storm in Inner Oslo Fjord
2	Long-Term Power Rationing
3	Flooding in Eastern Norway
4	Rockslide at Åkneset with Advance Warning
5	Quick Clay Landslide in a City
6	Pandemic in Norway
7	Three Simultaneous Forest Fires
8	100-Year Solar Storm
9	Long-Term Volcanic Eruption in Iceland
10	Earthquake in a City
11	Gas Emission from an Industrial Plant
12	Fire at an Oil Terminal in a City
13	Nuclear Accident at a Reprocessing Plant
14	Oil and Gas Blowout on a Drilling Rig
15	Collision at Sea Off the Coast of Western Norway
16	Tunnel fire
17	Terrorist Attack in a City
18	Strategic Attack
19	Cyber Attack on Financial Infrastructure
20	Cyber attack on electronic communications infrastructure

The DSB's national risk picture was criticized by some security milieus (national security, police), arguing that security risks should not be expressed using probability, referring to the security risk assessment standard on terminology (SN 5830:2012), part of the same series as the one investigated in this thesis. It was argued that security risks should not be presented in a risk matrix together with safety risks. There is a consistency in the argumentation pertaining to the DSB's risk picture and the reasoning described in articles 2 and 3.

The reaction from security milieus led to changes in the risk picture of 2013. The report referred to the standard SN 5830, stating that security risks should not be expressed using probability (DSB 2013). Security risks were included in the report, but without probability, and these risks were not part of the visual presentation of the risk picture.[14]

In summary, seen from a societal security perspective, all risks of societal magnitude, also malicious acts such as terrorism and military attacks, are part of societal security and belong together in an overview of national risks. Seen from a national security perspective, "security risks" should not be expressed in the same way as "safety risks," and not compared with such risks in a national risk picture.

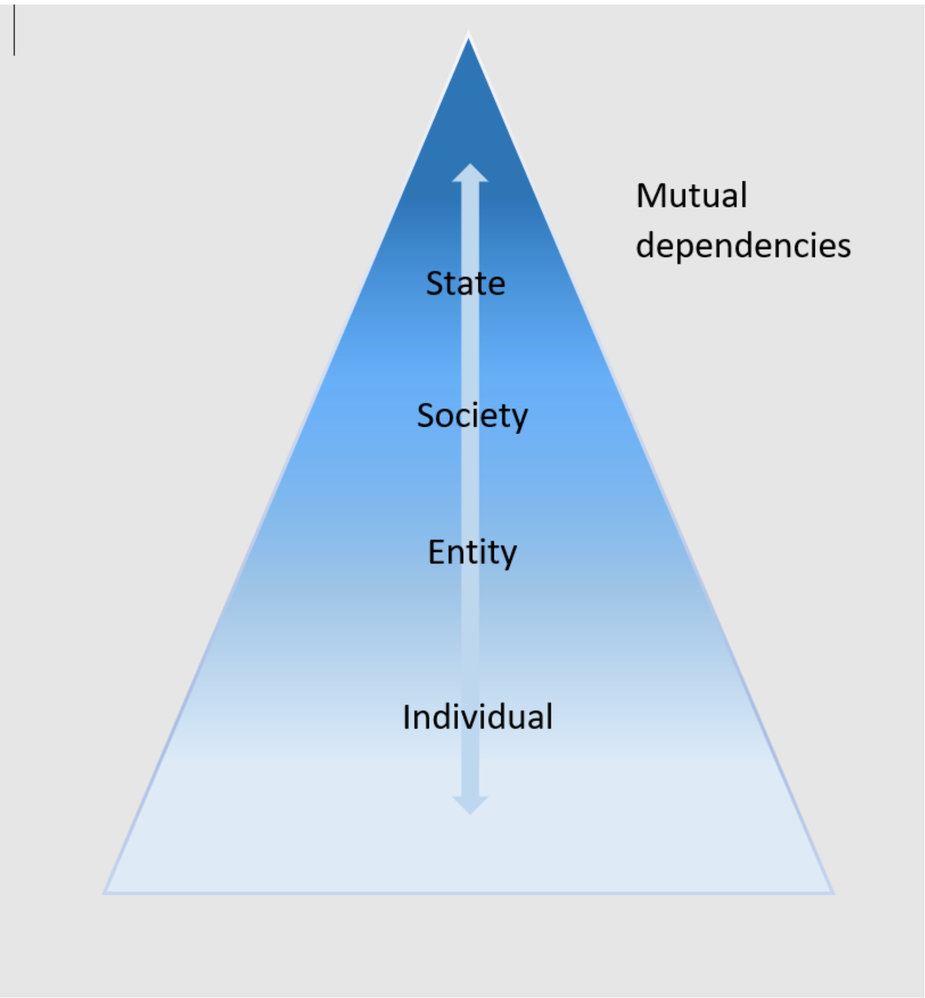
Picturing Different Types of Security from the National Security Side

Eventually, different conceptualizations evolved, also from the national security side. The concept of "state security" was introduced and linked to that which is traditionally taken care of by the armed forces and the defense sector (Norwegian Ministry of Justice and Public Security and Norwegian Ministry of Defense 2018). "National security" included mostly "state security", but also some "societal security" matters.

One visualization by NSM shows different types of security (NSM 2015, 9 see also NOU 2016) - see Figure 6.[15] Security here consists of four types: state, societal, entity, and individual security. Although not stated, it can be interpreted as a hierarchy, state security being at the top, sometimes referred to as "the pointed end of security."

[14] In 2014 the risk picture did include security risks. The next and to date the last report (Analysis of Crisis Scenarios) came in 2019, not including security risks in what is now labeled the overall risk profile (2019).
[15] The figure is translated and made by the author, to resemble the original Norwegian figure.

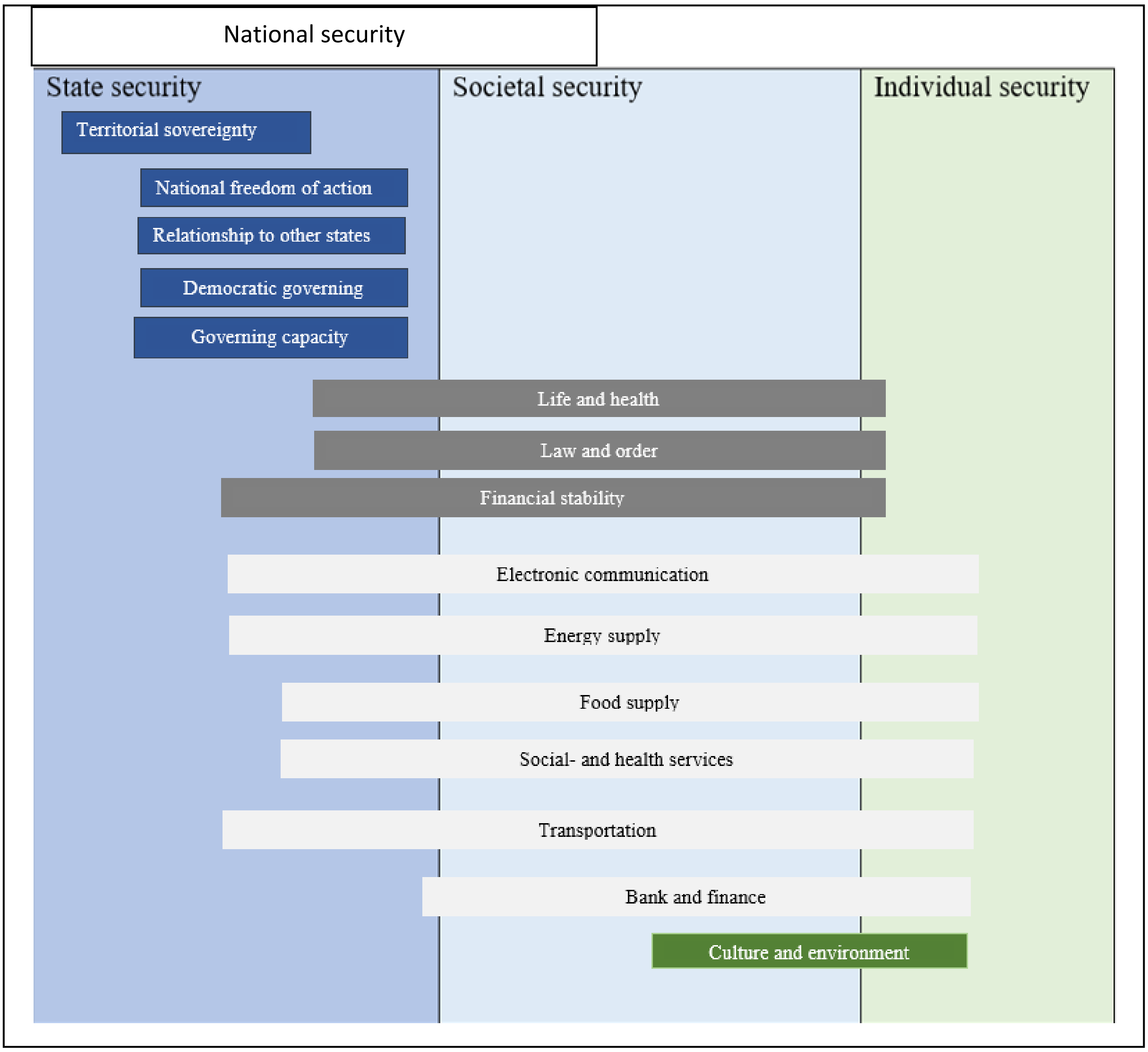
Figure 6 Levels of Security



Another graphical presentation comes from the pretext to the Security Act (2019) - see Figure 7. [16] Here, national security is portrayed as a combination of state security and societal security. It shows that national security is about a number of different things, from maintaining democracy to water supply.

Figure 7 Different Types of Security

[16] The figure is translated and made by the author, to resemble the original Norwegian figure.



In summary, different types of security are presented somewhat differently from societal and national security perspectives. The presentation of societal security in the Willoch report, as well as in the first national risk picture, regard all risks as part of societal security. From the national security perspective, during the Cold War, security was about “winning the war”, with both military and civil capacities. Eventually, a differentiated conceptualization of security developed, where national security is seen as a combination of state security and societal security.

3.4. Standards and Standards Norway

As mentioned above, standards have played an important role in safety management in the oil and gas industry (Antonsen, Skarholt, and Ringstad 2012; Engen 2020; P. H. Lindøe, Baram, and Renn 2013), but also, as this study indicates, in safety and security management more generally. Ending this background chapter, I provide a short presentation on Standards Norway (SN) and the relevant committee.

SN is an independent and non-profit membership organization, ruled by private law, publishing national and international standards. It was established in 2003, but its historical routes date to 1923 (Standards Norway 2021). SN is the Norwegian member of the European standardization organization Comtié Européen de Normalisation (CEN) and the International Organization for Standardization (ISO). When developing national standards, the process is based on international guidelines (ISO Directives and CEN's Internal Regulation) (Standards Norway 2018). The implementation of standards by national organizations is part of the EU's system of harmonising regulation (European Commission n.d.).

SN is financed mainly through selling standards, courses, etc., but also through grants, the largest from the Ministry of Trade, Industry and Fisheries (Standards Norway 2021).

The main principles of standardization by SN are the following (Standards Norway n.d.):

- **Openness**. All relevant parties can participate in the standardization process.
- **Voluntary**. Participation is voluntary. Participants must comply with established rules and regulations on standardization.
- **Consensus**. The goal is to achieve the "greatest possible degree of consensus," but not necessarily unanimity.

Table 1 presents an overview of how SN describes standards – bold in the original.

Table 1 Standards as Described by Standards Norway

Standards:

- Are developed after an initiative from **interest groups**
- Give **guidance** for which requirements should apply to products and services
- Regulates how **testing, certification** and **accreditation** shall be conducted
- Is a **proposal** for choice of solution
- Contributes to development of **beneficial** [*formålstjenlige*] **and secure** products, production processes and services
- Are often **voluntary** to use
- Give more detailed description to **EU-directives, national laws, and regulations**

(Standards Norway n.d.)

There is a clear distinction between SN's role as secretariat for standardization committees and the professional work done in the committees and working groups by external experts. "Experts" may represent expertise in the sense of exclusive knowledge on the subject matter or represent a stakeholder interest.[17] Technical committees (international) or national committees are overseeing the standardization activity, and working groups appointed by these committees, develop the standards (Standards Norway 2018). Participation in standardising is normally unpaid, that is, not paid by SN.

The committee responsible for the standard in question (SN 5832:2014) is the SN/K 296 on societal security in the building and construction sector (Standards Norway n.d.).[18]

[17] According to SN, approximately 3,350 Norwegian experts participate in national and international standardization in 2020. The total number of valid standards published by SN was 17,196 in 2020, most of them adaptions of international standards; 1,044 are developed in Norway (Standards Norway 2021).

[18] The committee responsible for societal security in general is the SN/K 211. The SN/K 239 Committee on Risk is responsible for the Norwegian NS 5814 on risk assessment and ISO/TC 262 Risk Management (ISO 31000-series).

Conclusion

The chapter has presented the development of risk management and assessment in Norway, and how two risk assessment approaches developed (2FA and 3FA) reflecting at least to some extent two security fields of “safety” and “security.” It has also given a historical background for security governance, and how the understanding of security has changed since the Cold War period, when national security was “everything” to the catch-all concept of “societal security.” I have also discussed how some national security milieus have delt with this development conceptually. Finally, I gave a brief introduction to Standards Norway.

4. Overview of the Articles

Table 2 Overview of the Articles

Article	Aim	Research Questions	Theory	Findings
Standardizing policy in a non-standard way – a public/private standardization process in Norway	Investigate the establishment of a Standard for security risk assessment as a policy process in three phases, utilizing a within-case, longitudinal comparative design	How can we account for the establishment of the standard utilizing an MSA perspective, and how does the different institutional contexts enable and constrain the policy process?	Adjusted multiple streams approach, supplemented with theories on SSO standardization	Policy entrepreneurs, characteristics of institutional contexts and "venue-shopping" between institutions were important for outcome. Ambiguous characteristics of SSO standardization seen as key. Introduces concept of "institutional deficit." Develops the MSA framework – incorporating two sets of institutions and the streams as logics.
Risk assessment without the risk? A controversy about security and risk in Norway	Investigate a controversy in Norway about the role of probability in risk assessment within security (intentional, malicious acts)	How is the question of the probability of incidents problematized and addressed by actors involved in the controversy over the standard on security risk assessment?	Michael Power's three ideal models of risk management logics, supplemented with elements from security theory	Those in favour of downplaying probability pay attention to probability's anticipating role, whereas critics point to its moderating role. Downplaying probability is interpreted as a subtle securitization move. The main reasons for downplaying probability are responsibility and security.
From prescriptive rules to responsible organizations – making sense of risk in PSM: a study from Norway	Investigate sensemaking by security professionals on risk assessment and management in a PSM context	How do security professionals make sense of risk assessment and the security risk assessment approach, and what does this sensemaking tell us about the use of risk assessment in PSM?	Michael Power's risk governance theory, three ideal models of risk management logics Security theory on protection	Risk assessment seen as more analytical than detailed, prescriptive rules. State's role as protector draws risk management in a risk-averse direction. Requirement to create "sound security" - potential for burdensome organizational responsibility and blame.

4.1. Article 1: Standardizing Policy in a Non-standard Way – a Public/Private Standardization Process in Norway

– review and resubmit to *Journal of Public Policy*

The article presents a case study of the institutionalization of a Norwegian standard on security risk assessment (SN 5832), investigated as a policy process. The article utilizes, and develops, the multiple streams approach (MSA), integrating both formal institutional characteristics and ideational elements linked to knowledge into the analytical framework. It also draws on the literature on standards and standardization.

The article finds both policy entrepreneurs and institutional contexts to be important for the institutionalization of the standard, but also the possibility to move between polities characteristic of polycentric governance. Special attention is given to SSO standardization. The in theory strong institutional barriers of SSO standardization did not work as such in the case, in that the policy field was split in two so that the institution in need of consensus consisted of those agreeing on policy. Contrary to the governmental phase, the rules and boundaries of the institution were thus negotiated during policymaking. The article also found that the differentiation between responsibility for process (SSO) and content (committee) makes the process vulnerable to both stream-independence and manipulation. The former materialized in the last phase, where SN did not relate to the policy debate that took place regarding its own standard.

4.2. Article 2: Risk Assessment without the Risk? A Controversy about Security and Risk in Norway

– published in the *Journal of Risk Research* (2022), volume 25, issue 2 (pp. 252–267).

The article investigates the controversy about the role of probability in risk assessment within security, and asks how the question of the probability of incidents is problematized and addressed by the actors involved. The key argument against estimating probability is that it is often difficult or impossible. Probability has, however, the role in risk estimates of turning unlikely futures into lower risks than likely futures. Those arguing against the 3FA point to the consequence of downplaying probability in risk estimates.

Utilizing Michael Power's three ideal models of risk management logics, but also insights from security theory, the article identifies a felt discrepancy in risk assessment. Security analysts are supposed to deal with threats as risks, implying scaling, comparison, and level of acceptance, but they are also supposed to create security, implying the opposite of scaling and risk acceptance.

4.3. Article 3: From Prescriptive Rules to Responsible Organizations – Making Sense of Risk in Protective Security Management – a Study from Norway

- published in *European Security* (2022)

The article investigates the sensemaking by security professionals on security risk assessment, linked to national security and PSM. The article finds that security risk assessment is seen as creating more analytical security management, compared to the prescriptive rules that have characterised the field.

Utilising Power's three ideal models of risk management logics, but also Bigo's investigation into discourses on protection, the article finds that national security and the role of the state as protector draw risk management in a risk-averse direction. The article argues that the Norwegian security risk assessment approach makes a tension visible, which will often be imminent in security risk management; the tension between the idea of creating security, linked to the state's role as protector, and of risk management, the latter creating flexibility to optimise outcomes.

The article discusses a requirement to create "sound security" and argues that this makes responsible organizations the focal point of creating security. The term "sound security" is Janus-faced, as it implies flexibility and choice in the planning phase, but the meaning may change in the case of an incident, where "sound security" implies that the incident should not have happened. The article hypothesizes that creating audit trails to document responsible process may become a priority in PSM.

5. Theoretical Frameworks

The purpose of this chapter is to provide a theoretical grounding that prepares for discussions in Chapter 7 on findings and contributions. The theoretical frameworks for the three articles are presented in each article, and this chapter builds on these presentations, but also expands and deepens the theoretical discussion. Most notably, considerable space is granted to give a theoretical grounding for the four risk management logics presented in chapter 7.

The study utilizes an abductive logic. Ashworth, McDermott, and Currie have explained abduction in the following way:

> Abduction stems from a puzzle, whereby there is an absence of an existing or sufficient theoretical explanation for data, causing the search for a new explanation. […] Puzzles prompt exploratory inference, and subsequent development of the best-fitting explanations, thereby combining deduction and induction to produce theoretical and empirical insights (2019, 320).

Abduction is *creative theorizing* (Swedberg 2014), where a "researcher is led away from old to new theoretical insights," searching for a "situational fit" between observed facts and theory (Timmermans and Tavory 2012, 170). One does not know in advance where the puzzles and inquiries lead. Accordingly, in this thesis, I have ended with quite a diverse set of theories.

I will start this chapter with presenting the main theoretical perspectives drawn upon in chapter 7, before addressing whether these theories are inconsistent from a philosophy of science perspective.

In the introduction, I asked the question: How can the establishment of the SRA as a Norwegian standard on security risk assessment be accounted for? Four literatures are drawn upon when answering the question: The multiple streams approach from policy process theory (1) and theories on standardization (2) in the first part of the study, and risk (3) and security

(4) studies in the second part. My presentation of each theoretical perspective must be somewhat limited, given the number of theoretical perspectives, and less contextualized in its own traditions than would otherwise be the case.

5.1. Policy Process Perspective and the Multiple Streams Approach

Policy process theory developed in the 1950s with the aim of integrating research on government and politics, with that of policy processes (Durnová and Weible 2020; Weible 2018). I argue that both the process within government, as well as the standardization process, can be seen as "public policies" and the thesis thus utilizes a policy process perspective.

Institutions and Institutionalization

One of the research questions utilize the term "institutionalization," and the theoretical framework also incorporates institutions. Steinmo sees institutions, in its broadest sense, as rules (2015). Scott has defined them as comprising regulative, cultural-cognitive, and normative elements that provide meaning and stability to social life (2014). Institutions create predictability and order (Jann 2016). In this thesis, both formal rules, but also ideas, what Schmidt labels the "structures and constructs of meaning" (Schmidt 2010, 1), are incorporated as "institutions."[19]

Institutionalization is here viewed as a process constructing, maintaining, and changing institutions (Scott 2014). Institutionalization can be based on the role of interests and incentives or be linked to the processes where meanings are produced (Scott 2014). When investigating the effect of formal rules, attention is given to the former.[20] When investigating

[19] (Neo-)institutional theory is relevant, and to a limited extent drawn upon in the investigation, such as when I draw on discursive institutionalism (Schmidt 2008). Due to lack of space and the number of theoretical perspectives, I do not present institutional theory.

[20] I do not suggest that this is the only role of rules in institutionalization.

the role of knowledge, and also the sensemaking by professionals, institutionalization is understood in line with the latter.

The Multiple Streams Approach

The multiple streams approach (MSA) was originally developed by Kingdon (first published in 1984), to explain agenda setting at the federal level in the United States (2013); and is one of the most cited books in public policy research (Béland 2016; Herweg and Zahariadis 2017; Jones et al. 2016). The MSA has been criticised for being "endlessly replicated and demonstrated, but not as fully exploited as it could be" (Greer 2016, 417). Innovative applications and theoretical developments have, however, occurred in later years (i.e., Bolukbasi and Yıldırım 2022; Howlett, McConnell, and Perl 2017; Reardon 2018; Winkel and Leipold 2016; Zohlnhöfer, Herweg, and Huß 2016).

Building on the garbage can model of bounded rationality, the MSA is based on two conditions, that of *ambiguity* and of *temporal sorting* (Zahariadis 2003). Ambiguity is a type of ambivalence, Zahariadis has argued, different from uncertainty, as more information does not reduce ambiguity, but it may (or may not) reduce uncertainty (2003). Temporal sorting implies that choices are made because of a simultaneous materialization of factors in time rather than that these factors are inherently correlated (Cohen, March, and Olsen 1972; Zahariadis 2003).

The two conditions (ambiguity and temporal sorting) make maneuvering possible, and the MSA is seen as particularly useful in challenging institutional settings, such as the analysis of EU policymaking (Ackrill, Kay, and Zahariadis 2013). As I argue in article 1, SSO standardization is ambiguous in several ways, and these conditions are thus a motivation for utilizing the framework.

At the heart of the MSA is the idea of three independent *process streams*: problems, policies, and politics. The problems stream consists of issues perceived as in need of being changed

(Kingdon 2013), and the policy stream of possible solutions. Consensus in the policy stream is built through persuasion and the diffusion of ideas. The politics stream describes the broader environment within which policy is made (Ackrill, Kay, and Zahariadis 2013). The political stream is influenced by organized political forces (Kingdon 2013), and consensus is achieved through bargaining, building coalitions, and other aspects of "playing the game" to win a sufficient majority/have authority to decide. The political stream clearly includes the struggle for power (Herweg & Zahariadis, 2017). The key assumption of stream independence is an analytical assumption, see article 1.

In order for policymaking to take place,[21] there is a need for an open "policy window" (Jones et al. 2016), often referred to as "window of opportunity." This occurs when all three streams are "ripe" (Engler and Herweg 2019) that is, a problem is pressing, a solution exists, and the necessary majority can be achieved. A policy window is an opportunity for policy entrepreneurs (PEs) to actively couple the streams (Dolan 2021).

Policy entrepreneurs are advocates willing to invest resources, time, reputation, and money to promote a favored solution (Kingdon 2013). The concept of PEs emphasizes the importance of actors actively engaging in "the politics of ideas" (Béland 2016, 233), and at the same time being rational and strategic, actively operating in particular contexts (Ackrill, Kay, and Zahariadis 2013) for certain gains. The two concepts of a policy window and PEs combine structure and agency, in that the window opens because of factors beyond the PEs, but the PEs take advantage of the opportunity (Kingdon 2013).

Adjusting the Multiple Streams Approach

The case investigated is radically different from most MSA studies, as described in article 1. I supplement the MSA in two ways. First, I incorporate two sets of institutional characteristics:

[21] Kingdon restricted the theory to agenda-setting, but it is also utilized on, for example, decision-making (Zohlnhöfer, Herweg, and Huß 2016) and implementation (Sætren 2016).

formal institutions, such as decision structures and number of veto points (Zohlnhöfer, Herweg, and Huß 2016), and "knowledge background," the latter linking the MSA to interpretative utilizations of the MSA (Béland 2016; Blum 2018; P. R. Brown 2020; Winkel and Leipold 2016), interpretive policy studies and discursive institutionalism (Durnová and Weible 2020; Schmidt 2010).

Second, I introduce a more radical change, seeing the streams as logics. There is no agreement among scholars on the nature of the streams (Blum 2018; Winkel and Leipold 2016). Those who have discussed the question most explicitly come from the discursive or argumentative traditions. Winkel and Leipold see streams as discursive patterns, unfolding through communication (2016). Streams are "perceptions of problems, policies, and politics" (2016, 108). They argue (rightly) that this way of understanding the MSA makes it a more internally coherent theoretical approach (2016).

As described in article 1, I see the *problem stream* as encompassing what needs to be changed, the *policy stream* is directed towards offering solutions, and the *political stream* consists of the struggle to get things the way one wants, that is, to create a necessary majority that can make a decision. Seeing the streams as logics make them independent of specific actors or organizations. Actors/organizations can move between arguments or concerns related to different streams and impact across streams. By labeling it logics, I assume that problems, policies, and politics each have a certain rationality and a structuring capacity independent from the two others. The streams have, as Zahariadis has stated, their own dynamics and rules (2003).

Seeing the streams as logics solves a challenge regarding the MSA in a small-scale case, pertaining to complexity. By theorizing that complexity and room for maneuvering can manifest itself in *qualitative* characteristics, it does not need a large number of actors, organizations, or policies.

My argument for utilizing the MSA in the radically different empirical situation, and adjusting it as described above, is that the underlying assumptions, such as ambiguity, temporal sorting, and analytical stream independence, but also key elements such as PEs and policy windows, are useful when investigating the case.

5.2. Standardization

Standards and standardization evoke ideas of uniformity and similarity (Brunsson and Jacobsson 2002). They may contribute to coordination between organizations, people, or countries (Olsen 2020b). The types of standards investigated in this thesis can be more narrowly understood as "a specific type of rule," that are "formally voluntary to potential adopters," (Brunsson, Rasche, and Seidl 2012, 615), although sometimes they become de facto binding. Standards are rules for common use (Rasche and Seid 2019).

Standard-setting organizations (SSOs) are voluntary meta-organizations[22] that create and publish formal, written standards (Higgins and Hallström 2007; Jacobsson and Brunsson 2000). SSOs such as the ISO and SN conduct committee-based standardization. In this type of standardization cooperation is the key coordinating mechanism (Wiegmann, de Vries, and Blind 2017). In their ideal-typical form, any interested stakeholder may join these committees (Wiegmann, de Vries, and Blind 2017). Committees are usually dominated by actors from the private sphere, to a lesser extent from public administration or NGOs (Büthe and Mattli 2011; Gustafsson 2020). SSOs typically aim at only one solution (Wiegmann, de Vries, and Blind 2017), such as only one definition of a concept across standards.

[22] Meta-organizations have other organizations as their members (Ahrne and Brunsson 2005).

The literature distinguishes between technical or non-technical standards, process or outcome standards, and *de jure* or *de facto* standards (Brunsson, Rasche, and Seidl 2012). A *de jure* standard is voluntary, but it is formulated as a set of rules that are compulsory if one chooses to follow the standard. The standardization process investigated in this thesis pertains to a non-technical, *de jure* standard regulating a management process. As a procedural standard, it specifies the steps that should be taken and how the risk assessment process should be performed on an abstract level.

Positioning SSO Standardization among Societal Institutions

Higgins and Hallstöm asks "how an originally modest, technical instrument of socio-economic coordination has attained the salience, ubiquity and authority that it enjoys as a discursive practice in today's global regulation" (2007, 685). This thesis pays attention to a more modest, but related, question of the many ambiguities of SSO's standardization.

Of relevance in this regard is Brunsson's comparison between organizations, markets, and standardization (2000). Standards, Brunsson argued, share with markets that they are voluntary – one can buy them or not. There is only a market for standards if they are perceived as good and thus worth following, the output legitimacy of standards (Botzem and Dobusch 2012). Standards also share with markets that, since they are voluntary, they generate fewer complaints than (hierarchical) organizations and thus less feedback (Brunsson 2000).[23]

Standardization by SSOs also share important traits with hierarchical governments, most notably that they create rules. Standards are sometimes labeled "soft regulation" and often co-exist with governmental regulation as a more indirect regulatory instrument (Ansell and Baur 2018; Baldwin, Cave, and Lodge 2011). Whereas governmental legitimacy rests on

[23] Sales numbers is the key feedback mechanism. This only gives market feedback, not on the content of the standard.

democratically elected officials, SSO standardization is legitimised more indirectly, not least through procedural legitimacy (Botzem and Dobusch 2012), as standardization is seen as an arena for bargaining and deliberation between stakeholders (Boström 2006; Engen 2020; Kalfagianni and Pattberg 2013).

It shares with government that it is a type of "governing," and standardization may be legitimized as more efficient or legitimate and a response to government failure (Hajer 2003; Sørensen and Torfing 2005). It may also be judged critically. Swyngedouw described such networked type of governance as a Janus-faced "governance-beyond-the-state" (2005; Djelic and Sahlin-Andersson 2006b). What is supposed to be empowering governing practices may de facto weaken civil society and democracy, as only some have the resources to participate, there may be an ill-defined system of representation, lacking explicit lines of accountability and where the "marked" becomes "the principal institutional form" (2005, 2003).

SSO standardization also relates to science and expertise. Standards are presented as "the distilled wisdom of people with expertise in their subject matter" (ISO n.d.), and "expert knowledge stored in the form of rules" (Jacobsen 2000, 41). As standardization is time-consuming, voluntary work, it is questionable whether experts – scientists or others – have the time and resources to participate without representing stakeholder interests. The consensus-driven approach is also at odds, one can argue, with scientific ambitions of "delivering high quality guidance… [not] the lowest common denominator of available options, at the expense of scientific quality" (Aven and Ylönen 2019, 280). A tension thus exists between SSO standardization as representing (scientific) "best practice" and negotiations between stakeholders representing different interests.

Zooming in on the responsibility of experts, Jacobsen has argued that "standardizers are seldom held to account for what they do" (Jacobsson 2000, 47). Although expert accountability can be challenging in many settings (Langvatn and Holst 2022), SSO standardization seems to stand out, as it is difficult to say "who is accountable to whom and for what" (Arnold 2022).

Finally, standards can be described as a tool between command-and-control regulation and no regulation ((Djelic and Sahlin-Andersson 2006b; Ansell and Baur 2018). There is a link between standardization, on the one hand, and inspections and enforcement, on the other, and hence the "auditability" logic, described in article 2 and 3, and built upon in the second part of this study (Power 2002). Standards such as ISO 31 000 on risk management becomes a system of compliance (Aven and Ylönen 2019) and reflexive regulation, where organizations are expected to observe themselves and make these self-observations visible to outsiders, that is, make them into auditable trails, where compliance can be negotiated (Power 2002, 2007, 2021).

In summary, several characteristics of standardization are ambiguous and "in-between" other societal institutions such as hierarchical organizations, markets, and science.[24] This lays the ground for SSOs fulfilling the MSA requirement of ambiguity, creating room for strategic maneuvering.

5.3. Risk and Security

In this part, I turn to the theoretical perspectives utilized when investigating the sensemaking. The section starts with a short history of risk and risk management; Power's risk governance theory and the three models of risk management logics will be incorporated into the general presentation. The risk management logics build on a historically situated "apparatus of risk"

[24] These societal institutions are here understood as ideal models, not as descriptions of an empirical reality, where i.e., government utilizes a mixture of several different institutions (experts, markets etc.).

(Power 2014), and thus synthesise complex insights on risk governance into "dense" models. Power's ideal models have to my knowledge not been utilized, not even by Power, and this study is thus an exploration of their potential as sensitizing concepts. Two of the models (anticipation and auditability) can be linked to the presentation of risk theory, the third model (resilience) to security theory. In Chapter 7, I further develop and alter these logics, and utilize them in the analysis of the case.

From Risk Assessment to Risk Governance

The emergence of "risk" as a phenomenon and concept is linked to developments of probability calculations – the idea that the future is, if not absolute predictable, then probabilistically predictable through "laws of large numbers" (Bernstein 1996; Hacking 1990). "By showing the world how to understand risk, measure it, and weigh its consequences […] risk-taking [was turned] into one of the prime catalysts that drives modern Western society" (Bernstein, 1996:1).

In these early phases, risk was seen as potentially both good and bad (Lupton 2013). Risk was *taken* to potentially gain wealth, but with the potential to create loss. The success criterion was the increasingly sophisticated probability calculation. Risk combined the probability of something happening with the magnitude of losses or gains (Zinn and Taylor-Gooby 2006). In terms of this understanding, risk is neutral (Lupton 2013). What is at stake is to get the calculation right. Power's first risk management logic – *anticipation* – builds on this conceptualization of risk (2014) and can be linked to risk assessment. The aim is knowledge about the future, using regularities from the past (Power 2014).

We may identify two connected reactions to this technical-instrumental (Lupton 2013) conceptualization of risk. One is directed at the lack of trust in science's ability to predict, and give advice about, risk (Jasanoff 1994; Wynne 1982). A reflexive awareness developed that science and technology not only are the masters of risk, they also produce risk (Beck 1992;

Burgess, Wardman, and Mythen 2018; Zinn 2008), climate change being a prime example.[25] The second disappointment relates to distributional consequences, as someone outside the risk-taking can potentially be harmed (Lupton 2013). Risk thus involves problems such as voluntariness, consent, and justice (S. O. Hansson 2007).

The causal dimension of risk is not only a technical or scientific matter, but also linked to someone's action and decision making (Å. Boholm and Corvellec 2011). Luhmann distinguished between seeing something as a risk or as a danger (Luhmann 1991). If we see a potential incident as contingent on decision-making, then it is perceived as a risk. If we think it "just happens" independent of our (the system's) decision-making, it is a danger. When something is a risk, this implies that it can be linked to a decision in the past that can be blamed for an outcome (Lupton 2013, referring to Mary Douglas).

In summary, risk is linked to two types of potential causation – empirical (a question of scientific knowledge) and human agency, that is, someone causes something to happen because of choices made.

Whereas Beck's risk society thesis sees a loss of responsibility, Luhmann sees the opposite. Situations are increasingly seen as dependent on someone's decision-making; there is an "expanded decidability of situations." (Power 2014, 375).[26] This creates a dynamic where more and more is seen as risks that someone (else) decided, and thus more and more is linked to responsibility, accountability, and potential for blame (Hood 2002).

Power describes a historical shift, where decreased trust created a need to look into, and control, experts and organizations dealing with risk (2007). This is challenging, however, as it

[25] The criticism is also directed at the idea that science gives the necessary information to base decisions upon. Scientists are mostly concerned with not saying anything false, even if this means that they can say very little, neither giving proof nor rejecting that something poses a risk (Beck 1992; Lewens 2007).

[26] Weather something is a risk or danger depends on the positioning of the observation, risk for decision makers are dangers for people outside the decision making (Battistelli and Galantino 2019; Luhmann 1991).

is difficult to assess when scientists or analysts in fact are doing a good job (Holst and Molander 2019; L. F. Hansson 1997). This is especially difficult with risk, since risk assessments are "complex counterfactuals about the distant future" (Pollack cited in Power 2007, 19). Thus "[t]he 'governing gaze' has increasingly shifted from the science of risk analysis itself […] to the organizational system within which it is embedded" (Power 2007, 19). Risk becomes key to organizations and organizational accountability (Hutter and Power 2005), and linked to management systems at large (Scheytt et al. 2006). Risk management merges with management in general (Hood, referred to in Power 2007).

In summary, we have identified two disappointments with scientific-technical risk assessment: one is the lack of trust in science, and the other linked to normative implications, including the calls for accountability and responsible decision-making. Very simplistically, we may identify two responses and debates following these concerns, which are echoed in Power's ideal models of risk management logics. One is the consequence of not trusting risk assessment's ability to predict, leading to more precautionary thinking (Furedi 2009; Klinke and Renn 2002; Sunstein 2005; Wardman and Löfstedt 2018) – see the ideal model of resilience below and "protection" as introduced by me in article 3 and Chapter 7. The second is linked to the management of risk, and how risk becomes a key organizing principle, that is, where procedures, systems, etc. are created to deal with potential harms (Hardy et al. 2020; Power 2007, 2021) –linked to risk governance and the auditability logic.

Risk Governance and Auditing

Power sees an intimate link between risk and organizations. Risk is "a powerful organizing category for managerial and administrative practice." (Power 2014, 371). Risk governance and internal control are enforced self-regulations (Power 2007), the latter turning "organizations inside out" (Power 2007; Power et al. 2009), so that they can be judged from the outside. Risk governance includes an idea of responsiveness to concerns from a broader community. In government conduct, this is linked to democratic ideals, whereas in corporate governance, it is linked to heightened calls for internal responsibility and the demonstration of legitimate conduct (Power 2007) In both, risk governance becomes a "benchmark of being a legitimate organization." (Power et al. 2009, 302).

Governance embodies two logics, Power argues, a neoliberal, managerial logic and a democratic and rights-based participative logic (2007). A valuable insight from Power is that auditing, internal control, and other tools often linked to economizing also, and maybe as much, are based on the perceived need to democratically scrutinize the internal workings of organizations, and for organizations to demonstrate trustworthy conduct (2007). The legitimacy claim of risk governance is mainly indirect, through society's trust in the management and control systems.

Power's risk management logic *auditability* builds on the premise described above, that risk is not only about knowledge, but about decision-making and corresponding responsibility (Douglas and Wildavsky 1982; Luhmann 1991). "The underlying feature of this logic is for risk management to be demonstrated and evidenced" (Power 2014, 386–387). Key to this logic is documenting processes to show responsible conduct. If there is no such evidence, the risk management did not occur (Power 2014, 2021).[27]

Power and colleagues have investigated *time* as a key dimension structuring risk in three "modes," *prospectively*, in *real-time*, and *retrospectively* (Hardy et al. 2020). In both articles 2 and 3, security professionals are sensitive to the difference in the reading of a situation before and after an incident. Few studies have analyzed the organizing of risk across the cycle, Hardy et al. argue (2020). The literature tends to assume that "the meaning of an object in relation to

[27] An auditability logic is not necessarily imposed from the outside. There can be a desire to externalize and objectify performance in an audit trail, as this can make organizational values operable, and they may acquire facticity in a way organizations would otherwise lack (Power 2021).

risk is singular and stable" (2020, 1032). They raise an important question, how different parts of the cycle influence other parts of the cycle. One could state this even stronger, that also the *prospect* of going through the phases influences dealing with risk, such as risk assessment approaches being influenced by ideas of what could happen in a retrospective inquiry and the "blame game" (Hood 2002).

A last social scientific perspective on risk of relevance to both Power and many of the cited security scholars is that of Foucault and the governmentality literature. Here, risk is considered a technology or practice – a *dispositif* (Aradau and van Munster 2007; Lupton 2013) creating "a specific relation to the future, which requires the monitoring of the future, the attempt to calculate what the future can offer and the necessity to control and minimize its potentially harmful effects" (Aradau and Van Munster 2007, 97–98). Attention is not on the ungovernability of risk, as with Beck, but on how it is actually "governed" and manifests itself through "riskwork" and systems of artefacts (Power 2016a), such as risk assessment standards.

5.4. Security, Securitization, and the Risk-Security Nexus

In this section I present the literature on security, limited to security studies. This is relevant for three reasons: to position PSM and "protection" in a relevant academic context, to present the idea of "securitization" as this is utilized (albeit briefly) in the discussion, and to present relevant understandings of risk and risk management seen from a security perspective. Whereas the risk-security nexus does not play a prominent role in the sociologically oriented risk literature, seen from the perspective of security studies, the distinction between risk and security "cannot be so quickly collapsed" (Aradau 2016, 291).

Security studies started as a distinct interdisciplinary field after World War II (Wæver and Buzan 2016). It narrowed its focus in the 1970s and 1980s, however, and gradually became a sub-discipline of international relations (IR) (Collins 2016; Wæver and Buzan 2016).

Traditionally, security relates to the defense of a sovereign state against external threats (Lucia Zedner 2009), with national security as the primary goal (Jarvis 2015). Security was eventually broadened to include other sectors than the military (Buzan, de Wilde, and Wæver 1998). It has also been deepened to new referent objects, such as individuals or (vulnerable) groups or institutions (Peoples and Vaughan-Williams 2021).

Securitization Theory and the Copenhagen School

Securitization theory, as described by the so-called Copenhagen school, offered a middle ground between a narrow and broad understanding of security. It kept the core focus of an existential threat, but broadened the security universe, linking security to certain types of speech acts, so-called securitization speech (Buzan, de Wilde, and Wæver 1998; Wæver 1995). This detaches security from the narrow referent object of the state.

Securitization speech acts present something as an existential threat to a designated referent object (Buzan, de Wilde, and Wæver 1998). A securitization process is successful if a relevant audience accepts the claim that an existential threat exists, and thus tolerates actions outside the bounds of normal political procedures (1998).[28] Securitization shortcuts argumentation and normal contestations with the argument that necessary measures must be taken. Securitization can be compared to raising a bet (Wæver 1995). This puts a special responsibility on those securitizing, since it "starts a process beyond democratic politics" (Buzan, de Wilde, and Wæver 1998, 211).

Securitization theory has as a key assumption that the security concept does something to politics (Berling et al. 2021). Securitization "blocks something specific and in a specific way: by defining what is not allowed to happen and can therefore be prevented with all means

[28] "Normal politics" does not possess any specific qualities, according to Wæver and Buzan (2020). It has however often been interpreted as linked to liberal and democratic societies, and the examples have often been drawn from such contexts (Buzan, de Wilde, and Wæver 1998).

necessary" (Wæver 2019, 17). The theory challenges attempts to present security solutions as natural and inevitable responses to threats (Berling et al. 2021).

Securitization theory, as developed by the Copenhagen School, has been criticized for lacking sensitivity to context (Ciută 2009), a criticism largely accepted by securitization scholars (Wæver 2011). Another criticism argues that there is a "Hobbesian trap," creating a blind spot for securitization theory and other critical scholars (Neal 2019). If any security politics is by definition "exclusionary and non-democratic," it excludes, a priori, the analytical possibility of finding forms of security politics that are not exclusionary and non-democratic" (Neal 2019, 13). This makes the detailed features of the political sphere less relevant for investigations of security issues (Neal 2019). A similar line of reasoning is put forward related to management, where the idea of military exceptionalism has left management questions mostly untouched within security and defense studies (Norheim-Martinsen 2016). This raises also the larger debate on whether legitimate public administration is not only based on its democratic anchoring – the concern of securitization theory – but also on a problem-solving capacity and the quality of decisions made (Christensen, Holst, and Molander 2023; Heath 2020).[29]

Lastly, the notion that securitization happens through speech acts has been criticized. Securitization often happens through "unspectacular processes of technologically driven surveillance, risk management and precautionary governance" (Huysmans 2011, 375). Securitization is not necessarily linked to the exceptional, but through routines and everyday practices (Nyman 2018; O'Malley 2010).

[29] What quality in security management would imply is challenging, see article 3. The point here is simply that "quality decisions" could be used as a yardstick for judging security practices.

The Risk-Security Nexus

The risk-security nexus is a key reference point of this thesis and, from now on, the perspectives presented in this chapter will be framed in light of this nexus.

Although risk and security both have to do with potential, uncertain adversities (M. Boholm, Möller, and Hansson 2016), they have largely been investigated separately (Petersen 2012b). The risk-security literature developed largely in the aftermath of 9/11 and the so-called "war on terror" (Amoore and De Goede 2005; Aradau and Van Munster 2007), but also investigations of "protection" (Bigo 2002, 2006; Bossong and Hegemann 2019) and the relationships between security and risk (Aradau and Van Munster 2007; Berling et al. 2021; Dunn Cavelty and Søby Kristensen 2008a; Petersen 2012a).

Amoore and others have argued that the principal technology emerging in contemporary domains of security is that of risk (i.e., Amoore 2013; De Goede 2008; O'Malley 2011; Petersen 2012b), where decisions must be made also when expert knowledge is insufficient. The limits of statistical knowledge of probability leads, Amoore and others have argued, to more speculative knowledges, such as scenario planning (2013). Here, risks are first imagined, and then actions are taken based on these imagined possibilities (2013). The potential catastrophic risk combined with the incalculability and uncertainty of risks introduces precautionary thinking and attention to possibilities instead of probabilities (Amoore 2013; Furedi 2009; Mythen and Walklate 2008).

Another relevant literature comes from investigations of the politics of protection (Bigo 2002, 2006; Huysmans, Dobson, and Prokhovnik 2009), see article 3. One meaning of "protection" is linked to the inside/outside of the state, where the state is seen as a "container" with walls (boarders) to be defended (Bigo 2009). Inside the "container," the Hobbesian sovereign state exists, with a social contract with its citizens (Søby Kristensen 2008).

In a newer understanding of protection, the clear inside/outside of the "container"/state is given up (Bigo 2009). Here, there is a grid that needs protection – a critical infrastructure. Mapping, monitoring, and risk management of vulnerabilities thus become the way to protect.

Critical infrastructure protection (CIP) is of interest to this study as much of what is deemed in need of protection, and a subject of security risk assessment, is CIP. The majority of critical infrastructure in Western countries are owned by the private sector. To the extent that the infrastructures are critical to national security, national security is created and shaped within the private sector (Dunn Cavelty and Søby Kristensen 2008b). National security thus needs to be "translated" into something the private sector can deal with (Petersen 2013; Søby Kristensen 2008).

Søby Kristensen has investigated the tension between the "exceptional" of security and corporate practices, and sees risk as a defining, but problematic, bridging concept (Søby Kristensen, 2008). When George W Bush, in the aftermath of 9/11 2001, stated that "every terrorist attack has a potential national impact" and the goal of Homeland Security is "the absolute protection of our citizens," the discourse was in line with a security logic and the sovereign state's social contract with its citizens (Søby Kristensen 2008). Since what is critical is privately owned, the government cannot act in a way traditional for security policy, the government utilizes "soft" measures such as "coordination," "facilitating," "encouraging" and "supporting" (2008). "By arguing in the terminology of risk, government and private sector actions are brought in line with each other," Søby Kristensen has argued (2008, p. 75). However, this leads to an unstable, "almost schizophrenic position" (Søby Kristensen 2008, 79). Risk-estimates based on cost-benefit and probability judgement imply that we should discriminate between various terrorist attacks based on their effects (Mueller and Stewart 2014; Søby Kristensen 2008). This is, however, diametrically opposed to the worst-case discourse of security (Søby Kristensen, 2008). Security is traditionally a binary concept: one is either secure or one is not (Manunta 2002). The risk logic is not binary; it is probabilistic, aimed at managing. To communicate both does not present a coherent or "stable" narrative (Søby Kristensen 2008). An existential threat and absolute protection justify strong and precautionary measures, but the logic of risk management is not consistent with this message.

Risk and Security – as Difference or Translations

Scholars have theorized about the differences between the concepts of risk and security. Corry has argued that we need to differentiate between a *security logic* and a *risk logic*, or securitization and "riskification" (2012; Friis and Reichborn–Kjennerud 2016; Judge and Maltby 2017; Macenaite 2017). Whereas threat focuses outward, and responses typically include deterrence, defense and offense, framing something as a risk produces security practices that are about probabilities, prevention, future scenarios, and management (Corry 2012).

Berling et al. are less concerned with accentuating the differences between risk and security and regard translations between the traditions and "disciplinary languages" as key (2021). Security and risk concepts embody distinct histories, but increasingly they are also connected and re-shaped (Berling et al. 2021). The authors have argued that "we are now approaching a situation, where these changes are often as important as the fixed categories and the predictable processes they encompass. Simultaneously, these changes can only be understood if taking into account those universes of meaning that actors speak from and how these are embedded in large societal patterns." (Berling et al. 2021, 4). In other words, "risk," "threat" etc. come from different traditions, but are also changed as they are "translated" into other disciplinary areas. In order to be sensitive to what is going on, we need to pay attention to the historical understandings rooted in different disciplines, but also carefully investigate the many different codifications that develop when actors coming from different approaches meet (Berling et al. 2021, 11).

Resilience is one of Power's risk management logics (2014), recognized as such also in security studies (i.e. Bossong and Hegemann 2016; Dunn Cavelty, Kaufmann, and Søby Kristensen 2015; Petersen 2017). In this logic, the existence of uncertainty and ignorance is accepted, and attention is directed towards creating resilience in the case of unforeseeable events, see article 3 and Chapter 7.

In summary, the relationship between security and risk management, and what security "becomes" when it is done through risk management, have been investigated in security studies. Risk management becomes relevant i.e., when the state's attention is drawn towards CIP. Søby Kristensen's investigation of the imbalance in the discourse on "security" and "risk" has been pointed out in particular.

5.5. Conclusion

The puzzle-driven and abductive approach of this thesis leads to several theoretical perspectives being drawn upon. Although the MSA is a more empirically grounded policy process theory, its premise of ambiguity and temporal sorting invites investigations also of the expert domains of risk managers and standardizers. There is thus room for including the sensemaking of professionals on issues such as risk and security.

Still, a question can be raised as to whether there are inconsistencies between the theories from a philosophy of science perspective. The MSA framework traditionally belongs to what Durnová and Weible have described as mainstream policy process studies (2020), and can resort under the umbrella of critical realism, where research functions mostly according to positivist criteria (Baert 2005), trying to find law-like patterns in the empirical material, with natural science as an ideal (Alvesson and Sköldberg 2018). Power's theory on risk governance and most of the security theories utilized, on the other hand, are grounded in some version of social constructivism (Agius 2016; Lupton 2013; Yanow 2014), where reality is conceived of as socially constructed (Alvesson and Sköldberg 2018).

I will argue along two lines for my study against such charges of philosophical inconsistency. First, the difference may to some extent be a question of how to interpret the MSA. Streams may be seen as discursive patterns, as described in section 5.1 above, unfolding through communication (Winkel and Leipold 2016). I see my perspective on the MSA as largely in line with an interpretative tradition, and compatible with Winkel and Leipold's perspective (2016). Rules can be seen as "sedimented discourse" (Hajer and Versteeg 2005; Winkel and Leipold 2016). When I do not describe formal rules and actions as "discourses," this is more a difference in framing rather than an incommensurable difference between the MSA and the other theories utilized in the study.

Second, abduction builds on pragmatism (Baert 2005; Swedberg 2014). From this perspective, puzzle-driven research does not start from one well-defined theory, but rather utilizes multiple theorical perspectives (Timmermans and Tavory 2012). "If our aim is to enrich the abductive possibilities of research, theoretical breadth is encouraged" (Timmermans and Tavory 2012, 173, referring to Henwood and Pidgeon). Theorists should, from this perspective, not "seek to uncover unchanging foundations of an all-embracing framework or science of the social" (Baert 2005, 153). The search for theories should instead be guided by their ability to help solve the puzzles, with interesting findings (Alvesson and Sköldberg 2018; Baert 2005), and their contributions to situational fits.

6. Analytical Approach, Methods, and the Civil Servant Background

The aim of this chapter is to present the research approach: data and data collection methods, research design, and analytical approaches. I also present some key concepts; "ideal models," "sensemaking," "sensitizing concepts," and "logics." I present and discuss the research implications of my background as a civil servant in section 6.4. A more self-reflective discussion is included in Appendix 1. Since the aim is in part to be reflexive, in chapter 6.4 I have allowed myself a personal voice. Finally, I utilize Schwartz–Shea's six criteria to evaluate the trustworthiness of interpretive research in section 6.5, before I end with discussing questions of generalizability or transferability of the findings.

6.1. Research Design and Some Key Concepts

The study utilizes an abductive logic, presented in the introduction to Chapter 5. There is a slight difference between the investigation of the standardization process and of sensemaking. Both are in line with Timmermans and Tavory's understanding, where "new theories depend on the inability to frame findings in existing theoretical frameworks as well as on the ability to modify and extend existing theories in novel ways" (James 1981, cited in Timmermans and Tavory 2012, 173). The sensemaking study is, however, closer to Alvesson and Sköldberg's description, where the abductive process is associated with hermeneutics and the emphasis is on interpretating the empirical through engagement with (theoretical) preconceptions and investigations (2018; Gilje 2017).

Below, I will present the research design of the case study. When it comes to sensemaking, the exploratory character of the investigation makes it more meaningful to discuss what is comparable to "design" in section 6.3 on the analytical process. In this section, I will present my understanding of some key concepts.

Case Study of a Standardization Process

The standardization process is treated or “cased” (Ragin and Becker 1992), as a policy process. As such, it is the movement and development both within, but also *between* organizations, public and private, and between different institutional arenas, which is essential.

The single case study utilises a within-case, longitudinal comparative design (Gerring 2007), analyzing the institutionalization process of the 3FA into the Norwegian standard SN 5832 (2006–2018). It compares three historical phases with distinctly different institutional arrangements. The first phase takes place within government, when three agencies developed one unified guideline on protection against terrorism (NSM, PST, and POD 2010), between 2006 and 2010. The second phase consists of the standardization process under the jurisdiction of SN (2009–2014), resulting in the standard NS 5832.[30] The last phase starts after the standard was published, as a debate unfolded among professionals and public servants on the content of the standard, between 2014 and 2018. What is analyzed are institutional characteristics, actions taken, and arguments raised of relevance to the 3FA becoming, and remaining, a standard. Whereas the boundaries of the case are relatively clear in the first and second phases, it becomes more difficult to draw the lines in the third phase, and what belongs to the “case” here is drawn more interpretatively.

The policy proposal (the 3FA) is the same in all phases, moving from one phase (institutional arrangement) to the next. The institutional context is different in each phase, whereas the outcome is the same, understood as the policy proposal (the 3FA) being successful (thus institutionalized) in all phases. In the first two phases, it is successful because a decision is made, in the last phase it is successful through a “non–event,” namely that the standard

[30] There is an overlap in time of approximately one year between phases 1 and 2, but the phases are still seen as independent as the overlap did not have a substantial consequence for either phase.

continues to exist despite criticism. The case is only a case because the policy proposal (3FA) is a constant, enabling the investigation. The design facilitates an investigation into how differences in the phases influenced the institutionalization of the standard.

I have chosen to utilise the multiple streams approach, or MSA. The theory builds on findings from a very different context (US policy making in the 1970s). The case investigated is very small in comparison; it involved far fewer participants, organizations, and policy proposals, and the participants differed, as there were no politicians, media or interest groups involved, but rather public servants and experts. From a case study and MSA perspective, it can be seen as a "least likely" case (Levy 2008), a design seen as suitable for testing the boundaries of the applicability of a theory. Abduction is not consistent with testing theory in a strict sense, but it is open to a deductive logic in a sequential way, in which theory is "tested" by looking at empirical findings, searching for a "situational fit" (Timmermans and Tavory 2012). The investigation thus explores the theory's ability to travel, its ability to "make sense" or "sensitize" (Blumer 1954; Timmermans and Tavory 2012) in a very different environment.

The study investigates a *national* standardization process. As little is known about such standardization, one does not know what type of standardization case it is – whether it is typical, extreme, etc., pertaining to such characteristics as participation, disagreement, and solutions. It is thus not possible to situate the case in a hypothetical larger universe of similar cases (Levy 2008; Ragin and Becker 1992). The idea of "similar cases" is also at odds with the studies intention to be sensitive to context. The investigation can, however, sensitize us to characteristics of standardization by SSOs, not least its institutional characteristics, see also section 6.5.

In summary, the study utilises a longitudinal, comparative design. The study explores the MSA framework's ability to make sense in a very different environment.

Sensemaking, Ideal Models, Sensitizing Concepts and Logics

The term "sensemaking" is intimately linked to meaning and meaning making (Alvesson and Jonsson 2022). Sensemaking research is typically about people's "capacity for turning complex and confusing circumstances into situations that can be comprehended" (Hultin and Mähring 2017, 567). I see sensemaking as social, developed "by socially embedded actors enacting a world through language use" (Helms, Thurlow, and Mills 2010; Sandberg and Tsoukas 2015, 9).

The investigation of sensemaking utilizes and develops Power's ideal models of risk management logics. An ideal model, or ideal type,[31] is a theoretical constitution (Rosenberg 2016) developed by Max Weber. He saw ideal types as theoretical, heuristic tools for social science analysis (Swedberg 2018). When constructing an ideal type, one accentuates what is seen as the key characteristics of an empirical case (Swedberg 2018). The ideal is created as a "thought experiment based on observed tendencies, which are gathered and distilled according to given logics and characteristics" (Byrkjeflot 2018, 22). Ideal types are used in a comparative way, in that the scientist can compare the ideal type to reality, with the potential for discovering something new (Swedberg 2018). An ideal type is not a hypothesis about the empirical, as the ideal type highlight observed tendencies from "acute angles" that cannot exist in reality (Byrkjeflot 2018, 22). Weber saw ideal models as context and time dependent, they will transform when the culture and society transforms (Byrkjeflot 2018).

My understanding and use of ideal models follow the description of ideal types given above. Michael Power's three ideal models of risk management logics are utilised heuristically as sensitising concepts in both articles 2 and 3. In article 2 they are introduced at the end of the article, reflecting the largely inductive process taking place. In Chapter 7, I develop Power's

[31] I use the term "ideal model," not "ideal type," in line with Power's use. I regard the terms as interchangeable.

three ideal models into four risk management logics, and also partly change their content, in order to create a "situational fit" between theory and findings, in line with the abductive logic.

Labeling the logics sensitizing concepts, underscores that the concepts are "grounded on sense instead of on explicit objective traits" (Blumer 1954, 9). Whereas "definitive concepts" give a clear definition of which attributes belong to a class of objects, sensitizing concepts "merely suggest directions along which to look" (Blumer 1954, 7). The sensitizing concepts have a truly exploratory aim (Blumer 1954). They attempt to stabilize meaning, but without giving it a "solid ontological existence" (Berling et al. 2021, 40). With sensitizing concepts, we are forced to accept that "what is common" (i.e. concepts) is expressed in a distinctive manner in each empirical instance (Blumer 1954).

In both parts of the study, I utilize "logics." Logics can be linked to discourse and rhetorical structure, as with securitization theory (Buzan, de Wilde, and Wæver 1998). "Institutional logics"[32] is a somewhat different framing, defining such logics more broadly to include "material practices, assumptions, values, beliefs, and rules" (Thorton and Ocasio 2008, 101). Institutional logics are "associated with a distinctive mode of rationalization – defining the appropriate relation between subjects, practices and objects" (Scott 2014, 90).

My use of "logics" is heuristic, both when I see the three MSA streams as logics (first part) and when I utilize "risk management logics" (second part). Seeing the MSA streams as logics tilts towards institutional logics,[33] as I do not only link it to "discourse," but also to actions and "what happens." It asserts that problems, policies, and politics each have a certain rationality and a structuring capacity independent from the other two. When the ideal models

[32] Thorton and Ocasio have defined institutional logics as "the socially constructed, historical patterns of material practices, assumptions, values, beliefs, and rules by which individuals produce and reproduce their material subsistence, organize time and space, and provide meaning to their social reality." (2008, 101).
[33] It differs, however, in that institutional logics often describe key societal logics such as "capitalism," "democracy" etc. (Scott 2014).

of risk management are described as “logics” in the second part of the investigation, they are linked to sensemaking and adhere more to a discursive understanding of logics.

In summary, by investigating sensemaking, I am concerned with how meaning is created in social contexts. The ideal models are seen as sensitizing concepts – they are theoretical, not empirical – developed to establish a “situational fit” in line with the abductive logic.

6.2. Data – Fieldwork, Documents and Interviews

This section discusses the different sources of data used: fieldwork, documents, and interviews. I present the data from what I regard as the least to the most extensive and important sources. As there are many sources, methods, etc., an overview may be called for before going through each part, see table 3.

Table 3 Overview of Data, Methods, and Analytical Approach

Parts	“Casing” / seen as	Design	Data	Data collecting methods	Approach/ methods	Techniques/ methods
Standardization	Policy process	Case study – within-case, long. comp. design	Interview transcripts Documents from MJ archive government, internet etc. Notes from ethnographic fieldwork	Semi-structured interviews Archive and literature search Ethnographic fieldwork at five courses *Only standardization*: *Case file application at MJ*	Process tracing Abductive “congruence” analysis/ situational fit	Sorting based coding in Nvivo Content analysis in memos Triangulation
Sensemaking	Sense-making	Inter-pretive research			Abductive, interpretative Ideal models as sensitizing concepts	Analytical and sorting based coding in Nvivo Memo and draft writing Triangulation

Fieldwork at courses

I have participated in 5 courses for practitioners. They were:

> ***Introduction to Standardization***, Standards Norway, Oslo 18–19 September 2017
>
> An open introductory course in national and international standardising by standard setting organizations, held by Standards Norway. Most people on the course were going to work with standardization at SN, ISO or CEN.
>
> ***Risk and Vulnerability Analysis***, The Emergency Planning College (NUSB) 24–26 September 2018
>
> A course in risk and vulnerability assessments (ROS) that covered key concepts, phases, and approaches to ROS. It included a section on security-risk assessment in line with NS 5832. Most participants were from government agencies and municipalities.
>
> ***Risk Assessment***, Norwegian National Security Agency (NSM) 18 September 2019
>
> A course in risk assessment from the perspective of NSM, that is, pertaining to security risks. Participants mostly worked in public agencies, but also the private sector, or as consultants.
>
> ***Security–Risk Analysis***, The Norwegian Business and Industry Security Council, 2–3 October 2019
>
> A course teaching the security–risk approach presented in NS 5832, directed at business organizations. Some participants also came from government.
>
> ***Basic Protective Security*** *[Forebyggende sikkerhet]*, NSM 7–10 October 2019
>
> A course in different aspects of PSM. A security clearance was required to participate. Participants worked in government or private organizations under the jurisdiction of the Security Act, or as consultants for such organizations.

Before and during the courses, I was open about my background and the reason for participating (research). Except for the course on standardization,[34] I asked permission in advance from the course providers that I could use the course information as a source under certain conditions.[35]

[34] At the course on standardization, I was open about the reason for my participation, but I had not agreed upon the terms before the course. I have thus used the course as background knowledge.

[35] If I wanted to cite from the course material or the presentations, I would ask for permission from the course providers in advance.
I have referred to one participant's statement at one course, but not cited the person (first article). This was in a conversation among only the two of us, and (s)he knew that my course participation was part of my research.

This part of the investigation follows basic principles of ethnographic studies, the most essential being observations on site, taking notes, and writing memos (Creswell 2018). My aim was in part to learn about risk assessment in the way practitioners do. I was also there with a more open, ethnographic agenda, searching for ideational dimensions, and observing language and metaphors, and things that "stood out."

I participated in the courses as a participating observant, taking part in the same way as the other participants, but being cautious, "becoming only as involved as necessary to obtain whatever information is sought" (Wolcott 2008, 51).

During the course, the notes were often close to what any participant could have made. At the end of the day, I wrote down broader reflections – impressions, anecdotes, observations, and loose thoughts. Relevant parts of my notes were coded together with the interviews in Nvivo (see below).

The fieldwork contributed to the study in three ways. It "thickened" my understanding of the field. It gave me insights that led to new paths of investigation. One example is how the course on basic protective security sensitized me to the "imbalance" between security and risk. This set me on a path to investigate the risk-security nexus. Lastly, I used the notes from the fieldwork to triangulate the other data sources.

Participating in the courses was something I could have done as a civil servant. It was thus at times challenging to observe as a researcher. At the end of the day, I often though, "there is not really much to note here." I took some notes, but they were not detailed in the sense of a full-fledged ethnographic study. Still, the fieldwork gave rise to important reflections and opened new paths of enquiry.

Documents

Documents were a data source in both studies, but for the sensemaking they played a more modest role. The following types of documents were collected and analyzed:

1. Documents stating relevant government policy, such as laws and preparatory work on laws, white and green papers, instructions, guidelines, handbooks, risk and/or threat assessments.
2. Documents in File Nr 2004_00153 at the MJ, pertaining to the first phase of the policy process.[36]
3. Other material, such as web pages, blog posts, newspaper articles, practically oriented research reports and books and commercial handouts.
4. Standards, primarily from Standards Norway (NS 5814:2008, NS 5830:2012, NS 5831:2012, NS 5832:2014),[37] ISO Standard 31 000 on Risk management, and other documents produced by standardization organizations, such as the Australian handbook HB 167–2006 on Risk Management.
5. Material on standardization (webpages, presentations) from Standards Norway, the ISO, and contract-based research on standardization (commissioned by the EU or Nordic standardization bodies).

See section 6.3 below on the analytical process, which includes document analysis.

Interviews

The interview data consist of 40 interviews. Nine of these were conducted by Busmundrud et al. in 2014 (see below) (2015). I conducted 31 interviews between 2018 and 2021. The total number of interviewees were 34, as some were interviewed more than once. Two people declined interview requests.[38] See interview request letter in Appendix 3.

Interviewees were selected combining strategic– and snowball sampling (Parker, Scott, and Geddes 2019). They were mainly risk and security professionals and civil servants, chosen for

[36] The file 2004_00153 at the MJ consisted of mostly classified material. I applied for access and most files were declassified, some only partly. I did ask for access also to the classified material and was given such access (I have security clearance). The agreement with the Ministry is that I will not write about classified information, and, if in doubt, I would discuss my use of information with the Ministry. The research questions and the interest of this study is of a kind where I have not had the need to utilize the classified information.
I was not given access to internal memos within the Ministry, in line with government policy. Through interviews and the other documents, I view my insight into the process as sufficient for the purpose of the study.

[37] SN 5832 is the standard investigated, but it is part of a standard series (the 5830-series), and the other standards are also analyzed.

[38] One because (s)he no longer worked in the relevant organization, thus referring to people in that organization. The other because (s)he remembered the process too poorly.

their insight into the debate and/or the policy process. I did not look for the "typical" security professionals, but people able to articulate an opinion, often influential in the field or in key organizations. The sample is thus not representative but chosen to elicit relevant perspectives on the controversy.

The interviewees are heavily skewed towards government, as government policy is important to national security and PSM. Some people from the private sector and research were included, because of their relevance to the study. Interviewees represent different perspectives, levels of government, and a variety of organizations. Some develop risk assessment methodology, while others conduct assessments, and yet others are recipients of such judgements. The interviewees did not speak on behalf of their organizations, but as experts/professionals.

I chose interviewees who work with risk management/assessment across different sub-disciplines, thus excluding people who work with one distinct security discipline, such as physical security, or within one area, such as railway security. I also did not include the local/municipal level.

Interviewees come from both security and safety milieus, but with more people from the former, given the subject matter – see Table 4.[39]

[39] The table cannot be too specific, as this would jeopardize the interviewees' anonymity. For this reason, the private sector and standardization are categorized together.

Table 4 Key Characteristics of Interviewees

Type of institution	Interviews	Interviewees	Organizations	Education[40]	Position	Gender
Ministry	9	9	5	Social science 10 Technical/practical 9 Law 5 Military 4 Police 3 Humanities 1 Medical 1 Business 1	Senior advisors 15 Leadership 12 Consultants 4 Researchers 3	Male 25 Female 9
Public agency	17	15	7			
Research	3	3	2			
Private sector/ Standardization	11	7	5			
Total	40	34	19	34	34	34

The interviewees come from a variety of backgrounds.[41] One “type” of interviewee often has a practical background, for instance from the military or as a craftsman, has security work experience and has completed part-time education, either within the military or in the form of an applied master’s degree from the UK or Norway. Another “type” is a social scientist working in an agency or a ministry and in this capacity has become engaged in risk management questions. Other backgrounds include technical-engineering and legal backgrounds.

Summaries of the interviews conducted by Busmundrud et al. are presented in an annex to their report (2015).[42] I coded relevant parts of these summaries and they are part of my data material. They are valuable primarily as a source of information for the third phase of the policy process, and to some extent with regard to the sensemaking. As these interviews were

[40] There are more people with work experience than education from the police and the military. Eleven interviewees work/have worked professionally within the defense sector, nine work/have worked within the police.

[41] The interviewees are referred to using a combination of letters and numbers. A for agency, M for ministry, R for research, and P for private/standardization.

[42] Their research was commissioned by the Norwegian Defence Estates Agency (FB), to compare the two approaches to risk presented in two standards (NS 5814:2008 and NS 5832:2014).

conducted at a different point in time, designed by other people and with a different purpose, I have mainly built my analysis of sensemaking on my own interview material.

The Norwegian Centre for Research Data has approved that the project complies with relevant regulations pertaining to data protection.[43]

The interviews were recorded with an audio tape recorder and transcribed in Nvivo using intelligent transcription.[44] Five interviews were transcribed by a master's student.[45]

Conducting the Interviews

The interviewees were ensured anonymity to encourage an open dialogue.[46] As described under the ethical considerations in section 6.4, full anonymity is sometimes impossible. As the interviewees in question knew this well, I regard their consent as accepting this premise.[47]

The interviews were mostly conducted face-to-face.[48] They lasted between 30 minutes and 4,5 hours. Most interviews lasted between 1 – 2 hours. The large variation in interview duration reflects in part "natural" variation, as some interviewees were key informants (Wolcott 2008). There was also a development on my part. In the beginning, I allowed the conversation to go on for a long time, whereas at the end I became more focused.

[43] Reference number 155948.
The requests were sent in part before and in part after the GDPR (General Data Protection Regulation) requirements. To secure equal treatment, those who were interviewed before the GDPR requirements received a new request in line with the GDPR requirements, see Appendix 3.

[44] This implies that it is the content of the conversation which should be conveyed through the transcribed interviews.

[45] She signed a non-disclosure agreement as part of the contract.
The last version of the interview request (after GDPR – see footnote 43), states that only I will have access to the taped interviews. This was not formulated in the same way in the first version of the request (before GDPR). It was included as it was a requirement from one interviewee, and to create coherence. The original request for the interviews transcribed by the master's student did not include such a promise.

[46] In article 2, I state that four interviewees were interviewed both by Busmundrud et al. and myself. As the former are not anonymous, this unfortunately jeopardizes anonymity to some extent. It is however not a total disclosure (we do not know which four out of the nine) and hopefully thus not seen as a breach of confidence.

[47] When using citations, I agreed with the interviewees that if there were any doubt about anonymity for the person or their organization, I would send the relevant citation for approval by the interviewees. I have asked for such approval for several citations, none were stopped or altered in the process.

[48] Because of COVID 19 restrictions, five interviews were conducted through video conferencing, one telephonically.

I conducted semi-structured interviews (Roulston 2010b). The interview guide changed somewhat as the project evolved, see Appendix 4 for an example (in Norwegian). Interviewees were sent a list of topics/overall questions in advance.

At the beginning of the interviews, I stated that the aim was an open conversation and that we would only talk about the topics he/she wanted. I also stated that there were no “right” and “wrong” answers on topics such as risk assessment – I was interested in their reflections.

I started the interview by asking for a brief account of the interviewee’s professional life history (Roulston 2010b). I also asked for a historical account of what has happened in the field of “security” management (societal, national) as they saw it, especially after the turn of the millennium. If applicable, I asked questions on the policy process (the phases they had knowledge of). This part of the interview primarily used a narrative perspective (Brinkmann and Kvale 2015).

The second part of the interview zoomed in on security risk assessment, and more broadly on questions of how to understand risk assessment in a security context. Elements of ethnographic interviewing were used, exploring “the meanings that people ascribe to actions and events in their cultural worlds, expressed in their own language” (Roulston 2010a, 12). This was combined with a more active approach, to explore the position of the interviewee in a “Socratic dialogue” (Brinkmann 2007). At times I critically challenged and “pressed” interviewees on certain issues.

The reason for the variation in interviewing, was that I did not only search for an interviewee’s own presentations and understandings. It is not only what interviewees talk *about*, but what they talk *from* that matters (Pouliot 2008). Both during the interviews, and in the analysis, I tried to “listen” and pay attention to both the representational accounts as well as potential underlying meanings.

I did not position myself in the controversy. In other words, I did not express, and I have also tried to not have, an opinion on what is the “right” way to do a security risk assessment.

Reflecting on my own interviewing was an important part of the process, facilitated not least by transcribing, coding, and memo writing (see below).

Limitations of the Interview Material

There is a great deal of variation in the interview material pertaining to perspectives and understandings. On the one hand, I see this diversity as beneficial, but on certain issues, the variation was a problem. It has made it difficult to identify consistent patterns and perspectives. This is amplified by what I regard as a relatively “thin” common, professional understanding (little authoritative literature, lack of common education, variation in descriptions). It may also be a result of my sampling strategy. Some of my interviewees see themselves as pioneers, and with some ideational power, and they might have developed their own conceptualizations and understandings.

A second limitation is linked to the exploratory nature of the study. At the beginning, I did not understand all the potential meanings of the concepts used (risk assessment, protective security). I came to realize that, in some interviews, what was talked about was not understood in the same way by the interviewee and me. One example is that one interviewee talked about preventive security (*forebyggende sikkerhet*) as preventing radicalization and terrorism, whereas I talked about it as used within the military and CIP. Some parts of interviews were therefore less utilised than others, because of such misunderstandings.

6.3. The Analytical Process

Investigating the Standardization Policy Process

The key analytical strategies used to investigate the standardization process were process tracing (Gerring 2007) and what in classical case study is labeled “congruence analysis,” to judge whether the case "correspond" (George and Bennett 2005), or, in abductive terms, "fits" (Timmermans and Tavory 2012) the MSA theory.

The transcribed interviews were coded in Nvivo with sorting–based coding (Tjora 2018), that is, codes constructed by me. The nodes for the process tracing were organized around a timeline documenting the course of events. When it comes to the MSA, I used nodes for the different elements of the theory, but also related to institutions and used a node for elements that did not fit the theory. See Appendix 5 for examples of nodes.

The importance of different data sources varied between the phases. Archive material from File No. 2004_00153 from the MJ was a key data source in the first phase, supplemented by interviews. In the second phase (standardization), interviews were the most important. In the third phase, both documents and interview data, displaying the different perspectives, were key.

Archive material from File No. 2004_00153 consisted of a number of letters and e–mails, memos, etc., which were analyzed using an Excel table, after which I conducted process tracing chronologically and content analysis of information of relevance to the MSA theory.

Different data sources (documents, several interviews) were triangulated to provide corroborating evidence (Creswell 2013; Natow 2020).

To establish "what happened," the key elements of the process were relatively simple. This is due to the simplicity of the process, but also because the sources, to a large extent, supported the same narrative. The three tables in article 1 summarize the analysis in each phase of the process.

What demanded more analytical effort was developing the theoretical framework. There was only partly "congruence" between theory and empirical material (George and Bennett 2005), creating a need for theorizing in line with the abductive approach. Again, the simplicity and clarity pertaining to the empirical data were a great advantage. I was in little doubt as to the importance of the institutional context, the PEs, and mostly also how to interpret the process in terms of the three policy streams. I could therefore dare to theorize.

Investigating Sensemaking – Coding, Analyzing, Writing

In terms of investigating sensemaking, the abductive approach is closer to hermeneutics (Alvesson and Sköldberg 2018). I utilised elements from different interpretative approaches. Techniques from grounded theory (Charmaz 2017; Tjora 2018), such as analytical coding and memo-writing, were important. I have also compared data (triangulation) and compared data with concepts (Adcock 2014; Charmaz 2017). My ambition was not in line with grounded theory when it comes to theory, as I did not intent to build concepts "from the bottom up," but looked for theories that could help me analyze the findings.

Although the study is not a discourse analysis, there are analytical elements obtained from discourse analysis. Attention is given to how the sensemaking is structured, the inner logic, and how it is represented – key to the idea of discourse in discourse analysis (Dunn and Neumann 2016). The analysis differs from much discourse analysis, however, in that I am less interested in language, and I am also not concerned with the link to power (although it looms in the background).

Zooming in on the analytical process, I started off with a rough coding into broad topics (probability, historical development, risk management, etc.) (see description of case study analysis above), then moved on to analytical coding (Charmaz 2017) within certain topics. Some codes were clearly analytical and "in vivo" (Alvesson and Sköldberg 2018), such as the statement "when it goes wrong, they are right," opening the investigation into the importance of temporality, responsibility, and blame. Other codes were constructed by me and more sorting based, but "closing in on" analytical coding – see Appendix 5 for examples.

To make meaningful contrasts, and necessary simplifications, I have given more attention to the “sides” of the controversy than those in the middle. At the same time, it is not “extreme” or peculiar positions that I looked for, but those representing a key position most clearly.

In some interviews, I felt uncomfortable about removing the code from the context of the larger interview, as it sometimes misrepresented the interview as a whole. To counter such tendencies, I decided to analyze some of the key interviews as separate entities, writing memos where each interview was an embedded unit of analysis (Yin 2009). I could then code the memo with both the citations, and my analysis and contextualization, together. The criterion for writing a memo was that the interviewee’s perspectives were not straightforward and clear; in other words, an analysis was needed. I wrote 12 such memos.

The exploratory and inductive character of the investigation, as well as the diversity of interviewees’ perspectives, made the coding and analyzing challenging in several ways. Very often I found that the text was about so many things at the same time, that it was close to paralyzing. Analyzing the data was a time-consuming, back-and-forth process between coding, comparing data, writing the analysis, and sensitizing the analysis and coding through the theoretical literature. I also conducted some additional interviews, in part aimed at “checking” some of my interpretations.

Comparing data has been key to developing both key nodes and findings. In many cases, it also forced me up the ladder of abstraction. Data that were on different matters on one level could be about the same issue at a higher level. One example is from article 2, where I conclude that some security professionals see their primary responsibility as creating a good risk assessment while others see it as creating good security. Here I find a pattern on a high level of abstraction in a material which does not necessarily communicate coherence at a lower level – they may talk about different things.

In article 2, I indicate which interviewees said something supporting each claim. In article 3 I do not refer to the exact sources for claims (except for citations). The latter is due to a development on my part, with a stronger emphasis on analytical coding. This makes the number of interviewees behind each statement less important than the analytical potential, that is, the potential for interpretation and understanding. I was still concerned with a certain level of "representativeness," that the statements represent key perspectives or sentiments within the larger discourse.

Lastly, the document analysis should be commented upon. This part of the analysis, relevant for both parts of the study, can best be described as content analysis, sometimes including discursive, argumentative, or conceptual elements (Boréus and Bergström 2005). The heuristic approach was chosen because most often only a small and relatively straight–forward element in the text was of interest: Is risk defined, and how? Is the standard mentioned, and how? I often wrote a brief analysis in memos, summarizing relevant texts.

In summary, I have utilised tools and perspectives from different interpretative traditions. The inductive character of the coding, the diversity, and also the abstract character of the inquiry, have made the analytical process challenging. Engagement with theory has been an important part of making sense of the empirical material.

Lastly, I will now turn to discussing and reflecting on my role as researcher, given my background from, and connection to, the civil service.

6.4. Can a Bureaucrat from a Ministry do Research? On Doing Research with a Civil Servant Background

"Will you be critical?" It was the first day of my PhD study at the Department of Sociology and Human Geography, and I was eating lunch with the staff. I tried to explain my PhD to a professor, who paused for a moment, before asking this question. Bingo! I knew this would be an issue, and I did not have to wait long.

I had asked myself the same question for quite some time. A ministry is a political institution with power, and key to its legitimacy is acting on behalf of the elected government. Civil servants have a certain duty to be loyal. A legitimate question is thus whether a civil servant from a ministry can do trustworthy research. This is in part a formal question. It is also linked to my abilities and perspectives as a researcher. Social location and – experiences shape and limit what one knows, – tacitly or explicitly (Rolin 2020). Although a research study's position should not be reduced to social properties and situatedness, reflecting upon their influence is key to trustworthy research conduct (Alvesson and Sköldberg 2018).

I will first present formal arrangements and whether there are requirements I have as a civil servant that could be an obstacle to the project. My professional background is presented, followed by some brief reflections on commitments and perspectives of relevance to the project. In Appendix 1, I compare my process with the process of another PhD candidate and reflect on the consequences of my background for the study, and the question of potential double loyalties to both the civil service and research. At the end of the section, I discuss methodological implications of my background and raise a few ethical considerations.

Formal Arrangements and Duties

I have had a leave of absent from the MJ to conduct the PhD research. The MJ is partly financing the research, and in part it is financed by the Norwegian Research Council. The MJ is also the project owner, as this is a requirement of the Public Sector PhD Program (The Research Council of Norway 2019).

The MJ and I have signed an agreement of scientific independence in line with relevant laws and ethical guidelines, guaranteeing the formal independence of my research (Appendix 2).

I started to work in the MJ in 2013, three years after the ministry played a limited role in the relevant policy process. Some of the discussions on security risk assessment took place during my time in the MJ, but I did not have a substantial role in these deliberations.

I am not doing research as a civil servant, but as a researcher. This builds on the formal arrangements, but to have the intended effect it must also be communicated. In all my encounters with interviewees and others, I have made clear my background, but also my agreed-upon independence as a researcher. To some extent, declaring independence facilitates independence.

One duty of civil servants is to carry out work in accordance with instructions given (Norwegian Ministry of Local Government and Modernisation 2019). Although not clearly stated, civil servants shall not voice external opposition or work against the will of the government on matters concerning their work as civil servant. This norm is not absolute, however. There are also obligations of truthfulness and professionalism (Norwegian Ministry of Local Government and Modernisation 2019). The norm is also limited to one’s own work area. Since my research is not directly related to my work, and I have gained access to data as a researcher, my background as a civil servant does not demand loyalty, formally speaking, in a way that collides with my obligations as a researcher.

Summing up, from a formal point of view, I am independent in my role as researcher. There might be subjective and emotional tensions between the two roles and corresponding loyalties, however. I reflect on this in the Appendix 1; see also the discussion below on “conceptual blindness.”

Author’s Background

I am a political scientist from the University of Bergen and Freie Universität, Berlin, with a minor in philosophy. My master’s thesis was about differences in scientific versus other (NGOs’) risk judgements pertaining to an international convention on the sea-disposal of low-radioactive material, utilising literature on risk and on scientific advice (Heyerdahl 1996). I have approximately 20 years’ work experience, mostly as a civil servant (Norwegian Ministry of Finance, General Audit Office, and MJ), but also as a university lecturer. In the MJ, I work in the Department of Public Security, in a section responsible for Analysis, Strategic Planning, and Audits. I was hired primarily for my knowledge on policy analysis. My responsibilities have been related to analysis, cross-ministerial planning and coordination, and to mandate research and research policy. I was the project manager for the White Paper *Risk in a Safe and Secure Society – On Public Security* (Meld. St. 10 (2016–2017b).

Before I started with the PhD research, I knew risk management principles and practices at a general level. I have never conducted a risk assessment but have occasionally given input to such processes.

To sum up, I am a security professional in a broad sense, working with societal security issues, but not in a narrow sense, as my background is not in security policy and not pertaining to malicious acts. There is certainly a familiarity and shared knowledge base with many of my interviewees, especially those from the ministries. Still, I view the study as about questions I have not worked with extensively (PSM, security risk assessment). I am an insider-outsider (Dwyer and Buckle 2009) investigating sensemaking and policy development in an area mainly different from my own background.

Methodological Consequences of Civil Servant Background

Alvesson and Sköldberg stated that “a strong feeling for the social reality under study can be insisted on as an important criterion for good research.” (2018, 369). My background entails such a "strong feeling for the social reality," and it has given me a good platform from which to investigate, from data collection to analysis. Access to elites for interviewing is often described as challenging (Goldman and Swayze 2012; Odendahl and Shaw 2012), but has not been so for me. Most interviewees were open and welcoming, often eager to present their position and discuss the issues raised. My knowledge has most likely enabled me to pursue issues more thoroughly during the interviews than without my background (Coar and Sim 2006). I perceived that rapport was quickly established with most interviewees (Warren 2012). In summary, there were many benefits due to my background when conducting the research.

My background shaped the data production and analysis in notable ways, and there are also potential drawbacks. I will discuss a few observations and reflections.

I noted the following after an interview:

> The interviewee stated, just before the interview started, something close to: "Well, I can say everything to you. You know what can be used [stated in public] and what cannot." I replied that I was interviewing him/her in the role as a researcher [not in the role of a public servant], and that (s)he should consider it in that way and answer accordingly. (S)he answered something like "you know what I mean," and I did not stress it further and started the interview.

The interviewee's statement contains a willingness to be open and, we may assume, also more honest, when the interviewer is a civil servant. I was given the role of the guardian, so that (s)he could be open. The line between the interviewee and the interviewed was thus "moved." In addition to responsibilities as a researcher interviewing, I was expected to take responsibility as a civil servant, not using information that "we both knew" should not be made public.

Not using internal information has not been too difficult, as the study is not directed towards detailed information of a sensitive kind. The statement exemplifies, however, that my connection to the MJ is part of the premise of the study, influencing the creation of interview data. My background has both methodological and ethical implications.

Being seen as a MJ civil servant may create (perceptions of) asymmetric power. If it is the MJ interviewing you, the answers may become important. For some, convincing me of their version of "the story," became, I sensed, important. My affiliation with the MJ potentially increased what was at stake, one may assume, with a corresponding urge for persuasion or positive representation. For others (a majority, I think), my background decreased the need to convince. I was perceived as "one of them," they could relax and did not need to "perform."

A second potentially negative outcome of me being familiar is a potential conceptual blindness (Coar and Sim 2006). Shared underlying assumptions may not have been exposed because I – the interviewee – have the same underlying assumptions as the interviewees. A key strategy to "estranging the familiar" (Timmermans and Tavory 2012, 177) has been to engage with the relevant academic literature – see Appendix 1. Equally important are tools and principles from qualitative methods. It is the combination of systematic data-handling and analysis, as well as sensitizing my investigation through theoretical encounters, which hopefully created sufficient distance and rigor to my investigation. Key is also my affiliation to the Department of Sociology and Human Geography at the University of Oslo as a PhD-fellow. I actively drew on their staff and others to reflect on and criticize my conduct and interpretations.

Ethical Considerations

The citation above about being more open because of my connection to the public service also indicate ethical consequences of my background. The interviewees might have been more open than otherwise, trusting that my use of the interview would be in line with their thinking. Being more open and "off guard" could, we may assume, make them feel misrepresented or misused, given that I do not simply put their perspectives forward. They may feel that my interpretations are unfamiliar, maybe even alien, and not represent their intended meaning. Hammersley has argued that one should do research "with" rather than "on" people, and criticizes some discourse analysis as potentially being a deception of the interviewee's consent (Hammersley 2014). Although I have sympathy with the perspective, I also see it as too limiting. The insider perspective must also be challenged. My key strategy to deal with this potential concern is to grant anonymity for the interviewee. If they do not feel represented, at least they are not exposed.

Although I ensure anonymity for my interviewees, some actions referred to will be non-anonymous for people familiar with the process. A new member in the SSO committee refers to only one person, and this will naturally and inevitable be recognizable. My ethical consideration pertaining to exposure is that people exercising power and influencing processes of public interest must accept that their actions are subject to research and thus exposed.

Ethical considerations in interviewing pay special attention to vulnerable groups. My interviewees are in general not vulnerable in a usual sense of the term. Some might, however, be vulnerable in a more subtle way. For some, criticizing the process might feel like criticizing them personally. If this is combined with a personality where it is important not to make mistakes, this may create a certain vulnerability. I hope it is the systemic level which stands out, as it is not my intention to criticize people who did their best in a given situation.

Summing up the factors concerning my public servant background, I do not see any formal limitations pertaining to my background. The study is influenced in various ways by my background as a civil servant. I hope that through tools from qualitative method, engagement with theory, a reflexive approach and not least through the presentation throughout the thesis, the study is deemed trustworthy.

6.5. Criteria for Trustworthiness, and Questions of Transferability

Summing up this chapter, the study consists of a rather complex combination of two parts with somewhat different methodologies (although they both fundamentally take an abductive approach), three different types of data sources, utilizing methods from case studies and interpretive studies.

Creating and assessing trustworthiness in interpretative, qualitative research is not straightforward. I will utilize Schwartz-Shea's six criteria to evaluate the trustworthiness of my research (2014). I will also discuss questions of generalization – to what extent I can draw conclusions outside of the case itself.[49]

Six Criteria for Trustworthiness

Schwartz-Shea's first criteria is "thick description," the presence of "sufficient descriptive detail […] to capture context-specific nuances of meaning such that the researcher's interpretation is supported by 'thickly descriptive' evidentiary data" (Schwartz-Shea 2014, 132). This is difficult in an article-based thesis, given limited space. I have prioritized citations in the two relevant articles, however, hopefully giving sufficient "thickness" to get a feel for the empirical material.

Reflexivity – the second criteria – is aimed at in section 6.4 on my background as well as Appendix 1.

Triangulation – the third criterion – is found both in the multiple data sources (i.e. number of interviewees) and methods for data generation (i.e. observation, interview, archive search),

[49] In Chapter 5 I discussed potential theoretical inconsistencies. A similar question could be raised about methodological or epistemological inconsistencies between a case-study approach and "sensemaking." As I have already in Chapter 5 argued that abduction builds on pragmatism, where methodological pluralism is defended (Baert 2005), I do not repeat a similar line of reasoning here.

creating potentially corroboration across sources, but also conflicting findings that needs to be grappled with (Natow 2020; Schwartz–Shea 2014).

Schwartz-Shea's criterion of *traceability* implies that sufficient detail should be given of the research process for peer reviewers and others to judge the research process and evidence (2014). Sections 6.1 –6.3 aims at this, presenting the different stages of the process, and how it is made traceable (transcribing, coding, memos etc.). Still, the process cannot be accounted for in detail. As Alvesson and Sköldberg points out, a crucial ingredient in interpretations are the researcher's judgement, intuition, and ability to "see and point something out" (2018, 329). Traceability can thus only partly be accomplished.

The criterion of *negative case analysis,* aims at preventing the "researcher from settling too quickly on a pattern, answer, or interpretation; …[searching for evidence] that will force a re-examination of initial impressions" (2014, 139). I described above how a challenge in the analysis was a "thin" shared professional description. Comparisons and contradicting descriptions on one level have led to moving into higher level of abstraction, where these contradictions are either not there or can be dealt with/accounted for.

The last criterion is *member-checking* or informant feedback (2014). I have let people with knowledge of the different phases of the policy process read relevant parts of the material. I have been somewhat reserved about discussing the project with civil servant peers and interviewees. Given my background, I have aimed at creating a distance facilitating analysis by "estranging the familiar" (Timmermans and Tavory 2012, 177); too close dialogue could, I sensed, challenge this.

Transferability Outside of the Case

Lastly, questions of transferability or "generalizability" should be discussed. Findings are context dependent, and I should be careful transferring them outside a Norwegian context. According to Schwartz–Shea, '[t]he responsibility of the interpretive researcher […] is to provide sufficient 'thick description' so that others can assess how plausible it is to transfer insights from that research study to another setting" (2014, 142).

There are however other ways of making something "general" – linked to analytical or theoretical reasoning. Adcock discusses Clifford Geertz' *experience-near* and *experience-distant* concepts in connection with the question of generalization. Geertz aims to understand experience-near concepts "well enough to place them in illuminating connection with experience-distant concepts." (Geertz sited in Adcock 2014, 91). To locate the particular in more general perspectives (Adcock 2014). In my case, this means that I investigate the Norwegian security professionals sensemaking (experience-near) and go in "dialogue" with larger theoretical (experience-distant) conceptualizations, such as Power's three ideal models of risk management logics. This way, I realize for example that the experience-near differ from the experience-distant when it comes to resilience. Through the creative theorizing (Swedberg 2014) of the abductive approach, the case-specific is linked to the broader literature on these issues. The theorizing – such as the model on risk management logics that will be developed in Chapter 7 – is context-dependent and historically situated. I *suggest* that the model might be relevant also outside the relevant Norwegian context, but I cannot say to what extent and how.

I utilize a similar way of reasoning also when I discuss standardization. I move between the empirical (findings from this study, other empirical investigations, rules of standardization) and theories on SSO standardization. Yin describes how single case studies may have a "revelatory" potential, the study reveals characteristics of a phenomenon (Yin 2009), in this case SSO standardization. The conclusions drawn built on combinations of institutional characteristics of SSO standardization, empirical findings from this and other studies, as well as engagement with theories on SSO standardization.

A final note of caution is called for. Timmermans and Tavory referred to the pragmatist Charles Peirce, who argued that abduction provides the least certainty, less than both induction and deduction; the strength of abduction is, however, its innovative potential (2012). My analysis is one way of creatively theorizing and interpreting the case.

7. Main Findings and Contributions

The thesis started with empirical puzzles on security professionals' reasoning pertaining to risk and security, and to the standardization process, and I asked how the establishment of the 3FA into a Norwegian standard can be accounted for. The two parts of the investigation points, at least initially, in somewhat different directions. Policies can be shaped by the characteristics of the process (article 1), or they can have to do with meaning and sensemaking (articles 2 and 3).

In this chapter, I build on the findings in the articles. Some findings will be elaborated on and supplemented somewhat more, to answer the research questions of the thesis. When it comes to sensemaking, I will further theorize the ideal models of risk management logics and present them in a model. The model will be utilized to draw key findings of this part of the thesis. Lastly, I will briefly discuss the two parts of the study together and the lessons learned.

7.1. Standardization as a Policy Making Path

In article 1, special attention was given to the standardization process and its many ambiguities. Here, I want to widen the discussion somewhat, and point out four influential elements: the role of PEs (1), the ambiguous characteristics of standardization by SSOs (2), and more general the role of institutions (3), and briefly, the importance of polycentric governance (4). Lastly, I will discuss a few critical points regarding the MSA approach and my theorizing in this regard.

Without Policy Entrepreneurs, No Standard

In line with the MSA, the study demonstrates the importance of PEs for the outcome of the process. They actively and persistently worked to get the approach institutionalized in the first two phases. In the last phase, the absence of PEs is noteworthy.

I will add to the discussion in article 1 some characteristics of the policy area of security risk assessment/PSM and the process, which most likely increased the importance of PEs.

First, the case has similarities to Ramanna's description of a "thin political marked," leaving room for "a few specialist players" (2015, xx). Risk assessment is abstract, for "the experts." It is not obvious what is at stake when different approaches to risk assessment are under scrutiny – even for risk assessment professionals and civil servants. This general point is most likely strengthened by the fact that the established knowledge base in the first two phases were not familiar with risk assessment, as described in article 1. They did not have knowledge or a "vocabulary" to discuss risk assessment, making the policy debate "thin."

Second, risk assessment is seen as a purely professional question, and is not "high attention, high stakes." The development of the 3FA was thus largely left to a few experts working on the issue.

Third, the PEs and the group favoring the standard are sometimes labeled the UK group, as key people had practically oriented master's degrees from the UK. They were thus seen as representing academic and up-to-date knowledge lacking in Norway.

Fourth, Cairney and Jones referred to a number of studies suggesting that PEs can be more successful and effective in smaller-scale government (2016). This case is small by any matrix, and in line with their findings.

Although the characteristics described above have most likely increased the importance of PEs, one should not reduce the PE influence to structural characteristics. Strong human agency – a willingness to "fight it through" in the first two phases – was also key to the outcome.

In article 1, I describe the success of PEs in the second phase of the process as maneuvering or even manipulation. This can be read as a conscious, illegitimate act. One could just as well read it as a creative attempt to get a solution (how can we solve this stalemate?). It is the malleability of the system that stands out – and how the standardization requirements in the case become formal barriers that needs to be "ticked off," rather than substantially dealt with.

All in all, given the analysis in article 1 as well as the nuances described above, I argue that without the persistent work of PEs, the standard in its current form would not have existed.

The Ambiguous Characteristics of Standardization by SSOs

Key to understanding the policy process is the institutional context of standardization by SN. I pointed out several ambiguities linked to SSO standardization in article 1, and found standards to be both "innocent" (voluntary, consensual) and potent (sanctioning good practice). The "innocent" part makes participation less attractive, whereas the potent part makes standardization potentially prone to stakeholders with resources and an agenda (see e.g. Ramanna 2015).

Government's role in SSO standardization could be described as a type of exchange. Government agencies contribute with expertise, sometimes leading the committees in question (as in this case), thus legitimizing, and helping in the production of, standards. On the other hand, government gets standards produced, which it may see a need for, and with assistance from private experts.

When contributing to the production of standards, the government is not burdened by hierarchic power and responsibility, as with government policy. A government document is laden with politics; a standard escapes such connotations and responsibilities, as discussed in the theory chapter (Jacobsson 2000). Hierarchical organizations (government), are seen as responsible and complaints are more frequent in such organizations, Brunsson argues (2000). Following, and we may assume also producing, standards, make the scope of governing more limited (Brunsson 2000).

The ambiguous connection between government and SSO standardization cannot be pointed out as a direct cause of the empirical development, but it is an underlying premise linked to the larger question of responsibility and professionalism. For an SSO, having government “on board” may strengthen the claim for both. For government, or rather, for the many decision-points within various governmental bodies, they are less responsible for SN processes and may prioritize this lower than their own governing.

Turning to the empirical case and how SSO standardization influenced the process, I draw two main conclusions pertaining to standardization. In phase 2, a new concept (security–risk), circumvented policy disagreement and created an institutional differentiation between two professional “turfs.” The institutional barriers were thus more malleable in the second phase than in the first, government phase of the process. Second, I also argue that differentiating between responsibility for process (SN) and content (committee) created stream-independence, notable in the third phase. SN, the potential organization for activating the political stream, did not relate to criticism of its own standard in the policy stream. Following Hajer, one could describe it as a decoupling of policy and polity (Hajer 2003), or, with the MSA, a decoupling of the policy and the politics streams.

When I state that responsibility for standards becomes diluted, this is primarily based on the structural characteristics of this type of standardization. Although there was a decoupling of streams, one should not take this too far. In the case in question, SN and the committee were clearly responsible for the standard and could have been engaged, one may assume, if approached.

The decoupling of responsibility for content and process, creates a more general vulnerability in the SSO system, becoming more problematic, one can assume, over time. This is especially the case with committees with high turnover and if it is difficult to engage expertise, something noted as a challenge (ResiStand 2018). The danger is, as Tang et al. have pointed out, that SSOs can create “a plethora of rules and procedures” (2019:502), but with a “general lack of a centralized authority responsible for developing a consistent policy in the regulatory sphere” (2019:514). I labeled this an *institutional deficit* in article 1. By this I mean that the SSO, the polity, produces policy in a government-like situation, but the polity is not structured such that it takes responsibility for policies in a government-like way. It becomes unclear who governs (Gustafsson and Tamm Hallström 2018; Jacobsson and Brunsson 2000), or put even stronger, it may *de facto* not be governed.

In summary, based on a combination of empirical and analytical reasoning, as well as other literature discussed, a concern for an institutional deficit in SSO standardization seems all in all well-founded.

Taking the above into account, I do not conclude that standardization in general, or even SSO standardization, is necessarily or in general inappropriate. Some version of standardization is needed; complex and efficient practices cannot be created anew each time. Given a functionally based regulatory system, a link between practice and rules is needed (Engen 2020), and standardization is one option. There are also indications that practitioners (such as from industry) view standardization positively (Menon-Publication 2018, commissioned by nordic SSOs; ResiStand 2017). Standards and standard-setting encompass many things, from product harmonization to risk assessment, and a general conclusion pertaining to standardization by SSOs stretches the implications of this thesis too far.

I will draw the conclusion, however, that standardization should be more critically investigated and vetted than what is often the case. It should neither be assumed that standards are “the distilled wisdom of people with expertise in their subject matter” (ISO n.d.), nor that the process has been characterized by extended cooperation and legitimacy among relevant stakeholders, as is often assumed. This and other investigations indicate that standardization by SSOs need to be approached for what it is, a "vulnerable and complex system" (Engen 2020, 269), often with substantial power (Jacobsson and Brunsson 2000; Olsen 2020a; Ramanna 2015; Slager, Gond, and Moon 2012) and with the potential for an institutional deficit, not able to handle what has been produced.

Both Formal Institutions and Knowledge Matter

The third element influential to the institutionalization of the standard is the importance of the institutional characteristics of the different phases. In article 1, I utilize two types of institutions, formal and knowledge background.

When it comes to the formal institutions, a single veto power in the government phase made it possible to decide despite disagreement. The formal rules of SSO standardization are more challenging, most notably the consensus requirement. These in theory strong institutional barriers did not work as such in the second phase, as described above. The rules shaped the process, though, in that two turfs were created to narrow the number of people who had to agree. In summary, in both the first and second phases, the political stream was decisively shaped by formal institutional characteristics, that is, decision-making rules and the number of veto points.[50]

I have noted a difference between the government and the standardization phases in article 1. The institutional rules of government shaped the process, not the other way around. In the second phase, however, the SN institution did not only shape the process, but the process shaped the institution (two professional turfs).[51] This can perhaps be attributed to the integrity of the institutions themselves. Despite disagreement, the "rules of the game" were accepted

[50] The outcome should not be regarded as an automatic consequence of the formal rules, however. The Ministry chose to utilize the single veto point; it did not have to. One may thus conclude that formal institutions were a necessary but not sufficient condition for the outcome.
[51] In article 1, this was attributed to the difference in veto-powers between the government (one veto power) and standardization (consensus requirement).

within government. Regarding the standardization phase, a hypothesis could be that it was more important to get a solution (a standard) than taking the requirements and norms of consensus among a broad group of experts seriously. I do not suggest that this was consciously manipulated, but that the integrity of the institution was less established and understood. One can hypothesize that the potential risks of standardizing are less visible, whereas the benefits – a finished product, a solution that can be offered – are perceived more clearly.

The last phase of the standardization process is labeled a "non-event" in article 1, as the standard was debated to some extent, but nothing happened. The most decisive thing that was done was that research was commissioned by a government organization (FB) to be conducted by a research institute (FFI). Security risk assessment and 3FA were also written about by university scholars. Research does not in itself create policy, however. The case may thus be a micro-cosmos for a larger challenge, that of academics writing papers with the hope that this matters, and public servants and others developing policy without necessarily relating to the academic literature in question. Those utilizing and those questioning the standard and the 3FA were often not connected.

In summary, both formal institutions as well as ideas and knowledge are different types of institutions that influenced the process. I also discussed how the integrity of the institution may have influenced the process – that the benefit of creating a standard may be clearly anticipated, and that the potential negative outcome of "circumventing" rules such as consensus requirements are less acutely felt.

A Fractured Process and Polycentric Governance

The investigation reveals that an important reason for the institutionalization of the approach lies in the fractured process, and how the policy (3FA) was "moved" across both organizational and institutional boundaries. As pointed out in article 1, there was no or very little institutional memory between phases. An important reason for the institutionalization of the approach should thus not only be found within each phase, but across phases – in the possibility for "venue shopping" (Ackrill, Kay, and Zahariadis 2013) – that actors can advance their agendas through strategic choices on where to go to get their project passed. The case may thus be linked to polycentric governance (Berardo and Lubell 2016; Hajer 2003; Swyngedouw 2005), and sensitize us to the fact that such tendencies do not only take place in large-scale, often international arenas, but also may influence small processes such as the one in question.

The MSA Framework

The simplicity and intuitiveness of the MSA is often pointed out as a reason for its excessive use. Terms such as PEs, policy windows, and policy streams are so intuitive, one could argue, that they are banal. There is some merit to such a criticism. When decisions are made, how can they *not* be described as a result of a "policy window"?

The MSAs underlying assumptions, such as stream independence, ambiguity, time as a sorting mechanism, etc. are however not trivial, and often the opposite is taken for granted. In this study, it is the combination of the MSAs' quality as a "sorting mechanism" and the non-trivial, underlying assumptions that give it merit. I thus concluded in article 1 that several elements of the process were described quite well by MSA concepts, and that, all in all, it has sensitized the analysis in meaningful ways.

I have theorized to adjust the MSA framework to the study. This theorizing is exploratory and abductive, and I see potential for criticism. Institutional factors are incorporated into the framework, but I do not merge them with the three process streams. I have labeled the streams as "logics," but what is the difference between a logic and an institution, especially taking the key term of "institutional logic" into account (Scott 2014)? Could one simply merge the politics stream with formal institutions and the policy stream with knowledge and ideas? I have not done so. The reason can be explained through the metaphors introduced by Winkel and Leipold (2016). The streams may be seen as water and the institutions as the "shore" of the river. The three process streams (water) are channeled in certain ways by institutions (shores), making some paths possible, others not. Process and institutions are not the same, my argument goes, but the relationships between streams and institutions are not clear and should be further theorized.

Seeing the streams as logics also require further investigation and theorizing. I see it as a great benefit that the streams become detached from specific groups and endless discussions within the literature of which groups "belong to" the different streams. However, both the notion that the streams are logics and the "nature" of the different elements of the theory need further investigation and theorizing.

Concluding Remarks

In summary, I conclude that a number of characteristics of the policy process influenced the institutionalization of the 3FA standard. Here, I have pointed out four. Human agency, most notably PEs, were decisive, but also the different institutional characteristics. Special attention has been given to standardization by SSOs. Building also on other SSO research, I raised a concern that – if not in a single case, then over time – an institutional deficit may occur. In other words, standards are created, but with little institutional capacity to deal with what has been created. Important to answering RQ1 is also a fractured process and polycentric governance.

7.2. Sensemaking by Security Professionals

I will now turn to the second part of the study, investigating sensemaking by security professionals. I will first present how security professionals have positioned the 3FA in opposition to other practices and perspectives, those of safety and of prescriptive rules. I will then further theorize Power's three ideal models of risk management logics into four logics, and utilize the theorizing to draw key findings from this part of the investigation. Finally, I will view the two parts of the studies together, aiming at answering the main research question, and discuss some lessons learned.

Positioning the 3FA – It Is Not Safety and Not Prescriptive Rules

The 3FA is positioned by the security professionals in two directions, contrasting it to what it is not. The 3FA is first positioned as *not* safety. Probability is communicated as the key marker of difference. Safety risks include probability, it is argued, because historical information can be used to predict the future through frequency-based estimates. Security risks are different, in that a potential, strategic "enemy" makes them unpredictable and uncertain, and can thus not be subject to probability judgements in the same way. The argument is also linked to natural versus social science, where "safety" is interpreted as more technical and mathematical, whereas "security" is about human beings, and thus security risk assessment is fundamentally a social science.

The second positioning of the approach is that it is different from following detailed prescriptive rules and checklists. Here, it is not so much the specific 3FA which is important, but that PSM should be conducted through tools and perspectives from risk management. A contrast between "following detailed rules" and "analytical conduct" is made, where security risk assessment is valuable because it brings systematic, analytical and (for some) academic method into PSM.

Although security risk assessment represents an analytical approach to PSM, it does not substitute prescriptive rules. Detailed rules in several areas still exist (personnel security, information security, etc.), and this is not questioned. However, the risk assessment and management add a layer and an over-all framework for the planning of security measures. It also represents a different type of regulatory approach. As argued in article 3, the introduction of a risk-based approach moves PSM from being a limited matter "for the security people," to being an integral part of the overall management of the organizations, as part of "corporate" governance.[52] This movement is recognized, seen as important and necessary by the professionals.

In summary, the 3FA is made sense of by positioning it in two directions, in part as a contrast to risk assessment from "safety." Being a risk assessment approach, it is also seen as representing a more analytical approach to PSM, in contrast to detailed, prescriptive rules.

From Three to Four Risk Management Logics

Articles 2 and 3 utilised, but also developed, Power's three ideal models of risk management logics as sensitising concepts (Blumer 1954; Power 2014). I propose to further develop the three logics into four ideal models – or dimensions. They are not mutually exclusive; on the contrary, practices will involve combinations to varying degrees (Power 2014). The logics are historically and contextually situated. The four risk management logics are proposed below:

1. Anticipation – this is the same as Power's ideal model of anticipation (2014). It is the *assessment* part of risk management. It aims at being descriptive, aspires knowledge of causations (Å. Boholm and Corvellec 2016), has science as an ideal and aims at foresight and prediction. The solution to our challenges is more knowledge: "information is key to victory" (Strickland, cited in Doty 2015, 349). The mode of disappointment is, in line with Power, an unexpected event, as it should have been predicted (2014).[53]

[52] *Virksomhetsstyring* literally means "entity governance" but is sometimes translated as "corporate governance."
[53] For science, the mode of disappointment is to say something false (Lewens 2007). However, "anticipation" is a risk management logic, and as such, an unexpected event would be the key disappointment.

2. Optimalisation –aims at getting the most out of one's resources through cost/benefit judgements (either calculated or qualitatively). This is linked to "taking risk," the origin of the term "risk." It is neutral, in the sense that it is both potentially positive and negative; and one is willing to lose some to gain some. What one gains must only be marginally more than what one loses. In this understanding "[t]here are risks on all sides" (Sunstein 2005, 4), also *not* taking risk is a risk. Economic risk calculation follows this logic, and at its core is probability. Success is achieved through getting the probability estimates right.

The mode of disappointment is wasting resources. This may hinder the most value for one's investment, or – in a competitive market context – one may "become broke" if someone else is better at estimating risk.

3. Governance – this is linked to decision–making. From this perspective, it is the decision causation that matters. One should take the right decisions and be responsible for these decisions. This logic is normative and legitimacy–oriented, building on ideals of democracy and the legal system.[54] Power's ideal model of auditability is part of this risk logic, as control and audit have become a way of holding organizations accountable and increase transparency. Lack of trust is met with audit trails aimed at showing responsible conduct (Power 2007, 2021).

When I describe this risk management logic as "governance," not "auditability" as Power does, it is to argue that the core of risk governance is *responsibility* for the choices made, in line with the findings in this study. Many professionals are burdened with a felt responsibility, as noted in article 3. Some feel responsible for creating security, others for doing a good risk assessment. To label the logic "governance" is to leave it more open to how the normative

[54] Luhmann's distinction between "risk" and "danger" is useful to understand this logic, as risk governance is linked to risks (decidable), not danger ("destiny") (1991). As Power noted, more and more is regarded as being a question of (deliberate) decisions; there is an "expanded decidability of situations" (Power 2014, 375), subject to risk governance.

dimension (responsibilizing and holding accountable) plays out. In line with Power's model, the mode of disappointment is "blame."

4. Protection - Insights from security studies are drawn upon when protection is seen as the fourth logic. There is a "path dependency" within national security which influences risk assessment in a national security context. This is linked to the sovereign state and the social contract with citizens of the state to protect them against enemies and the world outside. Although the inside/outside of states are blurred, it is still a perceived obligation of governments to protect their citizens and territory, in areas such as CIP. As Bigo has pointed out, it is the ability of the protector to protect which is at stake (2009). Given a globalized, interdependent world, the inside of the country is as much an arena for keeping this social contract as the outside. As argued in article 3, I substitute Power's ideal model of resilience with that of protection.

The precautionary principle has been extensively discussed and is acknowledged as characterising much risk decision making in our time (Furedi 2009; Klinke and Renn 2002; Mythen and Walklate 2008; Stern and Wiener 2006; Sunstein 2005). The protection logic is precautionary, "adopting a 'better safe than sorry' approach" (Wardman and Löfstedt 2018, 1802). Often, only the *possibility* (Amoore 2013; Stern and Wiener 2006) of something happening is enough for protective (or if possible, preventive) measures. Probability is less relevant, or even irrelevant, in this logic. As one interviewee referred to in both articles 2 and 3 stated, some values should be protected no matter what, making probability (at least in theory) irrelevant.

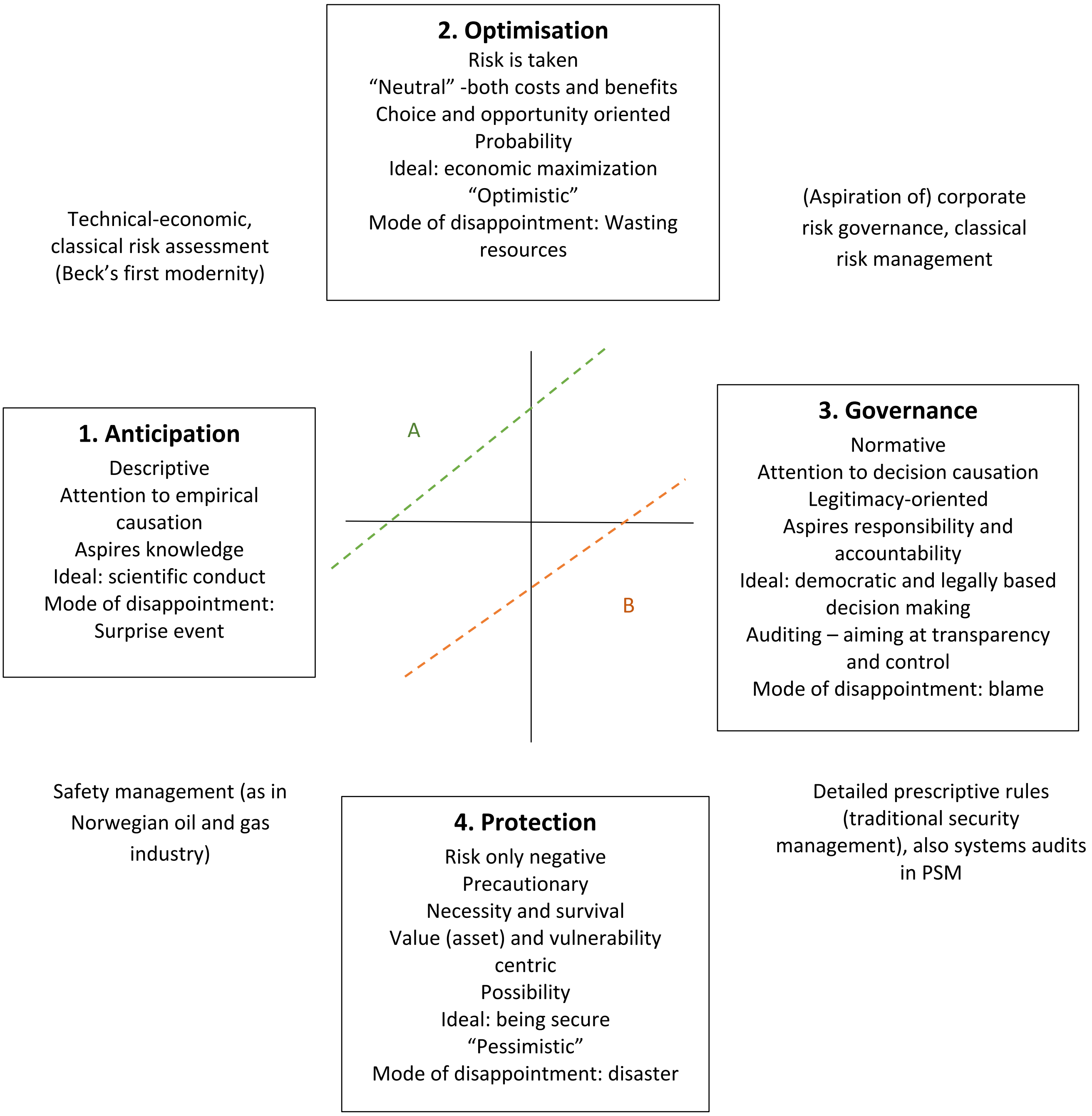
What is at stake in this logic is survival, not necessarily of human beings or nation states, but of critical objects or infrastructures. Risks are only perceived as negative; they are not chosen, but for all practical purposes imposed on you.

This logic combines insights from two areas. Security studies offers the insight that “security” is built on the core role of the state and its social contract of protecting its citizens inside the territory (Huysmans 2009), with perceived potential catastrophic consequences if the state fails. At the same time planning protection is undramatic, tedious “riskwork” (Power 2016b). Huysmans has argued for the introduction of “protection” as “opening security studies to the importance of everyday practices and routines…[not] to privilege extraordinary or exceptional situations” (2009, 14). Protection is bureaucratic work (Bigo 2002), but at the same time, and in line with the security perspective, a great deal is at stake.

I have chosen not to label the logic “resilience,” as argued for in article 3. This might be controversial, as what is described here as “protection” is often discussed under the umbrella of “resilience.” However, the resilience concept has connotations such as “bounce back” after an incident (Wildavsky 2017), different from protecting beforehand. It is also a much more complex and unclear concept (Jore 2020; Rogers 2017). Considerable discourse, especially within security studies, has linked resilience to neoliberalism (Aradau 2017; Dunn Cavelty, Kaufmann, and Søby Kristensen 2015), and an “abdication” of the state. This gives resilience a connotation that does not fit a case such as the one under scrutiny. For these reasons, the classical idea of “protection” seems a better solution.

In summary, the main differences to Power’s three logics are that resilience is substituted with protection. I have also differentiated between anticipation and optimization, something which is often lumped together in sociology of risk, as “technical-instrumental.” The third is to substitute the logic of “auditability” with that of “risk governance.”

Figure 8 Different Risk Management Logics



2. Optimisation
Risk is taken
“Neutral” -both costs and benefits
Choice and opportunity oriented
Probability
Ideal: economic maximization
“Optimistic”
Mode of disappointment: Wasting resources

Technical-economic, classical risk assessment (Beck’s first modernity)

(Aspiration of) corporate risk governance, classical risk management

1. Anticipation
Descriptive
Attention to empirical causation
Aspires knowledge
Ideal: scientific conduct
Mode of disappointment: Surprise event

3. Governance
Normative
Attention to decision causation
Legitimacy-oriented
Aspires responsibility and accountability
Ideal: democratic and legally based decision making
Auditing – aiming at transparency and control
Mode of disappointment: blame

Safety management (as in Norwegian oil and gas industry)

4. Protection
Risk only negative
Precautionary
Necessity and survival
Value (asset) and vulnerability centric
Possibility
Ideal: being secure
“Pessimistic”
Mode of disappointment: disaster

Detailed prescriptive rules (traditional security management), also systems audits in PSM

As illustrated in Figure 8, two axes emerge. The vertical axe goes from optimisation, where risk is neutral, to protection, where risks are potentially catastrophic and needs precautionary measures. The horizontal axis goes from anticipation, acquiring knowledge, to governance, taking action and making decisions.

The examples given between the four logics are meant as illustrative examples. The first is technical-economic activity, which involves both anticipation and optimisation; classical risk assessment and Beck's first modernity (1992) belong here. The second example lies between anticipation and protection, and an example here is safety management in high-complexity industries such as offshore oil and gas. It is highly risk-averse, but at the same time building on anticipation. The third example lies between optimisation and governance; corporate governance and classical risk management belong here, as the goal is both legitimacy and economic prosperity. The fourth example lies between governance and protection, where much is at stake, as there is a potential for both "disaster" (protection) and "blame" (governance). The old PSM system discussed in article 3 is placed here, where protection and accountability are aimed at through detailed, prescriptive rules. It is notably contested where the new functionally based system of sound security belongs – as will be discussed below.

The green (A) and orange (B) lines in the figure will be discussed below.

I will now utilise the four logics and their modelling on the empirical case which spans articles 2 and 3.

The Role of Probability – Optimization or Protection

A core finding in article 2 is that the goal to create security is at odds with the "riskiness" of risk, as classical risk optimization would entail. This can now be linked to the protective logic. Given this logic, it is no surprise that probability was singled out as the problem with traditional risk assessment. The judgement "low probability" is not "trusted" as a defense against an incident: also "low probability" risks can materialize.

I have noted probability's two roles, that of anticipating the future and of moderating the risk.[55] Those in favour of the 3FA argue that estimating the probabilities of security risks is often difficult or impossible –that is, linked to the role of anticipation. Opponents of the 3FA are concerned about the latter, the potential consequence of security risks being expressed without attention to probability. If probability is not taken into account estimating security risks, but taken into account with other risks, that would imply a privileging of security risks. Although not expressed in these terms, this criticism resonates with securitization theory. If expressing risks without probability, security risks are "spoken" as higher risks than they would have been if probability judgements were taken into account. These security professionals argue close to the "optimization" logic, in that a balanced treatment of different risks is called for.

Utilizing the risk logics helps identify that those favouring the 3FA do not only have epistemic arguments against probability. Probability, and the optimization logic, are also at odds with the ideal of protection and creating (national) security. When viewing risk assessment from the perspective of protection, precautionary measures are called for. Seen from this perspective, probability and optimizing between risks are dangerous, as this relativizes the risk. Probability estimates are not precautionary, there are no "better safe than sorry" judgement baked into the assessments themselves.

Seen from the perspective of optimization, on the other hand, to invest precautionarily is wasteful and "risky," and might backfire. Søby Kristensen's analysis of the "unstable" and incoherent narrative when national security was aimed at through tools of risk management in the aftermath of 9/11 is worth mentioning in this context (2008). The 3FA can be seen as an attempt to reduce the tension described by Søby Kristensen, or as described here, between

[55] I have not found a reference in the literature on probability's two roles in the expression of risk, but it must exist.

optimization and protection. 3FA is a risk assessment approach, but without, or at least with less attention to, probability, the risk moderator. It moves risk assessment towards "protection." Downplaying probability – the *consideration,* not the calculation – of probability, can be regarded as a slight securitizing move, as described above.

In summary, we see a tension reflected in the case pertaining to the vertical axis, between getting a "balanced" approach towards risks (optimization) versus concerns of getting sufficient protective measures. Probability plays a key role in the former but is a potential threat to the latter and vice versa; precautionary practices embedded in protection are at odds with optimizing resources.

Time – the Inconsistency between Requirements Before and After an Incident

A second important finding across articles 2 and 3 is linked to time and responsibility, in relation to hindsight judgements, or more precisely, how one expects judgements after an incident to be, in terms of what should have happened before the incident. In article 2 this is linked to the terrorist attack of 2011, and M8' conclusion that "when it goes wrong, they are right." Those who argued *before* for more security were proven right by the larger public *afterwards*. Some have linked this to probability estimates, that this shows the problem with including probability in risk estimates – when risk is reduced through probability, the estimates do not really reflect the security level people expect. Grubbegata, the street that was not closed before the July 22 terrorist attack, is used as an example in this regard.

In article 3 there is a similar argument pertaining to "sound security." Before an incident, "sound security" is about analyzing and optimizing security measures in a balanced way. After the incident, the lack of security measures will be judged as insufficient and not "sound," as the incident should not have happened.

In both cases, the analysis shows an expected inconsistency from a larger society between "before" and "after" an incident. Before, risk assessments aim at acquiring knowledge about risk and optimizing outcomes in a cost-benefit way. This is illustrated by the dotted green line (A) in Figure 8. After the incident, however, the expectation or fear is of a judgement that whatever went wrong should have been prevented, with a corresponding responsibility and blame, illustrated by the orange line (B).

Another way to see this is that a risk is only a risk before an incident (Beck 1992). Afterwards, it has changed to something that materialized. The uncertainty and openness characteristic of it being a risk is no longer there. It is no longer a risk. The knowledge base, but also the normative expectations, have dramatically changed.

One may argue that the movement from the green (A) to the orange (B) line in Figure 8 is also a more general movement in today's societies, from the "optimistic" green line, in line with Beck's notion of the first modernity (Beck 1992; Woodman, Threadgold, and Possamai-Inesedy 2015), to the orange line, representing more precautionary perspectives on risk (Amoore 2013; Furedi 2009), directed at protection (Bigo 2009) and with an urgency more familiar to security issues (Aradau and Van Munster 2007). It is also in line with Power's observation that risk management has moved from being primarily about anticipation, the content of risk assessment, to being more about the governing and organizing of, and regulatory control over risk, that is, the process of risk management (Power 2007, 2014).

In summary, to answer the sub-question of how security professionals make sense of risk in a security setting, I draw four conclusions. First, the 3FA is positioned as not coming from "safety" and as being analytical, not based on prescriptive rules. Second, utilizing the risk logics developed above, we may interpret security professionals' sensemaking as expressing a tension between risk assessment as a tool for optimization and for protection. Third, I noted that probability has two roles in the expression of risk – anticipation and moderation. Those arguing for the 3FA pay attention to risk as anticipation and argue that it is often not possible to anticipate probability. Those arguing against the 3FA pay attention to the second role, that of moderating the risk. This is more in line with the optimization logic, as a balanced approach to risk (and between risks) is what is important. The fourth conclusion has to do with time, and the perceived inconsistency between what is expected before and after an incident. Before, analytical conduct and optimization are called for, whereas afterwards, one perceives a responsibility for not having created security and protection.

7.3. Seeing the Two Parts Together

Initially, I asked the overall research question of how we can account for the establishment of the security risk assessment approach as a Norwegian standard. Seen from the policy process perspective investigated in the first part of the study, PEs' active role, the institutional characteristics of SSO standardization, and polycentric governance are paramount. The analysis gave knowledge and ideas all-in-all a modest role.

Investigating sensemaking by security professionals, such a conclusion should be nuanced, however. The 3FA and the standard reflect protective perspectives that build on national security traditions. The special "twist" of taking probability out reflects the ideals of creating protection and security. Seen from the sensemaking study, the 3FA is not only or primarily the result of a policy process, but the expression of sensemaking and meaning in a professional security community.

Protective security has not traditionally been framed as risk management. The introduction of risk management made the professional domain unclear and contested. When two professional "turfs" were created, those of "risk" and "security risk." this (re-)established protective security as a separate professional domain, much in line with the "safety" versus "security" distinction. The 3FA incorporates the idea that risk assessment and management are good ideas within PSM, but reflects at the same time that the goal of protection is "risk-averse."

I thus conclude that although the policy process was pivotal for the development of the standard, the approach reflects perceived challenges when utilizing risk assessment in a security context. It reflects struggles to combine contradictory risk logics in protective security management.

Final Remarks

If there are lessons to be learned from this thesis, it is that we cannot have it all. Much public discourse builds on a premise that we can. We do not want the government quarter to cost NOK 55 billion – to a large extent because of security measures – but we expect the government to prevent disastrous events from happening. We do not want to live in a surveillance society, but we also want the government to protect us against malicious activity. Hopefully, the thesis can offer some concepts and frameworks to reflect on these tensions.

Risk management has become a key framework that should encompass it all – a way to gain control, a governing tool for making organizations responsible, and a way to be cost-efficient. Perhaps I am too much of a public servant, but I am not against risk assessment and management as such. I cannot imagine a world without it. But our hopes of what it can accomplish should not be too high, and we should see the dangers of making organizations responsible in a way that does not match what they can, in any meaningful way, take responsibility for.

There are lessons to be learned also for security professionals. The second article started off with a citation from a security professional realizing how (s)he got a much "better" result, meaning investment in security measures, when presenting the risk in line with the 3FA. The framing of the risk became a securitizing act, in that probability judgements were not communicated and thus not a subject for discussion. A call to security professionals is thus also required. Their responsibility is not to create security, but to place “all the cards on the table.” Uncertainty and unpredictability, what we know about likelihood, dilemmas, unfortunate consequences, etc. should be expressed, so that decisions can be made on this often uncertain and messy grounding.

Is there a lesson to be learned for research? I will mention two. One is the value of thicker descriptions in areas such as risk and security management, and standardization. It is perhaps not surprising that a person with nearly 20 years’ experience in the public service regards many analyzes of these services as too “thin” and caricature-like. Still, I argue that thicker descriptions could bring some new blood into what too often constitutes relatively predictable research and findings.

Second, most likely given path dependencies in academia, some important societal phenomena, such as standardization and security (risk) management, are clearly under-investigated from a social science perspective. The second lesson is thus, bluntly, that they need to be investigated more and understood better. Cross-fertilization between research areas can be a valuable contribution in this regard, of which this thesis is hopefully an example.

When I started to work on this project in December 2017, the world looked very different. Terrorism – right-wing or jihadist – was the key security discourse, with cyber security a less emotional but troubling secondary concern. Since then, war in Europe is no longer a “low probability, high stakes” risk. The epistemic argument of the proponents of the 3FA – we cannot estimate the probability of these risks – has shown its merit. Probability seems, unfortunately, no longer to be a threat to security arguments.

However, one could also argue that probability has become acute. *Everything* cannot be protected. Protection, building on concepts such as in-depth security, is often very resource intensive, not to speak of its other potentially negative implications. The higher the perceived threat of, for instance, hybrid warfare, the smarter resources must be used.

The context of the controversy investigated is somewhat historically dated. The dilemmas are not gone, however, and may be more acute than ever. I thus both hope and believe the thesis is not outdated, although the empirical premises have changed.

In conclusion, the most important lesson to be learned could be about governing. The two governing tools investigated, standardization and risk management/assessment, are poorly understood, also by practitioners. They are abstract and somewhat intangible – perhaps therein lies one reason for their success? They provide flexibility and enable reflexive governing, a necessity in today’s complex system, one could argue. But the reflexivity is underdeveloped, and there is too much naivety, both within the public sector and outside of it. As such, the concluding lesson is for the public sector itself. It needs to (even) better reflect on what constitutes good governing. Legitimate public administration is based not only on its democratic anchoring, but also on its problem-solving capacity and the quality of decisions made (Christensen, Holst, and Molander 2023; Heath 2020). There is a need to further reflect on what creates good governance. This includes critically reflecting on the governing tools utilized in this regard.

8. References

Abrahamsen, Eirik Bjorheim et al. 2017. “A Framework for Selection of Strategy for Management of Security Measures.” *Journal of Risk Research* 20(3): 404–17.

Ackrill, Robert, Adrian Kay, and Nikolaos Zahariadis. 2013. “Ambiguity, Multiple Streams, and EU Policy.” *Journal of European Public Policy* 20(6): 871–87.

Adcock, Robert. 2014. “Generalization in Comparative and Historical Social Science. The Difference That Interpretivism Makes.” In *Interpretation and Method: Empirical Research Methods and the Interpretive Turn*, eds. Dvora Yanow and Peregrine Schwartz-Shea. Armonk, N.Y: M. E. Sharpe, 80–96.

Adler, Emanuel, and Vincent Pouliot. 2011. “International Practices.” *International Theory* 3(1): 1–36.

Agius, Christine. 2016. “Social Constructivism.” In *Contemporary Security Studies*, ed. Alan Collins. Oxford New York: Oxford University Press, 70–86.

Ahrne, Göran, and Nils Brunsson. 2005. “Organizations and Meta-Organizations.” *Scandinavian Journal of Management* 21(4): 429–49.

Alvesson, Mats, and Anna Jonsson. 2022. “Organizational Dischronization: On Meaning and Meaninglessness, Sensemaking and Nonsensemaking.” *Journal of Management Studies* 59(3): 724–54.

Alvesson, Mats, and Kaj Sköldberg. 2018. *Reflexive Methodology: New Vistas for Qualitative Research*. Third edition. Los Angeles, California: SAGE.

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

Amoore, Louise, and Marieke De Goede. 2005. “Governance, Risk and Dataveillance in the War on Terror.” *Crime, Law and Social Change* 43(2–3): 149–73.

Amundrud, Øystein, Terje Aven, and Roger Flage. 2017. “How the Definition of Security Risk Can Be Made Compatible with Safety Definitions.” *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 231(3): 286–94.

Ansell, Christopher, and Patrick Baur. 2018. “Explaining Trends in Risk Governance: How Problem Definitions Underpin Risk Regimes.” *Risk, Hazards & Crisis in Public Policy* 9(4): 397–430.

Antonsen, Stian, Kari Skarholt, and Arne Jarl Ringstad. 2012. “The Role of Standardization in Safety Management – A Case Study of a Major Oil & Gas Company.” *Safety Science* 50(10): 2001–9.

Aradau, Claudia. 2010. “Security That Matters: Critical Infrastructure and Objects of Protection.” *Security Dialogue* 41(5): 491–514.

———. 2016. “Risk, (in)Security and International Politics.” In *Routledge Handbook of Risk Studies*, eds. Adam Burgess, Alberto Alemanno, and Jens Zinn. Routledge.

———. 2017. “The Promise of Security: Resilience, Surprise and Epistemic Politics.” In *The Routledge Handbook of International Resilience*, eds. David Chandler and Jon Coaffee. Routledge.

Aradau, Claudia, and Rens Van Munster. 2007. “Governing Terrorism through Risk: Taking Precautions, (Un)Knowing the Future.” *European Journal of International Relations* 13(1): 89–115.

Argomaniz, Javier. 2015. “The European Union Policies on the Protection of Infrastructure from Terrorist Attacks: A Critical Assessment.” *Intelligence and National Security* 30(2–3): 259–80.

Arnold, Nadine. 2022. “Accountability in Transnational Governance: The Partial Organization of Voluntary Sustainability Standards in Long-Term Account-Giving.” *Regulation & Governance* 16(2): 375–91.

Ashworth, Rachel Elizabeth, Aoife Mary McDermott, and Graeme Currie. 2019. “Theorizing from Qualitative Research in Public Administration: Plurality through a Combination of Rigor and Richness.” *Journal of Public Administration Research and Theory* 29(2): 318–33.

Askeland, Tore, Roger Flage, and Terje Aven. 2017. “Moving beyond Probabilities - Strength of Knowledge Characterisations Applied to Security.” *Reliability Engineering and System Safety* 159: 196–205.

Åtland, Kristian. 2008. “Hva er sikkerhet? En drøfting av sikkerhetsbegrepets innhold og utvikling fra antikken til det 21. århundre [What Is Security? A Discussion of the Security Concepts Content and Development from Antiquity to the 21st Century].” *Norsk Statsvitenskapelig Tidsskrift* 24(1–2): 108–33.

Aven, Terje. 2014. *Risk, Surprises and Black Swans: Fundamental Ideas and Concepts in Risk Assessment and Risk Management*. London: Routledge.

Aven, Terje, and Ortwin Renn. 2010. 16 *Risk Management and Governance: Concepts, Guidelines and Applications*. Springer Berlin Heidelberg: Imprint: Springer.

———. 2020. “Some Foundational Issues Related to Risk Governance and Different Types of Risks.” *Journal of Risk Research*: 1–14.

Aven, Terje, and Marja Ylönen. 2019. “The Strong Power of Standards in the Safety and Risk Fields: A Threat to Proper Developments of These Fields?” *Reliability Engineering & System Safety* 189: 279–86.

Baert, Patrick. 2005. *Philosophy of the Social Sciences: Towards Pragmatism*. Polity.

Baldwin, Robert, Martin Cave, and Martin Lodge. 2011. *Understanding Regulation: Theory, Strategy, and Practice*. 2. Oxford University Press.

Battistelli, Fabrizio, and Maria Grazia Galantino. 2019. “Dangers, Risks and Threats: An Alternative Conceptualization to the Catch-All Concept of Risk.” *Current Sociology* 67(1): 64–78.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. London: Sage.

Béland, Daniel. 2016. “Kingdon Reconsidered: Ideas, Interests and Institutions in Comparative Policy Analysis.” *Journal of Comparative Policy Analysis: Research and Practice* 18(3): 228–42.

Berardo, Ramiro, and Mark Lubell. 2016. “Understanding What Shapes a Polycentric Governance System.” *Public Administration Review* 76: 738–51.

Berling, Trine Villumsen, and Christian Bueger. 2015. *Security Expertise: Practice, Power, Responsibility*. London: Routledge.

Berling, Trine Villumsen, Ulrik Pram Gad, Karen Lund Petersen, and Ole Wæver. 2021. *Translations of Security: A Framework for the Study of Unwanted Futures*. London: Routledge.

Berndtsson, Joakim. 2012. “Security Professionals for Hire: Exploring the Many Faces of Private Security Expertise.” *Millennium* 40(2): 303–20.

Bernstein, Peter L. 1996. *Against the Gods: The Remarkable Story of Risk*. New York: Wiley.

Bieder, Corinne, and Kenneth Pettersen Gould, eds. 2020. *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. Cham: Springer International Publishing.

Bigo, Didier. 2002. “Security and Immigration: Toward a Critique of the Governmentality of Unease.” *Alternatives* 27(1_suppl): 63–92.

———. 2006. “Internal and External Aspects of Security.” *European Security* 15(4): 385–404.

———. 2009. “Protection: Security, Territory and Population.” In *The Politics of Protection: Sites of Insecurity and Political Agency*, Routledge advances in international relations and global politics, eds. Jef Huysmans, Andrew Dobson, and Raia Prokhovnik. London: Routledge, 84–100.

———. 2010. *Europe’s 21st Century Challenge: Delivering Liberty*. Farnham: Ashgate.

Bigo, Didier, Philippe Bonditti, and Christian Olsson. 2016. “Mapping the European Field of Security Professionals.” In *Europe’s 21st Century Challenge*, Routledge, 71–86.

Bjerga, Kjell Inge. 2014. “Forsvarspolitikk og forvaltningspolitikk? Organisering, reformer og militæreksepsjonalisme i Forsvarets sentrale ledelse mellom 1940 og 2003 [Defense policy and administrative policy? Organization, reforms and military exceptionalism in the Defense’s central command between 1940 and 2003].” University of Bergen.

Bjerga, Kjell Inge, and Magnus Håkenstad. 2013. “‘Hvem eier krisen.’ Politi, Forsvar og 22. juli ["Who owns the crisis." Police, defence and 22. July].” In *Mellom fred og krig: norsk militær krisehåndtering*, eds. Anders Kjølberg and Tormod Heier. Oslo: Universitetsforlaget, 54–74.

Bjørgo, Tore, and Andres Ravik Jupskås. 2021. “Introduction by the Guest Editors of the Special Issue: The Long-Term Impacts of Attacks: The Case of the July 22, 2011 Attacks in Norway.” *Perspectives on Terrorism* 15(3): 2–13.

Blokland, Peter, and Genserik Reniers. 2019. “An Ontological and Semantic Foundation for Safety and Security Science.” *Sustainability* 11(21): 6024. https://www.mdpi.com/2071-1050/11/21/6024 (December 6, 2020).

Blum, Sonja. 2018. “The Multiple-Streams Framework and Knowledge Utilization: Argumentative Couplings of Problem, Policy, and Politics Issues.” *European Policy Analysis* 4(1): 94–117.

Blumer, Herbert. 1954. “What Is Wrong with Social Theory?” *American Sociological Review* 19(1): 3–10.

Bogen, Olav, and Magnus Håkenstad. 2017. “Reluctant Reformers: The Economic Roots of Military Change in Norway, 1990–2015.” *Defence Studies* 17(1): 23–37.

Boholm, Åsa, and Hervé Corvellec. 2011. “A Relational Theory of Risk.” *Journal of Risk Research* 14(2): 175–90.

———. 2016. “The Role of Valuation Practices for Risk Identification.” In *Riskwork: Essays on the Organizational Life of Risk Management*, ed. Michael Power. Oxford: Oxford University Press.

Boholm, Max, Niklas Möller, and Sven Ove Hansson. 2016. “The Concepts of Risk, Safety, and Security: Applications in Everyday Language.” *Risk Analysis* 36(2): 320–38.

Bolukbasi, H. Tolga, and Deniz Yıldırım. 2022. "Institutions in the Politics of Policy Change: Who Can Play, How They Play in Multiple Streams." *Journal of Public Policy*: 1–20.

Boréus, Kristina, and Göran Bergström. 2005. *Textens Mening Och Makt: Metodbok i Samhällsvetenskaplig Text- Och Diskursanalys*. 2. uppl. Lund: Studentlitteratur.

Børresen, Jacob, Gjeseth, G., and Tamnes, R. 2004. Norsk forsvarshistorie: 1970-2000. *Allianseforsvar i endring: 1970-2000 [The history of the Norwegian armed forces: 1970-2000. Changing alliance Defence]*. Bergen: Eide.

Bossong, Raphael, and Hendrik Hegemann. 2016. "EU Internal Security Governance and National Risk Assessments: Towards a Common Technocratic Model?" *European Politics and Society* 17(2): 226–41.

———. 2019. "Internal Security." In *Contemporary European Security*, eds. David J. Galbreath, Jocelyn Mawdsley, and Laura Chappell. Routledge, 101–19.

Boström, Magnus. 2006. "Regulatory Credibility and Authority through Inclusiveness: Standardization Organizations in Cases of Eco-Labelling." *Organization* 13(3): 345–67.

Botzem, Sebastian, and Leonhard Dobusch. 2012. "Standardization Cycles: A Process Perspective on the Formation and Diffusion of Transnational Standards." *Organization Studies* 33(5–6): 737–62.

Brinkmann, Svend. 2007. "Could Interviews Be Epistemic? An Alternative to Qualitative Opinion Polling." *Qualitative Inquiry* 13(8): 1116–38.

Brinkmann, Svend, and Steinar Kvale. 2015. *Det kvalitative forskningsintervju [The Qualitative Research Interview]*. 3. utg., 2. oppl. Oslo: Gyldendal Akademisk.

Brown, Gerald G., and Jr Louis Anthony Cox. 2011. "How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts." *Risk Analysis* 31(2): 196–204.

Brown, Prudence R. 2020. "Framing, Agency and Multiple Streams– a Case Study of Parks Policy in the Northern Territory." *Australian Journal of Political Science* 55(1): 55–71.

Brubaker, Rogers, and Frederick Cooper. 2000. "Beyond 'Identity.'" *Theory and Society* 29(1): 1–47.

Brunsson, Nils. 2000. "Organizations, Markets, and Standardization." In *A World of Standards*, eds. Bengt Jacobsson and Nils Brunsson. Oxford: Oxford University Press, 21–39.

Brunsson, Nils, and Bengt Jacobsson. 2000. "The Contemporary Expansion of Standardization." In *A World of Standards*, eds. Nils Brunsson and Bengt Jacobsson. Oxford University Press. 1–18.

Brunsson, Nils, Andreas Rasche, and David Seidl. 2012. "The Dynamics of Standardization: Three Perspectives on Standards in Organization Studies." *Organization Studies* 33(5–6): 613–32.

Burgess, Adam. 2016. "Introduction." In *Routledge Handbook of Risk Studies*, eds. Adam Burgess, Alberto Alemanno, and Jens O. Zinn. Abingdon: Routledge, 1–14.

Burgess, Adam, Jamie Wardman, and Gabe Mythen. 2018. "Considering Risk: Placing the Work of Ulrich Beck in Context." *Journal of Risk Research* 21(1): 1–5.

Busmundrud, Odd, Maren Maal, Jo Hagness Kiran, and Monica Endregard. 2015. 2015/00923 *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger [Approaches to Risk Assessments for Intentional Adverse Actions]*. Norwegian Defence Research Establishment.

Büthe, Tim, and Walter Mattli. 2011. *The New Global Rulers*. Princeton University Press.

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

Bye, Rolf J. et al. 2019. "The Institutional Context of Crisis. A Study of the Police Response during the 22 July Terror Attacks in Norway." *Safety Science* 111: 67–79.

Byrkjeflot, Haldor. 2018. "The Impact and Interpretation of Weber's Bureaucratic Ideal Type in Organisation Theory and Public Administration." In *Bureaucracy and Society in Transition*, Comparative Social Research, Emerald Publishing Limited, 13–35.

Cairney, Paul, and Michael D. Jones. 2016. "Kingdon's Multiple Streams Approach: What Is the Empirical Impact of This Universal Theory?" *Policy Studies Journal* 44(1): 37–58.

Charmaz, Kathy. 2017. "Special Invited Paper: Continuities, Contradictions, and Critical Inquiry in Grounded Theory." *International Journal of Qualitative Methods* 16(1): 1609406917719350.

Christensen, Johan, Cathrine Holst, and Anders Molander. 2023. *Expertise, Policy-Making and Democracy*. Routledge. https://doi-org.ezproxy.uio.no/10.4324/9781003106555 .

Ciută, Felix. 2009. "Security and the Problem of Context: A Hermeneutical Critique of Securitisation Theory." *Review of International Studies* 35: 2009: 2: 301-326.

Coar, Luan, and Julius Sim. 2006. "Interviewing One's Peers: Methodological Issues in a Study of Health Professionals." *Scandinavian Journal of Primary Health Care* 24(4): 251–56.

Cohen, Michael D., James G. March, and Johan P. Olsen. 1972. "A Garbage Can Model of Organizational Choice." *Administrative Science Quarterly* 17(1): 1–25.

Collier, Stephen J., and Andrew Lakoff. 2008. "The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem." In *Securing "the Homeland" − Critical Infrastructure, Risk and (in)Security*, ed. Myriam Dunn Cavelty and Kristian Søby Kristensen. London and New York: Routledge, 17–39.

Collins, Alan. 2016. "Introduction: What Is Security Studies?" In *Contemporary Security Studies*, ed. Alan Collins. Oxford New York: Oxford University Press, 1–10.

Committee to Review the Department of Homeland Security's Approach to Risk Analysis. 2010. *Review of the Department of Homeland Security's Approach to Risk Analysis*. National Academies Press.

Corry, Olaf. 2012. "Securitisation and 'Riskification': Second-Order Security and the Politics of Climate Change." *Millennium* 40(2): 235–58.

Cox, Louis Anthony (Tony), Jr. 2008. "Some Limitations of 'Risk = Threat × Vulnerability × Consequence' for Risk Analysis of Terrorist Attacks." *Risk Analysis* 28(6): 1749–61.

Creed, Irena F., Peter N. Duinker, Jacqueline N. Serran, and James W.N. Steenberg. 2019. "Managing Risks to Canada's Boreal Zone: Transdisciplinary Thinking in Pursuit of Sustainability." *Environmental Reviews* 27(3): 407–18.

Creswell, John W. 2013. *Qualitative Inquiry & Research Design: Choosing among Five Approaches*. 3rd ed. Los Angeles: Sage.

———. 2018. *Qualitative Inquiry & Research Design: Choosing among Five Approaches*. 4th ed., international student ed. Thousand Oaks, Calif: Sage.

Davies, Sandi J., Chrisopher A. Hertig, and Brion P. Gilbride, eds. 2015. *Security Supervision and Management: Theory and Practice of Asset Protection*. 4th edition. Amsterdam; Boston: Waltham, MA, USA: Butterworth-Heinemann.

De Goede, M. 2008. "Beyond Risk: Premediation and the Post-9/11 Security Imagination." *Security Dialogue* 39(2–3): 155–76.

Demortain, David. 2016. "The Work of Making Risk Frameworks." In *Riskwork: Essays on the Organizational Life of Risk Management*, ed. Michael Power. Oxford, United Kingdom: Oxford University Press, 26–49.

Djelic, Marie-Laure, and Kerstin Sahlin-Andersson. 2006a. *Transnational Governance: Institutional Dynamics of Regulation*. Cambridge: University Press.

Djelic, Marie-Laure, and Kerstin Sahlin-Andersson, eds. 2006b. "Contested Rules and Shifting Boundaries: International Standard-Setting in Accounting." In *Transnational Governance*, Cambridge: Cambridge University Press, 266–86.

Dolan, Dana A. 2021. "Multiple Partial Couplings in the Multiple Streams Framework: The Case of Extreme Weather and Climate Change Adaptation." *Policy Studies Journal* 49(1): 164–89.

Doty, Philip. 2015. "U.S. Homeland Security and Risk Assessment." *Government Information Quarterly* 32(3): 342–52.

Douglas, Mary, and Aaron Wildavsky. 1982. *Risk and Culture: An Essay on the Selection of Technical and Environmental Dangers*. University of California Press.

Dunn Cavelty, Myriam. 2008. "Like a Phoenix from the Ashes: The Reinvention of Critical Infrastructure Protection as Distributed Security." In *Securing "the Homeland": Critical Infrastructure, Risk and (in)Security*, eds. Myriam Dunn Cavelty and Kristian Søby Kristensen. London and New York: Routledge, 11–62.

Dunn Cavelty, Myriam, Mareile Kaufmann, and Kristian Søby Kristensen. 2015. "Resilience and (in)Security: Practices, Subjects, Temporalities." *Security Dialogue* 46(1): 3–14.

Dunn Cavelty, Myriam, and Kristian Søby Kristensen. 2008a. "Introduction − Securing the Homeland: Critical Infrastructure, Risk and (in)Security." In *Securing "the Homeland": Critical Infrastructure, Risk and (in)Security*, eds. Myriam Dunn Cavelty and Kristian Søby Kristensen. London and New York: Routledge, 1–14.

———. 2008b. *Securing "the Homeland": Critical Infrastructure, Risk and (in)Security*. Routledge.

Dunn, Kevin C., and Iver B. Neumann. 2016. *Undertaking Discourse Analysis for Social Research*. Ann Arbor, Mich: University Of Michigan Press.

Durnová, Anna P., and Christopher M. Weible. 2020. "Tempest in a Teapot? Toward New Collaborations between Mainstream Policy Process Studies and Interpretive Policy Studies." *Policy Sciences* 53(3): 571–88.

Dwyer, Sonya Corbin, and Jennifer L. Buckle. 2009. "The Space Between: On Being an Insider-Outsider in Qualitative Research." *International Journal of Qualitative Methods* 8(1): 54–63.

Eller, Warren S., and Adam S. Wandt. 2020. “Contemporary Policy Challenges in Protecting the Homeland.” *Policy Studies Journal* 48(S1): S33–46.

Endregard, Monica et al. 2016. *Protecting Society in a New Era*. Norwegian Defence Research Establishment (FFI). FFI Rapport.

———. 2019. “Totalforsvaret i et sivilt perspektiv [Total defense from a civil perspective].” In *Det nye totalforsvaret*, ed. Per M. Norheim-Martinsen. Oslo: Gyldendal, 62–80.

Engen, Ole Andreas. 2020. “Consensus and Conflicts Tripartite Model and Standardization in the Norwegian Petroleum Industry.” In *Standardization and Risk Governance. A Multi-Disciplinary Approach*, eds. Odd Einar Olsen, Kirsten Juhl, Preben H. Lindøe, and Ole Andreas Engen. London: Routledge, 255–74.

Engen, Ole Andreas, and Preben H. Lindøe. 2017. “The Nordic Model of Offshore Oil Regulation: Managing Crises through a Proactive Regulator.” In *Policy Shock*, eds. Edward J. Balleisen, Lori S. Bennear, Kimberly D. Krawiec, and Jonathan B. Wiener. Cambridge: Cambridge University Press, 181–203.

Engler, Fabian, and Nicole Herweg. 2019. “Of Barriers to Entry for Medium and Large n Multiple Streams Applications: Methodological and Conceptual Considerations.” *Policy Studies Journal* 47(4): 905–26.

European Commission. “CE Marking.” https://ec.europa.eu/growth/single-market/ce-marking_en (March 22, 2022).

Evensen, Vidar. 2000. *Metode for analyse av informasjonssikkerhet og objektsikkerhet [Method for Analyzing Information Security and Object Security]*. Trondheim: Norges teknisk naturvitenskapelige universitet.

Fimreite, Anne Lise, Peter Lango, Per Lægreid, and Lise H. Rykkja. 2013. “After Oslo and Utøya: A Shift in the Balance Between Security and Liberty in Norway?” *Studies in Conflict and Terrorism* 36(10): 839–56.

Fischer, Frank, and John Forester. 1993. *The Argumentative Turn in Policy Analysis and Planning*. Duke University Press.

Fløysvik Nordrum, Jon Christian. 2020. “Chapter 22. Legislation in Norway.” In *Legislation in Europe: A Country by Country Guide*, eds. Ulrich Karpen and Helen Xanthaki. Hart Publishing.

Frankel, Christian, and Erik Højbjerg. 2007. “The Constitution of a Transnational Policy Field: Negotiating the EU Internal Market for Products.” *Journal of European Public Policy* 14(1): 96–114.

Friedman, Uri. 2011. “Comparing How Norway and the U.S. Respond to Terror.” *The Atlantic*. https://www.theatlantic.com/international/archive/2011/07/comparing-how-norway-and-us-respond-terror/353336/ (March 28, 2022).

Friis, Karsten, and Erik Reichborn-Kjennerud. 2016. “From Cyber Threats to Cyber Risks.” In *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, Routledge Studies in Conflict, Security and Technology, eds. Karsten Friis and Jens Ringsmose. London, England New York, New York: Routledge, 27–44.

Furedi, Frank. 2009. “Precautionary Culture and the Rise of Possibilistic Risk Assessment.” *Erasmus Law Review* 2: 197–220.

George, Alexander, and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge, Mass: MIT Press.

Gerring, John. 2007. *Case Study Research: Principles and Practices*. Cambridge: Cambridge University Press.

Gilje, Nils. 2017. "Hermeneutik - teori og metode. [Hermeneutic – theory and method]" In *Kvalitativ analyse: Syv traditioner*, eds. Margaretha Järvinen and Nanna Mik-Meyer. København: Hans Reitzel.

Goldman, Ellen F., and Susan Swayze. 2012. "In-Depth Interviewing with Healthcare Corporate Elites: Strategies for Entry and Engagement." *International Journal of Qualitative Methods* 11(3): 230–43.

Greer, Scott. 2016. "John W. Kingdon, Agendas, Alternatives, and Public Policies." In *The Oxford Handbook of Classics in Public Policy and Administration*, eds. Martin Lodge, Edward C. Page, and Steven J. Balla. Oxford University Press, 17.

Grunnan, Tonje, Monica Endregard, Ragnhild E. Siedler, and Ann-Kristin Elstad. 2020. "Norwegian Societal Security and State Security - Challenges and Dilemmas." In *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, eds. Piero Baraldi, Francesco Di Maio, and Enrico Zio.

Gustafsson, Ingrid. 2020. How Standards Rule the World *Organizing a Global World: The Construction of a Global Control Regime*. Edward Elgar Publishing.

Gustavsen, Elin, and Torunn Laugen Haaland. 2019. "From Obligatory to Optional: Thirty Years of Civil–Military Entanglements in Norway." In *Civil–Military Entanglements*, Anthropological Perspectives, eds. Birgitte Refslund Sørensen and Eyal Ben-Ari. Berghahn Books, 80–99.

Haaland, Torunn Laugen. 2020. "Replikk til Harald Høibacks artikkel «Det omvendte militærkupp – en studie av militærprofesjonens vekst og fall» [Reply to Harald Høibacks article 'the reversed military coop - a study of the military professions' growth and descend']." *Nytt Norsk Tidsskrift* 37(3): 295–96.

Hacking, Ian. 1990. *The Taming of Chance*. Cambridge University Press.

Hagmann, Jonas, and Myriam Dunn Cavelty. 2012. "National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity." *Security Dialogue* 43(1): 79–96.

Hajer, Maarten. 2003. "Policy without Polity? Policy Analysis and the Institutional Void." *Policy Sciences* 36(2): 175–95.

Hajer, Maarten, and Wytske Versteeg. 2005. "A Decade of Discourse Analysis of Environmental Politics: Achievements, Challenges, Perspectives." *Journal of Environmental Policy & Planning* 7: 175–84.

Håkenstad, Magnus. 2019. "Den væpnede dugnaden - totalforsvaret under den kalde krigen [The armed vulentary community service during the Cold War]." In *Det nye totalforsvaret*, ed. Per M. Norheim-Martinsen. Oslo: Gyldendal, 25–40.

Hammersley, Martyn. 2014. "On the Ethics of Interviewing for Discourse Analysis." *Qualitative Research* 14(5): 529–41.

Hansson, Lars Fjell. 1997. "Ethical Problems of Preventive Medicine." University of Oslo, Faculty of Social Sciences, Department of Political Science.

Hansson, Sven Ove. 2007. "Risk and Ethics: Three Approaches." In *Risk: Philosophical Perspectives*, ed. Tim Lewens. London: Routledge, 21–35.

Harcourt, Alison, George Christou, and Seamus Simpson. 2020. *Global Standard Setting in Internet Governance*. Oxford University Press.

Hardy, Cynthia, Steve Maguire, Michael Power, and Haridimos Tsoukas. 2020. "Organizing Risk: Organization and Management Theory for the Risk Society." *Academy of Management Annals* 14(2): 1032–66.

Heath, Joseph. 2020. *The Machinery of Government: Public Administration and the Liberal State*. Oxford University Press.

Helms, Mills Jean, Amy Thurlow, and Albert J. Mills. 2010. "Making Sense of Sensemaking: The Critical Sensemaking Approach." *Qualitative Research in Organizations and Management: An International Journal* 5(2): 182–95.

Herweg, Nicole, and Nikolaos Zahariadis. 2017. "The Multiple Streams Approach." In *The Routledge Handbook of European Public Policy*, eds. Nikolaos Zahariadis and Laurie Buonanno. Routledge, 32–41.

Heyerdahl, Anne. 1996. "Et hav av risiko? Eller fra vitenskap til politikk? En systemteoretisk analyse av Londonkonvensjonens vurderinger av risiko forbundet med dumping av radioaktivt avfall [An Ocean at Risk? Or from Science to Politics? A Systems Theoretical Analysis of the London Convention's Prohibition of the Dumping of Low-Radioactive Waste]." Master Thesis. University of Bergen.

Higgins, Winton, and Kristina Tamm Hallström. 2007. "Standardization, Globalization and Rationalities of Government." *Organization* 14(5): 685–704. https://doi.org/10.1177/1350508407080309 (September 2, 2021).

Hjelum, Magnus Sirnes, and Per Lægreid. 2019. "The Challenge of Transboundary Coordination: The Case of the Norwegian Police and Military." *Safety Science* 115: 131–40.

Hoffmann, Sophia. 2021. "Circulation, Not Cooperation: Towards a New Understanding of Intelligence Agencies as Transnationally Constituted Knowledge Providers." *Intelligence and National Security* 36(6): 807–26.

Holst, Cathrine, and Anders Molander. 2019. "Epistemic Democracy and the Role of Experts." *Contemporary Political Theory* 18(4): 541–61.

Hood, Christopher. 2002. "The Risk Game and the Blame Game." *Government and Opposition* 37(1): 15–37.

Hovden, Jan. 2004. "Public Policy and Administration in a Vulnerable Society: Regulatory Reforms Initiated by a Norwegian Commission." *Journal of Risk Research* 7(6): 629–41.

Howlett, Michael, Allan McConnell, and Anthony Perl. 2017. "Moving Policy Theory Forward: Connecting Multiple Stream and Advocacy Coalition Frameworks to Policy Cycle Models of Analysis." *Australian Journal of Public Administration* 76(1): 65–79.

Høyland, Sindre Aske. 2018. "Exploring and Modeling the Societal Safety and Societal Security Concepts – A Systematic Review, Empirical Study and Key Implications." *Safety Science* 110: 7–22.

Hultin, Lotta, and Magnus Mähring. 2017. “How Practice Makes Sense in Healthcare Operations: Studying Sensemaking as Performative, Material-Discursive Practice.” *Human Relations* 70(5): 566–93.

Hutter, Bridget, and Michael Power, eds. 2005. *Organizational Encounters with Risk*. Cambridge University Press.

Huysmans, Jef. 2009. “Agency and the Politics of Protection. Implication for Security Studies.” In *The Politics of Protection: Sites of Insecurity and Political Agency*, Routledge Advances in International Relations and Global Politics, eds. Jef Huysmans, Andrew Dobson, and Raia Prokhovnik. London: Routledge, 1–18.

———. 2011. “What’s in an Act? On Security Speech Acts and Little Security Nothings.” *Security Dialogue* 42(4–5): 371–83.

Huysmans, Jef, Andrew Dobson, and Raia Prokhovnik, eds. 2009. *The Politics of Protection: Sites of Insecurity and Political Agency*. London: Routledge.

Idsø, Einar Skavland, and Øyvind Mejdell Jakobsen. 2000. *Objekt- og informasjonssikkerhet: metode for risiko- og sårbarhetsanalyse [Object- and information security: method for risk and vulnerability analysis]*. Trondheim: Institutt for produksjons- og kvalitetsteknikk, Norges teknisknaturvitenskapelige [sic] universitet.

ISO. “Standards.” *ISO*. https://www.iso.org/standards.html (March 16, 2021).

Jacobsen, Bengt. 2000. “Standardization and Expert Knowledge.” In *A World of Standards*, eds. Nils Brunsson and Bengt Jacobsson. Oxford: Oxford University Press.

Jacobsson, Bengt, and Nils Brunsson, eds. 2000. *A World of Standards*. Oxford: Oxford University Press.

Jann, Werner. 2016. *Michael D. Cohen, James G. March, and Johan P. Olsen, “A Garbage Can Model of Organizational Choice.”* eds. Martin Lodge, Edward C. Page, and Steven J. Balla. Oxford University Press.

Jarvis, Lee. 2015. *Security: A Critical Introduction*. Palgrave Macmillan.

Jasanoff, Sheila. 1994. “Acceptable Evidence in a Pluralistic Society.” In *Acceptable Evidence in a Pluralistic Society*, Oxford University Press.

Jensen, Susan B., Per Lægreid, and Lise H. Rykkja. 2019. “Changes in the Norwegian Central Crisis Management After the Terrorist Attacks in 2011.” In *Societal Security and Crisis Management*, eds. Per Lægreid and Lise H. Rykkja. Cham: Springer International Publishing, 205–23.

Jones, Michael D. et al. 2016. “A River Runs Through It: A Multiple Streams Meta-Review.” *Policy Studies Journal* 44(1): 13–36.

Jore, Sissel H. 2012. “Counterterrorism as Risk Management Strategies.” University of Stavanger, Norway.

———. 2019. “The Conceptual and Scientific Demarcation of Security in Contrast to Safety.” *European Journal for Security Research* 4(1): 157–74.

———. 2020. “Is Resilience a Favourable Concept in Terrorism Research? The Multifaceted Discourses of Resilience in the Academic Literature.” *Critical Studies on Terrorism*: 1–21.

Jore, Sissel H., and Anne Egeli. 2015. “Risk Management Methodology for Protecting against Malicious Acts? Are Probabilities Adequate Means for Describing Terrorism and Other Security Risks?” In

Safety and Reliability of Complex Engineered Systems: Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015, 7-10 September 2015, eds. Luca Podofillini et al. Zürich, Switzerland: CRC Press, 807–15.

Jørgensen, Lene, and Silvia Jordan. 2016. “Risk Mapping: Day-to-Day Riskwork in Inter-Organizational Project Management.” In *Riskwork: Essays on the Organizational Life of Risk Management*, ed. Michael Power. Oxford University Press.

Judge, Andrew, and Tomas Maltby. 2017. “European Energy Union? Caught between Securitisation and ‘Riskification.’” *European Journal of International Security* 2(2): 179–202.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Kalfagianni, Agni, and Philipp Pattberg. 2013. “Participation and Inclusiveness in Private Rule-Setting Organizations: Does It Matter for Effectiveness?” *Innovation: The European Journal of Social Science Research* 26(3): 231–50.

Kgl.res. 3. November 2000 and Kgl.res. 24. June 2005 – *see Ministry of Justice and the Police reference*.

Kingdon, John W. 2013. *Agendas, Alternatives, and Public Policies*. Second. Pearson Education Limited.

Kirchner, Emil, and James Sperling. 2018. EU security governance *EU Security Governance*. Manchester University Press.

Klima, Noel, Nicholas Dorn, and Tom Vander Beken. 2011. “Risk Calculation and Precautionary Uncertainty: Two Configurations within Crime Assessment.” *Crime, Law and Social Change* 55(1): 15–31.

Klinke, Andreas, and Ortwin Renn. 2002. “A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies.” *Risk Analysis* 22(6): 1071–94.

Koselleck, Reinhart. 2004. *Futures Past: On the Semantics of Historical Time*. Columbia University Press.

Krahmann, Elke. 2011. “Beck and beyond: Selling Security in the World Risk Society.” *Review of International Studies* 37(1): 349–72.

Lægreid, Per, and Synnøve Serigstad. 2006. “Framing the Field of Homeland Security: The Case of Norway.” *Journal of Management Studies* 43(6): 1395–1413.

Lampland, Martha, and Susan Leigh Star. 2009. *Standards and Their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life*. Ithaca, N.Y: Cornell University Press.

Lango, Peter, and Per Lægreid. 2011. “Samordning for samfunnssikkerhet [Coordination for Societal Security].” In *Organisering, samfunnssikkerhet og krisehåndtering*, eds. Anne Lise Fimreite, Peter Lango, Per Lægreid, and Lise H. Rykkja. Oslo: Universitetsforlaget, 39–64.

Lango, Peter, Lise H. Rykkja, and Per Lægreid. 2011. Risk Management Trends *Organizing for Internal Security and Safety in Norway*. IntechOpen. https://www.intechopen.com/books/risk-management-trends/organizing-for-internal-security-and-safety-in-norway (May 27, 2021).

Langvatn, Silje Aa., and Cathrine Holst. 2022. “Expert Accountability: What Does It Mean, Why Is It Challenging—and Is It What We Need?” *Constellations* n/a(n/a): 1–16.

Larsson, Sebastian, and Mark Rhinard, eds. 2020. *Nordic Societal Security. Convergence and Divergence*. 1st ed. London: Routledge.

———. 2021. “Introduction: Comparing and Conceptualising Nordic Societal Security.” In *Nordic Societal Security*, eds. Sebastian Larsson and Mark Rhinard. Taylor & Francis, 3–21.

Levy, Jack S. 2008. “Case Studies: Types, Designs, and Logics of Inference.” *Conflict Management and Peace Science* 25(1): 1–18.

Lewens, Tim. 2007. “Introduction: Risk and Philosophy.” In *Risk: Philosophical Perspectives*, ed. Tim Lewens. London: Routledge, 1–20.

Lindøe, Preben, Michael Baram, and Sverre Braut. 2017. “Risk Regulation and Proceduralization: An Assessment of Norwegian and US Risk Regulation in Offshore Oil and Gas Industry.” In *Trapping Safety into Rules: How Desirable or Avoidable Is Proceduralization?*, eds. Corinne Bieder and Mathilde Bourrier. CRC Press, 69–86.

Lindøe, Preben Hempel, Michael Baram, and Ortwin Renn, eds. 2013. *Risk Governance of Offshore Oil and Gas Operations*. Cambridge: Cambridge University Press.

Liodden, Tone Maia. 2017. no. 642 “The Burdens of Discretion: Managing Uncertainty in the Asylum Bureaucracy.” University of Oslo, Faculty of Social Sciences, Department of Sociology and Human Geography.

Luhmann, Niklas. 1991. *Soziologie des* risikos *[Risk: A Sociological Theory]*. Berlin: De Gruyter.

Lupton, Deborah. 2013. *Risk*. 2nd ed. London: Routledge.

Maal, Maren, Odd Busmundrud, and Monica Endregard. 2016. “Methodology for Security Risk Assessments – Is There a Best Practice?” In *Risk, Reliability and Safety: Innovating Theory and Practice*, eds. Matthew Revie, Tim Bedford, and Lesley Walls. London: Taylor & Francis, 860–66.

Macenaite, Milda. 2017. “The ‘Riskification’ of European Data Protection Law through a Two-Fold Shift.” *European Journal of Risk Regulation: EJRR; Berlin* 8(3): 506–40.

Mangset, Marte. 2017. “Margaretha Järvinen & Nanna Mik-Meyer (red.): Kvalitativ analyse. Syv traditioner [Qualitative analysis. Seven traditions].” *Tidsskrift for samfunnsforskning* 58(03): 361–63.

Manunta, Giovanni. 1997. *Towards a Security Science Through a Specific Theory and Methodology*. University of Leicester: PhD thesis.

———. 2002. “Risk and Security: Are They Compatible Concepts?” *Security Journal* 15(2): 43–55.

Martin, Paul. 2019. *The Rules of Security: Staying Safe in a Risky World*. New product edition. Oxford, England: Oxford University Press.

Meld.St. – *see references under Ministry of Justice and Public Security.*

Menon-Publication. 2018. *The Influence of Standards on the Nordic Economies*. Menon-Publication.

Metscher, Robert A. 2015. “What Is Asset Protection?” In *Security Supervision and Management: Theory and Practice of Asset Protection*, eds. Sandi J. Davies, Chrisopher A. Hertig, and Brion P. Gilbride. Amsterdam ; Boston: Waltham, MA, USA: Butterworth-Heinemann, 3–8.

Mikes, Anette. 2009. “Risk Management and Calculative Cultures.” *Management Accounting Research* 20(1): 18–40.

Molven, Olav. 2009. “Kravet til helsepersonell og virksomheter i helsetjenesten om forsvarlighet – Statens helsetilsyns tilnærming.” *Lov og Rett* 48(1): 3–26.

Morsut, Claudia. 2021. “The Emergence and Development of Samfunnssikkerhet in Norway.” In *Nordic Societal Security*, eds. Sebastian Larsson and Mark Rhinard. Taylor & Francis, 68–90.

Mueller, John, and Mark G. Stewart. 2011. “Balancing the Risks, Benefits, and Costs of Homeland Security.” *Homeland Security Affairs* 7(1).

———. 2014. “Terrorism and Counterterrorism in the US: The Question of Responsible Policy-Making.” *The International Journal of Human Rights* 18(2): 228–40.

Mythen, Gabe, and Sandra Walklate. 2008. “Terrorism, Risk and International Security: The Perils of Asking ‘What If?’” *Security Dialogue* 39(2–3): 221–42.

Natow, Rebecca S. 2020. “The Use of Triangulation in Qualitative Studies Employing Elite Interviews.” *Qualitative Research* 20(2): 160–73.

Neal, Andrew W. 2019. *Security as Politics: Beyond the State of Exception*. Edinburgh: Edinburgh University Press.

Nielsen, Kitt Plinia. 2020. “From Insurance to Intelligence: A Conceptual History of Political Risk.” University of Copenhagen.

Norheim-Martinsen, Per M. 2016. “New Sources of Military Change – Armed Forces as Normal Organizations.” *Defence Studies* 16(3): 312–26.

———, ed. 2019a. *Det nye totalforsvaret [The new total defense]*. Oslo: Gyldendal.

———. 2019b. “Introduksjon: Det nye totalforsvaret - utviklingstrekk og utfordringer [Introduction: The new total defense].” In *Det nye totalforsvaret*, ed. Per M. Norheim-Martinsen. Oslo: Gyldendal, 11–24.

Norwegian Defence Research Establishment. 2015. *FFI-Forum: Risikovurderinger for tilsiktede handlinger. [FFI-Forum: Risk Assessment for Intentional Undesirable Actions]*. https://soundcloud.com/ffiaudio/sets/ffiforum (April 29, 2021).

Norwegian Directorate for Civil Protection. 2011. *Nasjonal sårbarhets- Og beredskapsrapport 2011 [National Vulnerability and Civil Protection Report]*.

———. 2013. *National Risk Picture*. https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2013.pdf (February 11, 2022).

———. 2014. *National Risk Picture*. https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2014.pdf (February 11, 2022).

———. 2019. *Analyses of Crisis Scenarios 2019*. https://www.dsb.no/globalassets/dokumenter/rapporter/p2001636_aks_2019_eng.pdf (June 5, 2022).

Norwegian Ministry of Defence. 1995. *Beredskapslovgivningen i lys av endrede forsvars- og sikkerhetspolitiske rammebetingelser [Civil protection regulation in light of a changing defense- and security-political context]*. regjeringen.no. NOU.

———. 1997. *Ot.prp. nr. 49 (1996-97) Om Lov om forebyggende sikkerhetstjeneste [About the Security Act]*. regjeringen.no.

———. 2001. *Lov om forebyggende sikkerhetstjeneste [Security Act]*.

———. 2017. *Prop. 153 L Lov om nasjonal sikkerhet [Security Act Proposal]*.

Norwegian Ministry of Justice and Public Security. 2017a. *Instructions for the Ministries' Work with Civil Protection and Emergency Preparedness*.

———. 2017b. *Meld. St. 10 (2016–2017) Risk in a Safe and Secure Society - On Public Security. Executive Summary in English*.

———. 2019. *Lov om nasjonal sikkerhet [Security Act]*.

Norwegian Ministry of Justice and Public Security. 2021. *Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden [Societal security in an unsecure world]*. regjeringen.no.

Norwegian Ministry of Justice and Public Security, and Norwegian Ministry of Defence. 2018. *Støtte og samarbeid, En beskrivelse av totalforsvaret i dag*.

Norwegian Ministry of Justice and the Police. 1993. *St.Meld. Nr. 24 (1992-93) Det fremtidige sivile beredskap [The Future Civil Preparedness]*.

———. 2000. Kg.res. *Instruks om internkontroll og systemrettet tilsyn med det sivile beredskapsarbeidet [Instructions for Internal Control and Systems Audits with Civil Preparedness]*.

———. 2005. *Kgl.res. Instruks for Direktoratet for Samfunnssikkerhet og beredskaps koordinerende Roller [Royal Decree Regarding the Directorate for Civil Protection's Coordinating Role]*.

Norwegian Ministry of Local Government and Modernisation. 2019. *About the Relationship between Political Leadership and the Civil Service - Seven Duties for the Civil Service*.

Norwegian National Security Authority. 2006. *Veiledning i risiko- og sårbarhetsanalyse [Guideline - Risk- and Vulnerability Assessment]*.

———. 2015. *Sikkerhetsfaglig råd [Security Advice from a Professional Point of View]*.

———. 2020. "About the Norwegian National Security Authority."

———. 2022. "Fagområder [Areas of responsebility]."

Norwegian National Security Authority, Norwegian Police Security Agency, and National Police Directorate. 2010. *En veiledning. Sikkerhets- og beredskapstiltak mot terrorhandlinger [Guideline to protective and preparedness measures against terrorism]*.

Norwegian National Security Authority, Norwegian Police Security Service, and National Police Directorate. 2015. *Terrorsikring. En veildning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger [Terror Protection. A Guideline in Security- and Preparedness Measures against Intentional Unwanted Actions]*.

NOU. 2000. *Et sårbart samfunn. [A Vulnerable Society]*.

———. 2012. *Rapport fra 22. juli-kommisjonen [Report from the 22. July commission]*.

———. 2016. *Samhandling for sikkerhet [Cooperation for Security]*.

Nyman, Jonna. 2018. "Securitization." In *Security Studies: An Introduction*, eds. Paul Williams and Matt McDonald. London: Routledge, 100–113.

Odendahl, Teresa, and Aileen M. Shaw. 2012. "Interviewing Elites." In *The SAGE Handbook of Interview Research: The Complexity of the Craft*, eds. Jaber Gubrium, James Holstein, Amir Marvasti, and Karyn McKinney. Thousand Oaks: United States, California, Thousand Oaks: SAGE Publications, Inc.

Øksne, Anders, and Helge Rager Furuseth. 2004. *Risikohåndtering: bruk av risikoanalyser i det kontinuerlige sikkerhetsarbeidet [Risk management: The use of risk analysis in continuous security management]*. Trondheim: NTNU, Institutt for produksjons- og kvalitetsteknikk.

Olsen, Odd Einar. 2020a. "Dilemmas of Standardization in Risk Governance." In *Standardization and Risk Governance. A Multi-Disciplinary Approach*, eds. Odd Einar Olsen, Kirsten Juhl, Preben H. Lindøe, and Ole Andreas Engen. London: Routledge, 275–80.

———. 2020b. "The Standardization of Risk Governance." In *Standardization and Risk Governance. A Multi-Disciplinary Approach*, eds. Odd Einar Olsen, Kirsten Juhl, Preben H. Lindøe, and Ole Andreas Engen. London: Routledge, 3–15.

Olsen, Odd Einar, Bjørn Ivar Kruke, and Jan Hovden. 2007. "Societal Safety: Concept, Borders and Dilemmas." *Journal of Contingencies and Crisis Management* 15(2): 69–79.

O'Malley, Pat. 2008. "Governmentality and Risk." In *Social Theories of Risk and Uncertainty: An Introduction*, ed. Jens O. Zinn. Malden, Mass: Blackwell, 52–75.

———. 2010. "Resilient Subjects: Uncertainty, Warfare and Liberalism." *Economy and Society* 39(4): 488–509.

———. 2011. "Security after Risk: Security Strategies for Governing Extreme Uncertainty." *Current Issues in Criminal Justice* 23(1): 5–15.

Organisation For Economic, Co-Operation and Development. 2010. *Risk and Regulatory Policy: Improving the Governance of Risk*. Paris: OECD Publishing.

Parker, Charlie, Sam Scott, and Alistair Geddes. 2019. "Snowball Sampling." *SAGE research methods foundations*.

Peoples, Columba, and Nick Vaughan-Williams. 2021. *Critical Security Studies: An Introduction*. 3rd edition. London, New York, NY: Routledge.

Petersen, Karen Lund. 2012a. *Corporate Risk and National Security Redefined*. Milton Park, Abingdon, Oxon; New York, NY: Routledge.

———. 2012b. "Risk Analysis – A Field within Security Studies?" *European Journal of International Relations* 18(4): 693–717.

———. 2013. "The Corporate Security Professional: A Hybrid Agent between Corporate and National Security." *Security Journal* 26(3): 222–35.

———. 2017. "Risk and Security." In *Routledge Handbook of Security Studies*, eds. Myriam Dunn Cavelty and Thierry Balzacq. London: Routledge.

Pettersen Gould, Kenneth Arne, and Corinne Bieder. 2020. “Safety and Security: The Challenges of Bringing Them Together.” In *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*, SpringerBriefs in Applied Sciences and Technology, eds. Corinne Bieder and Kenneth Arne Pettersen Gould. Cham: Springer International Publishing, 1–8.

Pettersen Gould, Kenneth Arne, and Torkel Bjørnskau. 2015. “Organizational Contradictions between Safety and Security – Perceived Challenges and Ways of Integrating Critical Infrastructure Protection in Civil Aviation.” *Safety Science* 71: 167–77.

Pouliot, Vincent. 2008. “The Logic of Practicality: A Theory of Practice of Security Communities.” *Int Org* 62(2): 257–88.

Power, Michael. 1997. *The Audit Society: Rituals of Verification*. Oxford: Oxford University Press.

———. 2002. “Standardization and the Regulation of Management Control Practices.” *Soziale Systeme* 8(2): 191–204.

———. 2004. *The Risk Management of Everything - Rethinking the Politics of Uncertainty*. Demos.

———. 2007. *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

———. 2014. “Risk, Social Theories, and Organizations.” In *The Oxford Handbook of Sociology, Social Theory, and Organization Studies*, eds. Paul Adler, Paul du Gay, Glenn Morgan, and Mike Reed. Oxford: Oxford University Press, 370–92.

———. 2016a. “Postscript.” In *Riskwork: Essays on the Organizational Life of Risk Management*, ed. Michael Power. Oxford: Oxford University Press.

———. 2016b. *Riskwork: Essays on the Organizational Life of Risk Management*. Oxford: Oxford University Press.

———. 2021. “Modelling the Micro-Foundations of the Audit Society: Organizations and the Logic of the Audit Trail.” *Academy of Management Review* 46(1): 6–32.

Power, Michael, Tobias Scheytt, Kim Soin, and Kerstin Sahlin. 2009. “Reputational Risk as a Logic of Organizing in Late Modernity.” *Organization Studies* 30(2–3): 301–24.

President’s Commission on Critical Infrastructure Protection, Edward M. 1997. *Critical Foundations: Protecting America’s Infrastructures*.

Prime Minister’s office. 2011. “Speech by Prime Minister Jens Stoltenberg.”

Ragin, Charles C., and Howard S. Becker. 1992. *What Is a Case? Exploring the Foundations of Social Inquiry*. Cambridge: University Press.

Ramanna, Karthik. 2015. *Political Standards: Corporate Interest, Ideology, and Leadership in the Shaping of Accounting Rules for the Market Economy*. Chicago, London: The University of Chicago Press.

Rasche, Andreas, and David Seid. 2019. *Management Ideas as Standards*. Oxford: Oxford University Press.

Rashid, Imir, and Seamus Simpson. 2019. “The Struggle for Co-Existence: Communication Policy by Private Technical Standards Making and Its Limits in Unlicensed Spectrum.” *Information, Communication & Society* 0(0): 1–18.

Rausand, Marvin. 1991. *Risikoanalyse. Veiledning til NS 5814*. Tapir Forlag.

Reardon, Louise. 2018. “Networks and Problem Recognition: Advancing the Multiple Streams Approach.” *Policy Sciences* 51(4): 457–76.

Renå, Helge, and Johan Christensen. 2020. “Learning from Crisis: The Role of Enquiry Commissions.” *Journal of Contingencies and Crisis Management* 28(1): 41–49.

ResiStand. 2017. *Report on the Industry’s Participation in Standardisation – Current Situation and Future Expectations*. https://cordis.europa.eu/project/id/700389/results.

———. 2018. “ResiStand: Final Conference Brief.”

Roe, Paul. 2016. “Societal Security.” In *Contemporary Security Studies*, ed. Alan Collins. Oxford New York: Oxford University Press, 213–18.

Rogers, Peter. 2017. “The Etymology and Genealogy of a Contested Concept.” In *The Routledge Handbook of International Resilience*, eds. David Chandler and Jon Coaffee. London: Routledge, 13–25.

Rolin, Kristina. 2020. “Situated Knowledge and Objectivity.” In *The Routledge Handbook of Feminist Philosophy of Science*, Routledge.

Rose, Nikolas, and Peter Miller. 1992. “Political Power beyond the State: Problematics of Government.” *The British Journal of Sociology* 43(2): 173–205.

Rosenberg, M Michael. 2016. “The Conceptual Articulation of the Reality of Life: Max Weber’s Theoretical Constitution of Sociological Ideal Types.” *Journal of Classical Sociology* 16(1): 84–101.

Roulston, Kathryn. 2010a. “Asking Questions and Individual Interviews.” In *Reflective Interviewing: A Guide to Theory and Practice*. London: SAGE Publications Ltd.

———. 2010b. *Reflective Interviewing: A Guide to Theory and Practice*. London: SAGE Publications Ltd.

Ryggvik, Helge. 2008. *Adferd, teknologi og system - En sikkerhetshistorie [Behavior, Technology and System - a Security History]*. Trondheim: Tapir akademisk forlag.

Sætren, Harald. 2016. “From Controversial Policy Idea to Successful Program Implementation: The Role of the Policy Entrepreneur, Manipulation Strategy, Program Design, Institutions and Open Policy Windows in Relocating Norwegian Central Agencies.” *Policy Sciences* 49(1): 71–88.

Salter, Mark B., and Can E. Mutlu. 2018. “Methods in Critical Security Studies. An Introduction.” In *The Oxford Handbook of International Security*, Oxford handbooks online, eds. Alexandra Gheciu and William Curti Wohlforth. Oxford: Oxford University Press.

Sandberg, Jörgen, and Haridimos Tsoukas. 2015. “Making Sense of the Sensemaking Perspective: Its Constituents, Limitations, and Opportunities for Further Development.” *Journal of Organizational Behavior* 36(S1): S6–32.

Schmidt, Vivien A. 2008. “Discursive Institutionalism: The Explanatory Power of Ideas and Discourse.” *Annual Review of Political Science* 11(1): 303–26.

———. 2010. “Taking Ideas and Discourse Seriously: Explaining Change through Discursive Institutionalism as the Fourth ‘New Institutionalism.’” *European Political Science Review* 2(1): 1–25.

Schwalbe, Michael. 2020. “The Spirit of Blumer’s Method as a Guide to Sociological Discovery.” *Symbolic Interaction* 43(4): 597–614.

Schwartz-Shea, Peregrine. 2014. “Judging Quality? Evaluative Criteria and Epistemic Communities.” In *Interpretation and Method: Empirical Research Methods and the Interpretive Turn*, eds. Dvora Yanow and Peregrine Schwartz-Shea. Armonk, N.Y.: M.E. Sharpe.

Scott, W. Richard. 2014. *Institutions and Organizations: Ideas, Interests, and Identities*. 4th ed. Thousand Oaks, Calif: Sage.

Security Acts – *see references under Norwegian Ministry of Defense and Norwegian Ministry of Justice and Public Security.*

Sennewald, Charles A., and Curtis Baillie. 2020. *Effective Security Management*. Butterworth-Heinemann.

Shephard, Daniel D. et al. 2021. “Kingdon’s Multiple Streams Approach in New Political Contexts: Consolidation, Configuration, and New Findings.” *Governance* 34(2): 523–43.

Skotnes, Ruth Østgaard, and Ole Andreas Engen. 2015. “Attitudes toward Risk Regulation – Prescriptive or Functional Regulation?” *Safety Science* 77: 10–18.

Slager, Rieneke, Jean-Pascal Gond, and Jeremy Moon. 2012. “Standardization as Institutional Work: The Regulatory Power of a Responsible Investment Standard.” *Organization Studies* 33(5–6): 763–90.

Slovic, Paul. 1987. “Perception of Risk.” *Science* 236(4799): 280–85.

Smith, Clifton, and David J. Brooks. 2012. *Security Science*. 1st ed. Butterworth-Heinemann.

Søby Kristensen, Kristian. 2008. “‘The Absolute Protection of Our Citizens’: Critical Infrastructure Protection and the Practice of Security.” In *Securing “the Homeland”: Critical Infrastructure, Risk and (in)Security*, eds. Myriam Dunn Cavelty and Kristian Søby Kristensen. London and New York: Routledge, 63–83.

Society for Risk Analysis. 2018. “Risk Analysis: Fundamental Principles.” https://www.sra.org/risk-analysis-overview/fundamental-principles/.

Sørensen, Eva, and Jacob Torfing. 2005. “The Democratic Anchorage of Governance Networks.” *Scandinavian Political Studies* 28(3): 195–218.

Standards Australia. 2006. “HB 167-2006 Security Risk Management.” https://store.standards.org.au/product?designationId=HB+167-2006 (February 17, 2022).

Standards Norway. 1991. 5814 *NS 5814 Krav til risikoanalyser [Requirements for Risk Analysis]*. Standards Norway.

———. 2008. *NS 5814 Krav til risikovurderinger [Requirements for Risk Assessment]*.

———. 2012. *NS 5830 Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi [Societal Security. Protection against Undesireable Intentional Actions. Terminology]*.

———. 2014. *NS 5832 Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse [Societal Security. Protection against Intentional Undesirable Actions. Requirements for Security Risk Analysis]*.

———. 2018. “Regler for standardiseringsarbeid [Rules for Standardization].” https://www.standard.no/Global/PDF/2018%20Regler%20for%20standardiseringsarbeid.pdf (January 25, 2021).

———. 2021. *Årsrapport 2020 [Annual Report]*. https://www.standard.no/Global/PDF/Standard%20Norge/%c3%85rsrapport%202020.pdf (March 22, 2022).

———. “Hvordan lages standarder? [How Are Standards Made?].” https://www.standard.no/standardisering/hvordan-lages-standarder/ (March 25, 2021a).

———. “SN/K 296.” https://www.standard.no/standardisering/komiteer/sn/snk-296/ (October 9, 2022b).

Steinmo, Sven. 2015. “Institutionalism.” In *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, ed. James D. Wright. Oxford: Elsevier, 181–85.

Stern, Jessica, and Jonathan B. Wiener. 2006. “Precaution against Terrorism.” *Journal of Risk Research* 9(4): 393–447.

Stewart, Mark G., and John Mueller. 2020. “Terrorism Risks, Chasing Ghosts and Infrastructure Resilience.” *Sustainable and Resilient Infrastructure* 5(1–2): 78–89.

St.Meld. *see reference under Ministry of Justice and the Police*

Stranden, Roy. 2019. *Sikring: En innføring i teori og praksis [Securing. An Introduction in Theory and Practice]*. 1. utgave. Oslo: Gyldendal.

Sundelius, Bengt. 2005a. “A Brief on Embedded Societal Security.” *Information & Security: An International Journal* 17: 23–37.

———. 2005b. “From National Total Defense to Embedded Societal Security.” In *Protecting the Homeland: European Approaches to Societal Security: Implications for the United States*, eds. Daniel S. Hamilton, Bengt Sundelius, and Jesper Grönvall. Washington, D.C: Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, 1–16.

Sunstein, Cass R. 2005. *Laws of Fear: Beyond the Precautionary Principle*. Cambridge: Cambridge University Press.

Swedberg, Richard. 2014. *The Art of Social Theory*. STU-Student edition. Princeton University Press.

———. 2018. “How to Use Max Weber’s Ideal Type in Sociological Analysis.” *Journal of Classical Sociology* 18(3): 181–96.

Swyngedouw, Erik. 2005. “Governance Innovation and the Citizen: The Janus Face of Governance-beyond-the-State.” *Urban Studies* 42(11): 1991–2006.

Synstnes, Hans Morten. 2016. *Den innerste sirkel: den militære sikkerhetstjenesten 1945-2002 [The innermost circle: the military security service 1945-2002]*. Oslo: Dreyer.

Tang, Yi Shin, and Bruno Youssef Yunen Alves de Lima. 2019. “Private Standards in the WTO: A Multiple Streams Analysis of Resisting Forces in Multilateral Trade Negotiations.” *Contexto Internacional* 41(3): 501–27.

The Research Council of Norway. 2019. “Public Sector Ph.D. Scheme.” https://www.forskningsradet.no/en/apply-for-funding/funding-from-the-research-council/public-sector-phd-scheme/ (July 10, 2022).

Thompson, Kimberly M., Paul F. Deisler Jr., and Richard C. Schwing. 2005. “Interdisciplinary Vision: The First 25 Years of the Society for Risk Analysis (SRA), 1980–2005.” *Risk Analysis* 25(6): 1333–86.

Thorton, Patricia H., and William Ocasio. 2008. “Institutional Logics.” In *The SAGE Handbook of Organizational Institutionalism*, SAGE, 99–128.

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.

Timmermans, Stefan, and Iddo Tavory. 2012. “Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis.” *Sociological Theory* 30(3): 167–86.

Tjora, Aksel. 2018. *Qualitative Research as Stepwise-Deductive Induction*. London: Routledge.

Vlek, Charles. 2013. “How Solid Is the Dutch (and the British) National Risk Assessment? Overview and Decision-Theoretic Evaluation.” *Risk Analysis* 33(6): 948–71.

Wæver, Ole. 1995. “Securitization and Desecuritization.” In *On Security*, New Directions in World Politics, ed. Ronnie D. Lipschutz. New York: Columbia University Press, 46–86.

———. 2011. “Politics, Security, Theory.” *Security Dialogue* 42(4–5): 465–80.

———. 2019. “What Is Constantly Changing? Continuity Is!” ed. Mark B Salter. *Security Dialogue* 50(4_suppl): 17–18.

Wæver, Ole, and Barry Buzan. 2016. “After the Return to Theory: The Past, Present, and Future of Security Studies.” In *Contemporary Security Studies*, ed. Alan Collins. Oxford New York: Oxford University Press, 417–335.

———. 2020. “Racism and Responsibility – The Critical Limits of Deepfake Methodology in Security Studies: A Reply to Howell and Richter-Montpetit.” *Security Dialogue* 51(4): 386–94.

Wardman, Jamie K., and Ragnar Löfstedt. 2018. “Anticipating or Accommodating to Public Concern? Risk Amplification and the Politics of Precaution Reexamined.” *Risk Analysis* 38(9): 1802–19.

Wardman, Jamie K., and Gabe Mythen. 2016. “Risk Communication: Against the Gods or against All Odds? Problems and Prospects of Accounting for Black Swans.” *Journal of Risk Research* 19(10): 1220–30.

Warren, Carol A. B. 2012. “Interviewing as Social Interaction.” In *The SAGE Handbook of Interview Research: The Complexity of the Craft*, Thousand Oaks: SAGE Publications, Inc., 129–42.

Weible, Christopher M. 2014. “Introducing the Scope and Focus of Policy Process Research and Theory.” In *Theories of the Policy Process*, eds. Christopher M. Weible and Paul A. Sabatier. Boulder, Colo: Westview Press, 3–21.

———. 2018. “Introduction: The Scope and Focus of Policy Process Research and Theory.” In *Theories of the Policy Process*, eds. Christopher M. Weible and Paul A. Sabatier. New York, NY: Westview Press.

Weible, Christopher M., and Paul A. Sabatier, eds. 2018. *Theories of the Policy Process*. Fourth edition. New York, NY: Westview Press.

Weick, Karl E., Kathleen M. Sutcliffe, and David Obstfeld. 2005. "Organizing and the Process of Sensemaking." *Organization Science* 16(4): 409–21. https://pubsonline.informs.org/doi/abs/10.1287/orsc.1050.0133 (August 3, 2022).

White, Adam. 2015. "The Impact of the Private Security Industry Act 2001." *Security Journal* 28(4).

Wildavsky, Aaron. 2017. "Anticipation Versus Resilience." In *Searching for Safety - Social Theory and Social Policy*, ed. Aaron Wildavsky. Routledge, 85–114.

Wiegmann, Paul Moritz, Henk J. de Vries, and Knut Blind. 2017. "Multi-Mode Standardisation: A Critical Review and a Research Agenda." *Research Policy* 46(8): 1370–86.

Winkel, Georg, and Sina Leipold. 2016. "Demolishing Dikes: Multiple Streams and Policy Discourse Analysis." *Policy Studies Journal* 44(1): 108–29.

Wolcott, Harry F. 2008. *Ethnography: A Way of Seeing*. 2nd ed. Lanham, Md: Altamira Press.

Woodman, Dan, Steven Threadgold, and Alphia Possamai-Inesedy. 2015. "Prophet of a New Modernity: Ulrich Beck's Legacy for Sociology." *Journal of Sociology* 51(4): 1117–31.

Wynne, Brian. 1982. *Rationality and Ritual: The Windscale Inquiry and Nuclear Decisions in Britain*. Chalfont St Giles, Bucks: British Society for the History of Science.

Yanow, Dvora. 2014. "Thinking Interpretively. Philosophical Presuppositions and the Human Sciences." In *Interpretation and Method: Empirical Research Methods and the Interpretive Turn*, eds. Dvora Yanow and Peregrine Schwartz-Shea. Armonk, N.Y: M.E.Sharpe, 5–26.

Yin, Robert K. 2009. 5 *Case Study Research: Design and Methods*. 4th ed. Thousand Oaks, Calif: Sage.

Zahariadis, Nikolaos. 2003. *Ambiguity and Choice in Public Policy: Political Decision Making in Modern Democracies*. Washington, D.C: Georgetown University Press.

———. 2016. "Delphic Oracles: Ambiguity, Institutions, and Multiple Streams." *Policy Sciences* 49(1): 3–12.

Zedner, L., and A. Ashworth. 2019. "The Rise and Restraint of the Preventive State." In *Annual Review of Criminology, Vol 2*, Annual Review of Criminology, eds. J. Petersilia and R. J. Sampson. Palo Alto: Annual Reviews, 429–50.

Zedner, Lucia. 2009. *Security*. London; New York: Routledge.

Zinn, Jens O. 2008. "Risk Society and Reflexive Modernization." In *Social Theories of Risk and Uncertainty*, John Wiley & Sons, Ltd, 18–51.

———. 2016. "'In-between' and Other Reasonable Ways to Deal with Risk and Uncertainty: A Review Article." *Health, Risk & Society* 18(7–8): 348–66.

Zinn, Jens O., and Peter Taylor-Gooby. 2006. "The Challenge of (Managing) New Risks." In *Risk in Social Science*, eds. Jens O. Zinn and Peter Taylor-Gooby. Oxford: Oxford University Press.

Zohlnhöfer, Reimut, Nicole Herweg, and Christian Huß. 2016. "Bringing Formal Political Institutions into the Multiple Streams Framework: An Analytical Proposal for Comparative Policy Analysis AU -

Zohlnhöfer, Reimut." *Journal of Comparative Policy Analysis: Research and Practice* 18(3): 243–56.

Appendix 1 Civil Servant Background

Familiarity and Being/Becoming Estranged

In order to sensitize myself to the strengths and weaknesses of my background, I compared my process to another PhD thesis. Liodden investigated how public servants in Norwegian immigration authorities engage in decision-making about asylum applications (Liodden 2017). We both studied professional judgements by public servants.
When reading Liodden's thesis, the differences stand out – how we perceive both the expectations of and the encounters with public administration. She labels the process of gaining research access *institunoia*, the "slightly paranoid and anxious relationship between a researcher and the institution under research" (2017, 35–36). She describes the process as very difficult.

Throughout the research study, I thought of my familiarity with and knowledge of the public service as being mainly advantageous. Reading Liodden's account, I was further sensitized to how different my expectations and experiences of, and not least my emotions regarding, the process and the system were compared to hers.[56] I realise that my ability to interpret and contextualize made a significant difference. I did not experience the system to be an "impenetrable and powerful" institution (Liodden 2017, 42), but a diversity of matters, such as people who have too much to do, rules that have to be abided by, professional judgements I agree or disagree with, etc. My familiarity had methodological implications, as described in Chapter 6, but it also made the process easier.

Contrary to Liodden's experience, a key stress generator in my case was the academic literature and positioning myself in this literature. Whereas Liodden writes about how her notes were full of stress pertaining to empirical access, my notes, especially in the beginning, are full of reactions to the (critical) literature. Here is a typical reflection early on in the project:

> The articles based on critical security theory seem to be very critical of the entire security management regime – they lack political, social, etc. legitimacy, are based on illegitimate claims of expert knowledge, scientification, securitization, etc. The interpreters [researchers] are finding everything it is possible to think critically of, tipping towards a cartoon version of the subject under investigation, where "ministerial," "expert," etc. are all laden with illegitimacy and critique. On the other

[56] Liodden was dependent on a positive decision from an agency, whereas I had several sources. Our processes are thus only partly comparable.

> hand, the suggestions for solutions – what is lacking, what should be instead – are unclear and, at least in some cases, seem naïve.

My notes are full of complaints about the “thin” empirical basis on which conclusions are drawn, the content of criticisms, and the critical perspective. One example is the research on national risk registers and similar “technologies.” I note that the scholars seem to know, without doubt, that such registers are banal scientifications, acting as if the “incalculable could be calculated.” I objected:

> This does not describe very well what is going on in many processes, e.g., DSB [Directorate for Civil Protection], municipalities. It is a highly negotiated process where professionals are asked to give professionally based judgements, not anything near calculations. As close to Habermas as it is to economics?

Some of the literature I would describe as creating nothing short of shock and disbelief on my part. Neal described the position of Bigo, a key reference in the literature, as follows:

> For Bigo, a field of security professionals has displaced the political arena altogether: it has “discarded some actors, like parliaments … [they are] only a shop front for a competitive and bureaucratic industry of security experts and professionals. […] Analytically and politically, Bigo thus abandons the field of professional politics as already “discarded.” (Neal 2019, 26)

Democracy, in this interpretation, is only a shopwindow for a competitive bureaucratic security industry. Many scholars do not go as far as Bigo. Still, my perception is of an atmosphere of great distrust and skepticism regarding governmental conduct.

Bigo described France and the situation might be different for Norway. Still, it felt dizzying in its implications for democratically founded and legitimate security practice, or alternatively, dizzying in terms of the implications for the academic field I was about to enter. Should I really engage with this literature? And how?

I can summarize the problems I encountered with the literature in three main concerns. One has to do with the confidence with which one “knows” what is critique-worthy and what is not. Since the “critical perspective” stands so firmly and confidently on the good side of the debate, and correspondingly knows who are critique-worthy (security management), it becomes risk-free [sic] to criticize: “lining up” the “suspects and then convicting them with little doubt of critical theory’s authority” (Alvesson and Sköldberg 2018, 355).

Second, there are few nuances regarding *better* or *worse* government. If “management” is always illegitimate neoliberalism that can quickly be discarded, there is not much to talk about. Governmental conduct becomes banal, thus only requiring “thin” descriptions. Viewed from my perspective, governmental conduct is complex, ambiguous, *better* or *worse.* It should therefore be investigated with curiosity and a measure of openness. My frustration resonates with Schwalbe's description of analytical foreclosure, where concepts such as "neoliberal" are substitutes for a thorough analysis and become "a readymade answer, in the form of a Big Concept" (2020, 605).

Lastly, I also struggled with the "critical" alternative. It is fine to be on the side of the oppressed, but then what? In a complex world, some kind of "managing" has to happen. Coming from my background, I often queried for the practical/governing implications of the literature, especially regarding what goes beyond the normative perspectives.

Although I have had a mental "boxing match" with the literature, as the years went by, my reaction subsided. Notably, I have also utilized critical scholars extensively. I cannot fully account for what has happened, but I read the literature somewhat differently. Key was also reading Blumer, as I was given an "instrument" I found very useful, to treat theoretical concepts and theory as sensitizing concepts, rather than exact or eternal "truths" (Blumer 1954). I have thus interpreted the literature as avenues for interpretation, as models or concepts that can sensitize my reading of the empirical material.

I do not agree with many perspectives in the critical literature, but I have at the same time found analysis and theorizing that have enriched my investigation. The scholars that have engaged me have investigated the "deeper meanings" of what interests me. I did not want to reduce the questions in my thesis to functional questions of method, as I do not see them as such. It is mostly critically inclined scholars (in a wide interpretation of the term "critical") who have investigated and theorized such meanings, and whom I have thus engaged with and found useful, at least parts of their writing.

My agenda and perspectives also changed during the process: I have become more critical. This can be seen in, for example, my investigation of the standardization process, which raised concerns on my part, and where I have argued more in line with, and utilized perspectives from, critical investigations of subjects such as polycentric governance.

Summing up the comparison with Liodden, I see a key difference regarding the part of the research process we have become familiar with, and what has felt "alien." We both adopted an outside perspective to becoming familiar – she with the perspectives of the public service, and I with the relevant academic literature.

Reflections on the Roles of Researcher and Civil Servant

In the main text, I concluded that there are no formal limitations on my research because of my civil servant background. However, I am still shaped by the two backgrounds (researcher, civil servant), and will now reflect on the two roles and potential tensions between the two.

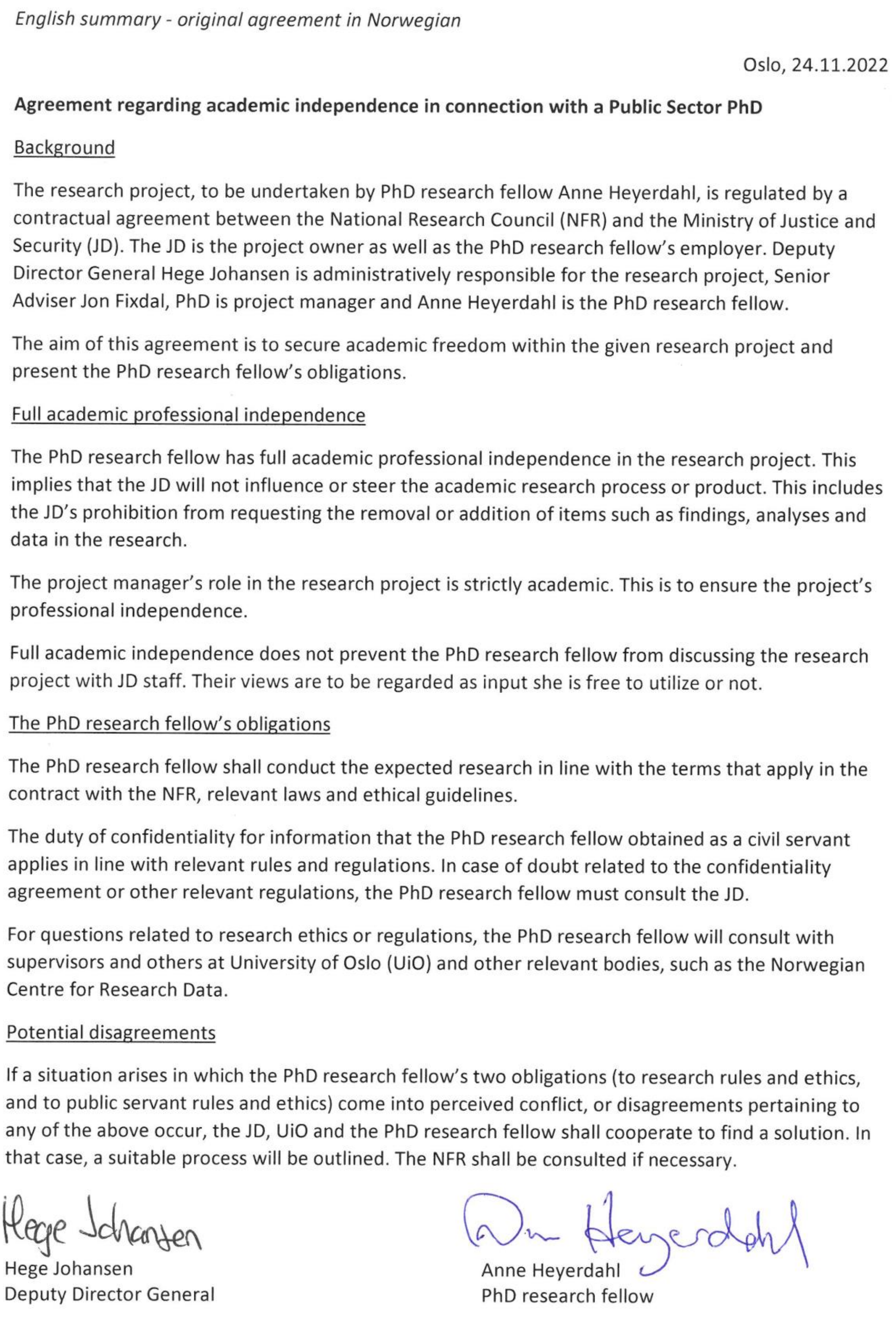
Before I started this project, I was already aware that there had been disagreements pertaining to the standard (NS 5832). I also knew that this controversy had been described as "a religious war'" by one of the interviewees in Busmunrud et al.'s (2015) report. I thought this was mainly a question of professional disagreement, with an element of "turf." As the project went along, however, I realized that the "story" was more conflictual and "unfortunate" from a civil servant perspective. From a research perspective, this is neutral, maybe even positive. To the researcher, what matters is if the findings are interesting and provide new insights. Seen through the lens of the civil service, this looks (or maybe better, feels) different. From a civil servant perspective, the question may arise as to the wisdom of digging into the process. Why display a relatively unimportant, 15-year-old fight between a few people in agencies under the jurisdiction of the MJ? In both the media and in research, there have been descriptions of a conflictual relationship between the police and national security agencies (i.e. Lægreid and Serigstad 2006). Many people within the agencies are working hard both to strengthen cooperation and to change the narrative. Should I, after all employed by MJ, still dig into and display this "old story"? Why? Whose or what interests does this serve?

I must stress that this is not expressed from others but has at times been my own concern. It is not so much my own presentation that concerns me, but that it could be twisted into something else by others. I state this in the honour of reflexivity, not as a prediction. For media, conflict inside the civil service tends to be a scoop. One inclination, given my background, could have been not to focus on the conflict at all, to not give any ground for attention I do not want.

Manoeuvring through the empirical study has made me feel the tension between my reflexes as a civil servant and as a researcher at different points in time, such as when choosing what data to include and exclude or determining the level of analysis. For instance, some interviewees referred to the governmental project (first phase) as having been labelled "the suicide project" in one of the agencies. Should I use this term? What about the statement in which it is likened to "a religious war"? A civil servant reflex would be to not directly cite such expressions but write "around them." I first thought it unnecessary to feature these statements. The process should be described as "dry" as possible, I thought. After some consideration, however, I realized that given the RQ and MSA theory, these statements were dense expressions of value. Should I still exclude them? If I did, was this out of an underlying concern for how they could be potentially misused by others? When I realised that the citations would help answer the RQ, I could not, of course, leave them out. My obligation is now that of doing sound research. Perhaps a bit melodramatic, it is a point of no return. I must act based on my research considerations alone.

I have ceased – or aimed to cease – asking questions such as "is there something potentially controversial I am putting on display?" It is impossible to do research with this controller mindset and I have told myself to stop. As the years have gone by, I have found it easier to let my concerns fade away and concentrate on the research process itself.

Appendix 2 Agreement Academic Independence



English summary - original agreement in Norwegian

Oslo, 24.11.2022

Agreement regarding academic independence in connection with a Public Sector PhD

Background

The research project, to be undertaken by PhD research fellow Anne Heyerdahl, is regulated by a contractual agreement between the National Research Council (NFR) and the Ministry of Justice and Security (JD). The JD is the project owner as well as the PhD research fellow's employer. Deputy Director General Hege Johansen is administratively responsible for the research project, Senior Adviser Jon Fixdal, PhD is project manager and Anne Heyerdahl is the PhD research fellow.

The aim of this agreement is to secure academic freedom within the given research project and present the PhD research fellow's obligations.

Full academic professional independence

The PhD research fellow has full academic professional independence in the research project. This implies that the JD will not influence or steer the academic research process or product. This includes the JD's prohibition from requesting the removal or addition of items such as findings, analyses and data in the research.

The project manager's role in the research project is strictly academic. This is to ensure the project's professional independence.

Full academic independence does not prevent the PhD research fellow from discussing the research project with JD staff. Their views are to be regarded as input she is free to utilize or not.

The PhD research fellow's obligations

The PhD research fellow shall conduct the expected research in line with the terms that apply in the contract with the NFR, relevant laws and ethical guidelines.

The duty of confidentiality for information that the PhD research fellow obtained as a civil servant applies in line with relevant rules and regulations. In case of doubt related to the confidentiality agreement or other relevant regulations, the PhD research fellow must consult the JD.

For questions related to research ethics or regulations, the PhD research fellow will consult with supervisors and others at University of Oslo (UiO) and other relevant bodies, such as the Norwegian Centre for Research Data.

Potential disagreements

If a situation arises in which the PhD research fellow's two obligations (to research rules and ethics, and to public servant rules and ethics) come into perceived conflict, or disagreements pertaining to any of the above occur, the JD, UiO and the PhD research fellow shall cooperate to find a solution. In that case, a suitable process will be outlined. The NFR shall be consulted if necessary.

Hege Johansen
Hege Johansen
Deputy Director General

Anne Heyerdahl
Anne Heyerdahl
PhD research fellow

Appendix 3 Interview Request

Vil du delta i forskningsprosjektet

" Utvikling og bruk av ny standard for risikoanalyse for tilsiktede uønskede handlinger"?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt om utvikling og bruk av en standard for risikoanalyse for tilsiktede uønskede handlinger (NS 5832:14). I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Formålet med prosjektet er å belyse hvordan risikostyringen i Norge har utviklet seg de senere årene knyttet til tilsiktede uønskede handlinger, inkludert betydningen av at det er utviklet en norsk standard på området (NS 5832). Det er videre et mål å vurdere om valg av tilnærming til risikoanalyse påvirker vurderingen av risiko og risikoanalyse, og i tilfelle på hvilken måte.

Hvem er ansvarlig for forskningsprosjektet?
Forskningsprosjektet er et doktorgradsprosjekt som er finansiert av Norges Forskningsråd og Justis- og beredskapsdepartementet gjennom Offentlig sektor PhD-ordningen: Forside - OFFPHD

Hvorfor får du spørsmål om å delta?
Du blir spurt om å delta i form av et intervju på grunn av din kunnskap til, eller erfaring med, spørsmålene som reises i prosjektet.

Hva innebærer det for deg å delta?
Prosjektet er et kvalitativt forskningsprosjekt som i hovedsak baserer seg på dokumentanalyse og intervju. De fleste som deltar i prosjektet vil bli intervjuet en gang. For noen få kan det bli aktuelt med oppfølgende intervju.

Intervjuene vil bli tatt opp på en båndopptaker med mindre noe annet avtales. Lydfiler og eventuelt notater fra intervju blir lagret i tråd med Universitetet i Oslos lagringsguide for fortrolige dokumenter, og i tråd med godkjenning fra Norsk senter for forskningsdata. Alle intervjudata vil bli anonymisert, med mindre annet er avtalt. Ikke-anonymisert bruk av data vil kun være aktuelt i tilfeller der personen vil være gjenkjennbar ut fra rolle eller kontekst. Der gjenkjenning er mulig, vil sitater eller annen informasjon som baserer seg på intervjuet, bli forelagt deg for godkjenning på forhånd.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil da bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Samtykke
For at du skal inkluderes i forskningsprosjektet må du gi samtykke til dette. Samtykke gis gjennom at du avtaler å delta på intervju og bekrefter ønske om deltagelse innledningsvis i intervjuet mens båndopptaker er på. Hvis intervjuet gjennomføres uten båndopptaker, må skriftlig samtykke gis innledningsvis under intervjuet.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Opplysningene om deg vil bare bli brukt til formålene beskrevet i dette skrivet. Opplysningene vil bli behandlet konfidensielt og i samsvar med personvernregelverket. Det er kun stipendiat Anne Heyerdahl som vil ha tilgang til lydfiler og annen informasjon som gjør det mulig å identifisere intervjuobjektene. Navn og kontaktopplysningene dine vil bli erstattet med en kode som lagres på egen navneliste adskilt fra øvrige data.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes sommeren 2021. Når prosjektet er avsluttet blir datamaterialet anonymisert (alt som kan identifisere intervjuobjekter slettes). Anonymiserte data vil bli lagret videre under samme eller tilsvarende sikkerhet som skissert i dette skrivet for videre forskning og dataene vil derfor bli lagret på ubestemt tid.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Oslo har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Institutt for sosiologi og samfunnsgeografi, Universitetet i Oslo ved stipendiat Anne Heyerdahl anne.heyerdahl@sosgeo.uio.no eller telefon: 991 60 461.
- Universitetet i Oslos personvernombud: Maren Magnus Voll personvernombud@uio.no
- NSD – Norsk senter for forskningsdata AS, på personvernombudet@nsd.no eller telefon: 55 58 21 17.

Med vennlig hilsen

Anne Heyerdahl
Stipendiat ved Institutt for sosiologi og samfunnsgeografi
Universitetet i Oslo
anne.heyerdahl@sosgeo.uio.no
+47 99 16 04 61

Appendix 4 Example of an Interview Guide

Bakgrunn

Kort om deg selv – Hva er bakgrunnen din (utdanning, erfaring)? Hva jobber du med nå?

Utvikling av security og sikring i Norge

Det har skjedd mye på security-feltet og med sikring som fag og praksis de siste 10-20 årene.

- Hvordan vil du beskrive utviklingen, sett fra ditt ståsted?
- Hvem og hva har ledet an i utviklingen?
- Hvor er vi nå, og hvor er vi på vei?

Risikoanalyser på securityområdet – historisk utvikling

- Kan du beskrive den historiske utviklingen av risikoanalyse og risikostyring innenfor forebyggende sikkerhet/security?
- Kan du beskrive utviklingen av trefaktormodellen?

Utviklingen av terrorveiledning/standardiseringsprosessen

- Kan du beskrive prosessen (den delen du deltok i eller observerte)?
  - Terrorveilederen
  - Utviklingen av SN 5832
  - Diskusjonen etter at standarden ble gitt ut

Trefaktormodellen

- Hvorfor ble en egen tilnærming til risikoanalyse på sikkerhetsområdet utviklet?
- Skiller den seg fra andre tilnærminger, og i så tilfelle, på hvilken måte?
- Hva er bra/dårlig? Hvorfor?
- *Hvis aktuelt: Sannsynlighet*
  - *betydning – hvorfor ta det ut eller ikke ta det ut?*
  - *hvorfor ble sannsynlighet viktig i diskusjonen?*
- Hvor står debatten om tilnærmingen i dag?
- Hvordan er den norske utviklingen sammenliknet med andre land?

Standardisering

- Hva er dine erfaringer med standardiseringsarbeid?
- Hvordan ser du på standarder og standardisering?
  - Hva *er* egentlig en standard?
  - Hvordan vil du sammenlikne standarder med veiledere eller regulering fra det offentlige?
  - *Hvis aktuelt: Hva er eventuelle suksesskriterier eller fallgruver i standardisering?*
- Hvilken betydning har standardisering hatt innen risikostyring og forebyggende sikkerhet?
- Hvordan er bruken av 5832 i dag? Hvor stort gjennomslag vil du si standarden har hatt?

Noe jeg burde ha spurt om? Noe du ønsker å tilføye?

Appendix 5 Examples of Node Trees

Example 1 – the standardization process

- First phase (terrorism protection guideline)
    - What happened – for process tracing
    - MSA
        - Problem stream
        - Policy stream
            - Ideational arguments
            - Professional arguments
            - Reference to a specific policy (3FA, ISO standard etc)
        - Politics stream
            - Turf
            - Change of key personnel
            - Use of veto point/power
        - Human agency
            - Policy Entrepreneurs
            - Something else than PE
        - Windows of opportunity
    - Institutional factors
        - Rules and formal things
        - Knowledge, education etc
    - Does not fit MSA
    - Noteworthy

Example 2: Coding risk management

- Probability
    - Arguments for using probability
    - Arguments against using probability
    - Precaution
        - possibility
    - Frequency based versus subjective/intersubjective
    - 3FA and probability
    - Other approaches (SN 5814, ISO etc)
    - The risk matrix
    - Uncertainty and black swans
    - Communication of
    - Misunderstandings, strawmen etc
- Responsibility
    - For creating security
    - For analysis
    - Normative arguments and duty
    - Blame-game
    - Experience with
        - Grubbegata
            - *Continues with in vivo codes such as ‘When it goes wrong, they are rig*

I

II

Journal of Risk Research

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rjrr20

Risk assessment without the risk? A controversy about security and risk in Norway

Anne Heyerdahl

To cite this article: Anne Heyerdahl (2022) Risk assessment without the risk? A controversy about security and risk in Norway, Journal of Risk Research, 25:2, 252-267, DOI: 10.1080/13669877.2021.1936610

To link to this article: https://doi.org/10.1080/13669877.2021.1936610

JOURNAL OF RISK RESEARCH
2022, VOL. 25, NO. 2, 252–267
https://doi.org/10.1080/13669877.2021.1936610

OPEN ACCESS

Risk assessment without the risk? A controversy about security and risk in Norway

Anne Heyerdahl

Department of Sociology and Human Geography, University of Oslo, Oslo, Norway

ABSTRACT

Security and 'securing' is high on the public agenda. Questions are raised on where, to what degree and against what the government and others should introduce preventive security measures. This article investigates a controversy in Norway about the role of probability in risk assessment within security. The article asks how the question of the probability of incidents is problematized and addressed by actors involved. It discusses how the controversy can be interpreted and what it might tell us about security and risk. The article builds on an exploratory study of the reasoning of security professionals in relation to a standard on security risk assessment. It shows how the downplaying of probability is defended, but also how it creates dilemmas and is criticized. The argument against estimating probability is that it is often difficult or impossible. Probability is, however, also a moderating factor. Probability turns unlikely futures into lower risks than likely futures. Those arguing against the security risk standard point to the consequence of downplaying probability in risk estimates. A key finding is how risk assessment in areas of low tolerance for incidents introduces a discrepancy that is difficult to handle. On the one hand, security analysts are supposed to deal with threats as risks, implying scaling, comparison and level of acceptance. On the other hand, they are supposed to create security, implying the opposite of scaling and risk acceptance. Risk assessment becomes difficult if there is little appetite for taking risk. Michael Power's three ideal models of risk management logics are introduced in the discussion as heuristic tools of a sensitizing kind. The article concludes that risk research could benefit from engaging with security theory, to investigate how risk management might be shaped by security practises.

ARTICLE HISTORY
Received 8 January 2021
Accepted 4 May 2021

KEYWORDS
Risk assessment; security; probability; precaution; sociology of risk

Introduction

Security and 'securing' have appeared high on the public agenda in recent decades and national security is not only a topic for the international arena, it is also to be created domestically. Preventive security measures range from barriers such as surveillance systems and critical infrastructure protection, to fostering security cultures and individual responsibility.

Creating (national) security has for some time been interwoven with and managed trough tools and perspectives from risk and risk management (Vedby Rasmussen 2006; Aradau and Van

CONTACT Anne Heyerdahl anne.heyerdahl@sosgeo.uio.no Department of Sociology and Human Geography, University of Oslo, Oslo, Norway.
This article has been republished with minor changes. These changes do not impact the academic content of the article.

Munster 2007; Petersen 2012; Heng 2018). This article aims at investigating the intersection of security and risk management practices, and how a seemingly methodological question within a security risk standard also has more fundamental and normative implications. In 2014, Standard Norway issued a standard for security risk assessment pertaining to when the risk stems from harmful, malicious acts (Standards Norway 2014).[1] During and primarily after the standardization, a controversy arose between risk- and security experts and civil servants on the usefulness of the approach (Maal, Busmundrud, and Endregard 2016; Amundrud et al. 2017; Jore 2020).[2] The security risk approach presented in the standard represents a critique of an existing standard (Standards Norway 2008). This approach is referred to as the 'two factor approach' (2FA) in the debate, since risk is defined as a combination of *probability* and *consequence*. In the new security risk standard, risk is defined without an explicit reference to probability. Risk is 'an expression of the relationship between the *threat* against a certain *value* [asset] and this value's *vulnerability*.' (Standards Norway 2014, 5).[3] This approach has been labelled the 'three factor approach' (3FA) in the debate, building on the three dimensions.

A defining characteristic of the 3FA is that it does not have an explicit reference to probability or likelihood.[4] Judgments of probability are traditionally at the heart of the very idea of risk (Hacking 1990). A key element of the controversy was related to the role of probability in risk assessments, and the potential consequences of including or not including probability judgements. Accordingly, the present article asks: how is the question of the probability of incidents problematized and addressed by actors involved in the controversy over the standard on security risk assessment? The article also discusses how the controversy on probability can be interpreted, and what it might tell us about security and risk, and the relationship between the two.

Securing as high politics

The controversy investigated unfolded in the aftermath of a terrorist attack in Norway in July 2011. A right-wing terrorist killed eight people in a bomb attack at a governmental building accommodating the Prime Minister's office and the Ministry of Justice and Public Security. He then killed 69 young people at a political youth party camp in a shooting massacre. The attack shook Norwegian society in several ways. A key question raised, of relevance to this article, was the lack of preventive measures that made it possible, and relatively easy, to attack the governmental buildings. Questions were raised about the government's ability to plan and implement sufficient security measures. Security planning, and 'acknowledging risks', became an acute problem that needed solving. Investigations, audits, parliamentary hearings and a new security law are indications that security and 'securing' have become high politics in Norway.

The controversy investigated takes place within a Nordic societal security context (Larsson and Rhinard 2020), but similar debates on probability's role in security risk assessment has taken place in other countries (Klima, Dorn, and Vander Beken 2011; Mueller and Stewart 2014) and in research on risk and security (Manunta 2002; Ezell et al. 2010; Aven and Guikema 2015; Amundrud et al. 2017).

The article presents an empirical investigation of professionals reasoning on questions that have been extensively debated in risk research for a long time, such as what risk is, how to best present risk, and the link to risk management and decision making (Aven 2020; Klinke and Renn 2002; Zinn 2008). Although the meaning of risk in a security context has been debated, few scholars have looked into how those engaged in security risk management actually reason about risk in a security context. Consequently, this article investigates the actors' understandings of risk and security in a social context. This has been far less studied. One possible explanation for the altogether low number of empirical studies is that security cultures are understood as 'extremely difficult to penetrate or to participate in' (Salter and Mutlu 2018, 7; Pouliot 2008), making empirical investigations difficult. The present article attempts to be an exception, and builds on unique, qualitative data on how security and risk professionals in Norway reason on probability's role in security risk assessment.

The article shows how the professionals deal with a perceived tension between risk and security. A key finding is how risk assessment in areas of low tolerance for incidents introduces a discrepancy that is difficult to handle. On the one hand, security analysts are supposed to deal with threats as risks, implying scaling, comparison and level of acceptance. On the other hand, they are supposed to create security, implying the opposite of scaling and risk acceptance. Probability is downplayed, it is argued, because probability 'makes' risks relative. This is not in line with the idea of creating security, where there is little room for something to go wrong.

The article starts with a brief presentation of two relevant research traditions dealing with the risk-security nexus. It then introduces data and method, before it presents the empirical investigation on how security professionals reason on probability. The empirical part starts with a citation, showing the difference between reasoning in line with 2FA and 3FA and how the interviewee clearly preferred the latter. Secondly, the empirical section displays arguments used against probability and perceived implications for the estimated risk level. It then looks at the tension between risk and security, and reasoning on scaling and comparing risks. The final empirical part looks at how the interviewees reason on the burden of hindsight judgements, and how this influences their judgements of risk assessment. In the final discussion of the article, a perspective from research on risk management is utilized. Michael Power's three ideal models of risk management logics are shortly introduced; risk management as *anticipation*, *resilience* or *auditability* (2014; 2007). The three ideal models have not been subject to much investigation but are regarded as useful, heuristic tools of a sensitizing kind (Bowen 2006; Swedberg 2018). By including Power's theory, the article also aims at inspiring cross-disciplinary fertilization in the intersection between risk-, security- and management research.

The risk-security nexus

The meaning of 'risk' and 'security' is context dependent (Ciută 2009), complex (Boholm, Möller, and Hansson 2016), and builds on different traditions both within academia (Petersen 2012; Aradau 2016; Battistelli and Galantino 2019) and among practitioners. In this article, the meanings of the terms are part of the empirical investigation, but for a rough clarification, 'security' is linked to malicious acts (Jore 2019b), 'risk' to the idea of anticipating or 'managing' the future.

For the purpose of this article, two research areas on risk and security should be noted. First, within risk and safety research, the increased attention to security risks has spurred discussions of similarities and differences between the fields of 'safety' and 'security' (Pettersen et al. 2015; Høyland 2018; Jore 2019b; Bieder and Pettersen Gould 2020). Risk and risk assessment are viewed as something the two fields have in common, the question being if risk tools and models developed within safety research can be used also for analysing security risks (Abrahamsen et al. 2017; Boustras and Waring 2020), or if they are in need of a separate 'security science' (Smith and Brooks 2012). The perceived unpredictability of security risks links the discussions to wider topics within risk research such as how to deal with uncertainty and the precautionary principle (Sunstein 2005; Paté Cornell 2012; Wardman and Löfstedt 2018). One debate has been on the limits to risk assessment; where unknowns are reduced to measurable 'risks', trying to create a level of predictability which might be counterproductive (Stirling 2010; Taleb 2010). Another path is to see uncertainties not as a contrast to risk, but as a key dimension of it (Pettersen 2016). Probability is in this perspective an instrument adopted to represent or express uncertainty, where the degree to which it is a suitable tool can be questioned (Aven 2020). A key debate of relevance to this article is the distinction between frequentist and subjective interpretations of probability. Frequentist approaches allow estimates of probability based on historical data, and is thus limited to questions where available samples are sufficient (Van Coile 2016).

Subjective probabilities reflect a degree of belief or a measure of confidence, allowing incorporation of all available evidence in the probability assessment (Aven 2020). A key question has thus been if risk assessments only can rely on 'objective' knowledge, or if it should – and has to – include subjective judgements; that is, it is dependent on the knowledge of the assessor (Aven 2020). In a security context, uncertainties are viewed as especially challenging pertaining to certain phenomena (i.e. terrorism). It includes not only lack of knowledge of the phenomena (epistemic uncertainties), but ambivalences as to the phenomena itself and trade-offs, such as the tolerability of the measures taken to reduce the risk (Abrahamsen et al. 2017; Jore 2019a) .

Secondly, a somewhat different debate has taken place within international relations, critical security studies and criminology, especially in the aftermath of 9/11 and the 'war on terror'. Here, risk – not safety – is investigated in contrast to security (Aradau and Van Munster 2007; Mythen and Walklate 2008; Petersen 2012). Building on sociological theories, risk is linked to economic and scientific anticipations of potential futures, weighing benefits against costs (Petersen 2012; Mythen 2018). Security, on the other hand, is understood as a matter of survival (Buzan, Wilde, and Waever 1998). Contrary to risk, where costs can be weighed against benefits, security implies a core value that cannot be compromised (Søby Kristensen 2008). The distinction between risk and security 'cannot be so quickly collapsed' (Aradau 2016, 291),[5] when viewed from a security perspective. The literature resonates with suggestions that an analytical distinction between risks and threats can contribute to more nuanced interpretations (Battistelli and Galantino 2019).

In both the risk and security literature, a low risk acceptance and a growing lack of confidence in the ability to predict or estimate the future has been investigated, leading to precautionary approaches (Furedi 2009; Wardman and Mythen 2016; Ansell and Baur 2018), feelings of anxiety and a search for security (Wardman and Lofstedt 2020). Instead of reasoning based on knowledge and probability, questions of what could possibly happen are raised, opening up for actions based on speculations and 'worst case' thinking (Stern and Wiener 2006; Mythen and Walklate 2008; Amoore 2013). This 'crisis of causality' has notable consequences for our approach to risk, Furedi argues: 'Of course once risk is detached from probabilities it ceases to be a risk' (2009, 205). If the calculation of relative likelihood cannot be used as a basis of decision-making, the key rationale for action becomes the potentially disastrous impact (McInnes and Roemer-Mahler 2017). Linked to this is a concern of what comes instead of probabilities. Without 'the "decision-analytic" rigour conferred by risk-based thinking' (Wardman and Mythen 2016, 1226), possibilistic reasoning and the question of 'what if?' might become a prevailing logic (Mythen and Walklate 2008; Amoore 2013). Another much studied response to the perceived unpredictability of risks is the idea of building resilience (Dunn Cavelty, Kaufmann, and Søby Kristensen 2015). Resilience 'moves' attention from external threats to the organization's ability to respond (Aradau 2014).

Within critical security studies, the introduction of risk in the security domain has been interpreted as widening and deepening a problematic securitization[6] process (Aradau and Van Munster 2007; Amoore 2013). The case investigated in this article suggest however that, seen from a risk perspective, the argument could be turned around. The quest for security can influence the framing of risk judgements (Battistelli and Galantino 2019). The utopian character of security, the idea that 'some things should be secured no matter what', is at odds with the 'riskiness' of risk. It is thus important, also from a risk research perspective, to investigate how attempts to create security through risk and risk management might influence understandings and practices also of risk management.

Method and data sources

The present article builds on an exploratory study using a mixture of interviews, written material and fieldwork. It builds on 28 interviews, 19 conducted by the present author in 2018-2020 and nine conducted in 2014 by Busmundrud et al. (2015), in both cases with security professionals

Table 1. Interviewees – key characteristics.

Interviews and institutions	Abbreviation	Educational background	Role[a]	Gender
Ministries: 8	M1 – M8	9 social science	12 civil servants	17 male
Agencies/governmental institutions: 14	A1 – A8, C1, C2, C4 – C6, C8	5 technical/engineering	5 consultants/ private sector	7 female
Private sector: 6	P1 – P3, C3, C7, C9	4 military/security	5 leadership	
		3 police	3 researchers	
		2 law		
		1 humanities		

[a]One of those interviewed twice changed role between interviews.

and civil servants. Four people are interviewed both by Busmundrud et al and the author, making the number of interviewees 24; coming from 16 different organizations. Verified interview summaries are included as an appendix to Busmundrud et al, labelled C1 – C9.[7] The interviews conducted by the author have been anonymized, as the interviewees do not speak on behalf of their organizations and to encourage an open dialogue. Three interviewees are academic scholars, the rest work with risk assessment policy (public or as standards) and/or conduct risk assessments. Most interviewees do not have an academic education in risk studies (Table 1).

Interviewees were chosen through a combination of strategic and snowball sampling. The intention of the sampling was to gain insights into the questions raised and to elicit multiple perspectives. The interviewees are influential or well positioned advisors, either in terms of the controversy itself or relevant policy developments. The author has also conducted fieldwork at four courses for practitioners of risk assessment and security planning.[8] Written material, such as standards, guidelines, reports and administrative documents, has also been analysed.

The present article builds on an inductive and exploratory study. The material has been analytically coded (Charmaz 2017) in nodes developed from the material (examples of nodes are 'uncertainty', 'possibility', 'security is special'). The reading has attempted to be sensitive to a potential representational bias. That is, interviews represent what agents say, their conscious deliberations. What might be as important, is the tacit, often not articulated knowledge; the know-how and perspectives the agents 'think from' (Pouliot 2008). Careful interviewing and coding practise is necessary to take both the representation, as well as the potential representational bias, into account. Of importance in this respect is that the author has a background of nearly 20 years as a civil servant in Norway, and thus possesses extensive knowledge about the institutional frameworks of and cultural codes within the Norwegian civil service. Arguably, this has resulted in high degrees of trust and openness from the interviewees, with the potential for unique insights. It diminishes the usual challenge of attaining experience-near knowledge. It might however instead result in a lack of sufficient distance to observe meanings. In an attempt to create transparency, the present article prioritizes empirical quotes from interviews to invite the reader to challenge the author's interpretations.

Security risk Assessment - Risk assessment without probability?

To introduce the controversy on probability, it may be helpful to look at an experience referred to by one of the interviewees, when (s)he worked for a government agency:

> P2: [Our] head was on a fixed-term contract. I came up with a proposal to invest several hundred million kroner over a period of time on security measures. This would extend beyond his tenure as head of the institution … We ended up with a [probability] estimate that this could happen every seventieth year.
>
> 'Why would I invest in this when I have all these projects "screaming" [for attention] and needing doing?' [the head said]. I realized I had a problem …
>
> In order to create an understanding … I asked him: 'Are these your institution's values?' 'Yes,' he agreed … Then we carried out an analysis of the threats, where we found the actors' modus operandi, and

> then we looked at the vulnerabilities. We asked: '…do we have a real chance of defending ourselves against the aggressors, if they decide to attack us? The crucial point being - if *they* decide to attack… ?'
>
> I had to turn the question round for him: 'You are not the one deciding anything here…What we have uncovered is that, if the aggressor decides to attack us, we will not be able to oppose that attack. Can you live with the fact that *he* is the one making a decision here, not you?' Then *everything* changed.
>
> This was the first time I had presented a risk picture without saying anything about probability. I did not need probability. I got my message through. Then I started to think: probability - does it create more problems than it solves?'

The quote above describes two different ways of communicating risk, corresponding to the two competing approaches of the controversy, 2FA and 3FA, with the interviewee arguing for the latter. In the first version (2FA), the key argument refers to probability, that scenario X could happen every seventieth year. Mathematically speaking, the probability of X happening in any given year is, all else being equal, 1/70 = 1.4%. The probability of X not happening is, correspondingly, 69/70 = 98.6%. In other words, the probability that X will happen is much lower than the opposite at any one point in time.

Exactly how the head understood 'every seventieth year' is difficult to say. It might be understood as 'many years from now', as '70 years from now' or in line with the mathematical expression. In all cases, the probability of X happening while the head was still in office is relatively low. P2 explains the first decision not to invest in security measures in terms of the short-term tenure of the head's position.

It is noteworthy how the risk is first linked to a threat assessment, which by definition is an assessment of something external to yourself; it is the potential attacker, not you, who decides whether to attack or not. Uncertainty is imminent in such a situation; a threat is, at least within a civil organization, close to 'destiny' - an attack might happen and it might not. In the second line of reasoning (3FA), the head is asked whether he wants the enemy to be 'in charge' or if he wants to be 'in charge' of the destiny of the organization himself. It is no longer the threat actor who is seen as responsible if something happens - it is the head. If the enemy attacks, it is because he allows this to take place.

It is also noteworthy that the perception of the risk related to temporality is developed differently in the two descriptions in the quote above. The risk according to the first line of reasoning is not especially large or pressing, since 70 years is a long time period and a probability of 1.4% is intuitively not that high. According to the second line of reasoning, however, the risk is described in a way that makes it a pressing problem. As the enemy can attack whenever 'he' wants, the risk is an urgent one. Insecurity is linked to urgency in a way risk within traditional risk management regimes is not.

Arguments against probability

The main argument in favour of the 3FA is related to probability and the fact that probability is not an explicit part of the expression of risk (Busmundrud et al. 2015). By most proponents of 3FA, probability is understood as numerical, based on frequency, and probability can be calculated only if 'we have statistics' (A2). 'If you take probability into account, we often do not need any preparedness at all. Because probability is often estimated based on historical numbers and a lot of what we are working with has never happened' (M2). Probability builds on historical data, it is argued, and historical data are often lacking (A2,A6,M2) or are irrelevant, because the enemy is strategic and unpredictable.

Some have expressed a general warning against using 'numbers': 'Rely on sensible judgements, be careful with numbers and indexes…'.[9] Some suggest that it is dangerous to present probabilities because they are easily misunderstood as more precise and scientific than is actually the case (A2,P1,C4). Qualitative estimates of probabilities are also problematic (C8,A6,P3). When asked, for example, whether it would be reasonable to describe the probability of a shooting at a Norwegian school as i.e. 'low', P3 responded that such an approach would be 'too mechanical'.

A number of interviewees described it as almost meaningless to estimate the probability of an attack and expressed relief that 3FA had 'pierced probability' (A6) so they themselves did not have to.[10] Behind much of the reasoning against probability lies what is regarded as an inevitable lack of knowledge and an inescapable uncertainty. Using probability depends on certain qualities of the information on which the estimate is based, and if these qualities are lacking, it is argued, probability cannot be estimated in a meaningful way (P3,A6,C9).

The proponents of 3FA are critical of the idea of estimating probability. This is not, however, an argument against estimating risk; it is an argument for a certain *way* of estimating risk, where probability plays a less prominent role.

Probability influences the level of risk

Implicit in much of the criticism of 3FA is an assumption, that when probability becomes less important, the risk will be estimated as being higher (A4,M6,M7). If probability is not part of the reasoning, the risk is judged primarily by its consequence. Probability is in other words a moderating factor, especially for risks with presumably low probabilities.[11]

Some of the interviewees argue that the reason for using 3FA as an approach is precisely because of the effect of security risks becoming 'higher', and thus more important, through a 3FA. This is regarded by some as legitimate (M8,A2) because security risks are seen as special (M8) and need more attention and investment:

> A2: … when you … have quite serious actions … with the great potential for damage, but you have so few of them that I would say it is impossible to calculate the probability.
>
> I: … one could say that the probability is then low?
>
> A2: Well, that is exactly what it ends up being … the probability will end up being low … and then you do not get the right answer, I think. Then we end up never protecting ourselves against these types of actions … .This is what 22/7 [2011 terrorist attack] showed … . It had a great potential for damage, but one chose not to do anything. Because the probability was too low.

The first line of argument is that there is a lack of historical cases to calculate frequency. When asked whether this could be interpreted as 'low probability', the interviewee does not contradict this in itself. The implication of 'low probability' is, however, regarded as unacceptable. One does not get the 'right answer', meaning necessary investments in security measures.

The fact that security risks tend to 'become' higher through a 3FA is not seen only as an advantage by those favouring the approach. Two government institutions that have implemented risk assessment tools building on the 3FA have struggled with the data tool producing higher risk estimates than they feel comfortable with (A3, fieldnotes). In one case, this was solved through the last step of the assessment, where risk analysts can manually adjust the risk, where probability and other factors can be taken into account. The analysts are encouraged to 'dare' to reduce the risk, if the risk intuitively seems too high, as stated by the data tool (A3). A3 regards implementing this manual adjustment as a challenge, but sometimes it is necessary, because high risks involve using too many resources on reducing a risk that is assessed as too high. A6 expresses a similar concern:

> A6: We have had some analyses where I thought that some of the risks were too high and … not especially likely … I wish I had a finger in the pie when it came to the scenarios used.
>
> I: It is during the scenarios you do something about it?
>
> A6: Yes, you do not make scenarios for things you think you shouldn't work on … not everything is something you want to entwine yourself into …

> I: You think it’s better to just drop the scenario?
>
> A6: Yes. If it is impossible for us to introduce measures against it, why should you analyse it?… nuclear bomb… espionage, electromagnetic…. We don’t have a chance to secure ourselves against it, so why would we bother?

A6 thus thinks that some of the risks in their analyses end up at a level (s)he perceives as too high because the probability of the scenario is low. For A6, the answer to this is not to include probability but to choose the right scenarios for the risk assessment. To A6, the criterion for choosing a scenario becomes a combination of excluding very low probability scenarios and using a pragmatic argument; there is no point in analysing scenarios if the organization in question has no chance of dealing with them anyway.

What is described is often, de facto, a dualistic form of probability. If a scenario is part of the planning premise, the threat is ‘assumed’ (i.e. the probability of the scenario is treated, de facto, as 100%, at least initially). If the scenario is not planned for, it is ‘dropped’ as a planning premise (probability is treated, de facto, as 0%). A key part of being professional is advising against including scenarios that have a probability that is too low, since scenarios that are included will be consequential (P1).

To sum up, if probability is given less weight, higher priority will be given to low-probability risks. Some interviewees regard this as positive, because security risks are often low probability risks that will not be allocated the attention and investment seen as necessary to prevent them. However, risk becoming high is also regarded as a challenge and is dealt with, for example, by reducing the number of scenarios used; in reality, this introduces the dualistic probability of either/or.

The tension between risk and security

Strategies such as being highly selective about scenarios are clearly difficult in a security domain. Security professionals are encouraged to ‘think the unthinkable’ and ask ‘what if? (NSM, PST, and POD 2015). Many prefer to use the term ‘possibility’ instead of probability (A1,P3,C4,C8) which draws attention to possible scenarios, not likely ones. The enemy is a rational agent and if something is possible, the enemy may find this weakness and misuse it. The notion of ‘testing’ security measures points in the direction of ‘possible’. Can the security measures withstand all possible, ‘thinkable’ attacks? Defence in Depth security (Reason, 1997), where several barriers are supposed to be built, is a key strategy when security measures are chosen. This is at odds with the idea that one can be selective when it comes to security measures. Defence in Depth and the idea of ignoring low probability scenarios are not easily aligned.

Fieldwork, most notably at the course on preventive security, shed light on this tension between risk and security. At the course, a risk-based approach to security measures was promoted, indicating both an analytical approach and choices about what the extent of securing should be. Many lectures were, however, directed towards details and being alert (‘entrance cards should be displayed at all times’). One participant expressed frustration during a break; (s)he did not understand how to bridge the gap between a risk-based approach and the specific security measures. Risk was too abstract, security measures too concrete. Risk indicates choices, Defence in Depth security indicates necessities.

Within this context, it may be helpful to present the definition of the concept of security in the 3FA, in line with a classical definition of security: ‘security is a real or perceived state of affairs, which implies the absence of unwanted incidences, fear or danger.’ (Standards Norway 2012). Security implies in this definition a state of affairs without trade-offs. It represents a ‘stable’ situation, which is either secure or not; ‘a bit secure’ or degrees of security seem impossible (C1). This utopian idea of security as an absence of unwanted incidences is at odds with risk as a concept linked to scaling, choice and levels of acceptance.

To sum up, there is a tension between risk and security in the case at hand. On a practical level, a key strategy is to be selective and not use scenarios of especially low probability. The vulnerability of this strategy is exposed, however, if what can possibly happen is supposed to be investigated simultaneously. The framework of Defence in Depth indicates that low probability incidents are also important. One is supposed to be selective (scenarios) and not selective (Defence in Depth) at the same time.

Scaling and comparing risks

Let us return to risk assessment and one of its key purposes, namely the scaling and comparing of risk. The focus of many of the security professionals in favour of the 3FA is that of creating security, implying going deeply into understanding each risk separately and judging whether additional security measures are needed. Probability is seen as a tool for comparison and perceived as a distraction, perhaps even a threat: 'But why can we not simply say that it is a possibility? Because with probability, we start to measure something against something else' (A1).

Risk assessment often has exactly that aim: to compare different risks in order to prioritize between potential, risk-reducing measures. Comparing risks is a challenge for many of the interviewees, not least because the three dimensions (value, threat, vulnerability) are not directly comparable to the two dimensions (probability and consequence) used in general. The solution suggested (P1,P2,A6,M8) is to use a recognizable, one-dimensional scale for all the risks. P1 gives an example: if the board of an organization is given information by the 'financial' department that some risks are serious ('red'), and the security department reports some risks as serious ('red'), this is comparable. 'Red' can be compared with 'red'. The ways of arriving at this judgement of 'red' can differ. The 'financial' department can use actuarial models of probability and consequence, while the security department can use a combination of value, threat and vulnerability (P1).

The critics of 3FA regard this line of reasoning as highly problematic. Probability or likelihood has to be part of the description of a risk, both to describe risks and compare them with other risks (C3). If security risks are not 'reduced' by an estimate where the risk is expressed in terms of both probability and consequence, where the primary focus is only on consequence, the comparison is not neutral or 'fair', according to this perspective. Similar degrees of seriousness (the number of deaths, etc.) have to be 'levelled out' using a judgement of probability on all the risks to produce a meaningful comparison.

Risk assessment is a tool for decision makers, and without an explicit scaling of probability or likelihood, 3FA does not help in prioritizing (C2). Risk described without probability 'breaks down' the logic of risk and risk assessment:

> M6: You do have to judge probability - when the costs exceed one billion … should you say that this is something we just have to do? You have to make cost/benefit judgements of security measures … [The proponents of 3FA] don't want to explicitly express a judgement of probability. Or they are unable to. But, then, they are also unable to justify why you should implement different measures.

M6's reasoning is in line with an economic reasoning about risks, where a future, perceived benefit of a security measure is linked to the hypothetical situation of the difference between preventing an incident and not preventing it. Low probability implies the lower benefit of an investment than high probability. Without probability, the criticism goes, there may be an excessive focus on consequence: 'If you have a risk approach, focusing very much on consequences and vulnerabilities, then there will be maximalist solutions all the way.' (M7). Security estimates can end up with a one-sided focus on consequence if probability is not an explicit part of the risk evaluation. Investment costs and their potential benefits are not properly levelled out.

The argument against probability used by the proponents of the 3FA, where probability is understood as frequency-based, is described as a 'straw man' (C1) by critics and logically rejected

(Busmundrud et al. 2015). To view probability assessments as necessarily frequency-based is described as:

> C5: 'an old-fashioned understanding of the probability concept which originates from before the turn of the millennium and is based on old textbooks where "risk = probability X consequence" - a simple number. It is a long time since the most prominent risk milieux departed from this simple understanding of probability'.

'Softer', qualitative judgements of likelihood are most often used, according to C5, in the risk literature labelled as 'subjective' or 'knowledge-based' probabilities (Amundrud et al. 2017).

To sum up, the 3FA builds on the argument, which will be understood by many, that estimating probability is often difficult or impossible. Probability, however, has another 'role' in the expression of risk; it is a moderating factor. It makes unlikely futures lower risks than likely futures. Whereas the argument in favour of the 3FA is linked to the difficulty of estimation, the argument against it is linked to the consequence of not including probability in risk estimates.

The burden of hindsight judgements

In the following, we will focus on the perceived *consequence* of including or not including probability as a planning premise and the burden of hindsight judgements. A3's reasoning seems an apt point of departure:

> A3: … in much of what we are dealing with, probability is not relevant. Because there are some values that should be protected no matter what. And [then] … it is not how likely it is that an incident may happen that matters.
>
> … you can use the model of big numbers when you have an empirical basis for it … But then you have to be clear about it. That we have now used probability and this means that we accept a certain degree of probability for loss … that there will be some things that are missed. You will never get 100% weighting when you choose to use probability.
>
> Then you need a leader who is willing to say that 'I gambled on … ' - he won't use that word, but 'I gambled on it going well, because there was a 90% chance of it. These deaths - too bad, but this is 'the cost of doing business'. It was cheaper to let these people die than it was to secure ourselves … this was my decision.

A3 thus expresses the view that some values should be protected 'no matter what'. The consequence of using probability is that the chance of loss is introduced. Using probability involves introducing an element of 'gambling', accepting that there is 'a cost of doing business'. If gambling is to be avoided, probability should not be given weight. A3's statement builds on the classical understanding of risk, where risk is genuinely 'risky', and that is *because* it includes some version of probability. If the aim is security, understood as protection 'no matter what' (A3), probability is at odds with the aim of creating security.

A number of the interviewees point to the 2011 terrorist attack as a reference point in the debate about the approach to risk assessment (A2,A3,P1, field notes). They note the criticism that followed in its wake, regarding it as an example of the erroneousness of using probability in risk assessment.[12] M8 reflects on the experience of hindsight judgements:

> M8: I can see that it must be frustrating for those who … thought that security was not prioritized highly enough. It turns out that they are right. When it goes wrong, they are right.
>
> I: … when something happens, then it turns out that there should have been more securing?
>
> M8: You will often get that answer. It lies in the paradox, and it's here that we need to become much better at this thing with costs/benefits … dare to stick to it … No politician would do that. … This is the dilemma of the field … To be professional about security - often I feel that when one does real risk assessments, then one does not become as disaster-oriented. But when the same case gets to the media, then it becomes a whole different story. You're in total checkmate … You [the politicians] will never be able to defend yourself - with a dry risk assessment.

M8's conclusion is that the people who made the 3FA were right with hindsight: 'When it goes wrong, they are right.' They were right because probability becomes irrelevant with hindsight. In the aftermath, (s)he resonates, there is little or no acceptance for the fact that the potential, future incident is treated - beforehand - as a risk. As a risk, different futures are weighed up against one another, with costs and benefits, action and inaction. With hindsight, however, we know the answer. It should have been secured.

M8 does not, however, think it is right from a professional point of view to follow this logic. The solution is therefore not to stop carrying out cost/benefit judgements – it is to dare to stand for them. M8's solution lies in the 'sobering effect' of the professional risk assessment, however difficult it may be for politicians to stick to the choices made in the aftermath.

Discussion and conclusion

The 3FA builds on the argument that estimating probability is often difficult or impossible. The argument against the 3FA is linked to the consequence of not including probability and the need for a balanced comparison of risks. The security professionals often relate their arguments to responsibility. What they regard as their primary responsibility, however, differs. For some, but not all, arguing in favour of the 3FA, the underlying responsibility seems to be to create security; the risk assessment tool has to be seen in light of this goal. Those critical of the 3FA regard their responsibility as producing a balanced and 'fair' risk assessment as a basis for decisions.

To understand the case in question, the present article argues that we need to broaden our understanding of what is at stake. Michael Power suggests that there is a complex and historically situated 'apparatus of risk' that can be divided into three ideal types of risk-management logics (2014). The first is *anticipation*, which builds on what is often linked to a scientific aspiration to know and calculate the future, using regularities of the past. The second logic builds on the disappointments of the ambition to anticipate risks and is the logic of *resilience*. This logic accepts the existence of ignorance and uncertainty as it is impossible to anticipate what will happen in many cases. The attention thus shifts, from the character and severity of presumed, external threats, to internal matters and whether the subject itself can mitigate and survive detrimental events (Dunn Cavelty, Kaufmann, and Søby Kristensen 2015). The third logic of risk is that of *auditability*, where risk management is a way of 'making individuals and organizations responsible and accountable for managing contingent events … ' (Power 2014, 386). The underlying feature of this logic is for risk management to be demonstrated and evidenced. Risk has become so important because it is 'responsibilizing': 'Risk implies outcome responsibility in a way that uncertainty does not.' (Power 2014, 381).

All of Power's three logics are useful to understand the case in question. The 3FA *is* an attempt to anticipate risk, but the probability of attack plays a more implicit role. This moves the risk assessment towards resilience thinking, directing attention towards what is potentially vulnerable within the organization. In an interconnected world, understanding large organizations' critical inputs and outputs, interdependencies and vulnerabilities, is challenging at best. Whereas the difficulty involved in estimating the probability of attacks leads to a conclusion that it should not be estimated, the organization's values and vulnerabilities should be anticipated, however challenging.

A question arises, of why probability is singled out as the one dimension where anticipation should be 'given up'? The answer is in the present article interpreted as pertaining to *responsibility* and *security*. When risks are seen as characteristics of one's own organization, risk assessment becomes self-assessment (Power 2007). Risk is thus moved to the realm of choice and hence linked to what the organization, at least in theory, can do something about. Negative outcomes are the organization's responsibility, since decisions could always have been made differently. As was clearly shown by the first quote, when P2 asked their head if he wanted the enemy to be in charge of his organization's destiny or if he himself wanted to be in charge, risk management becomes tightly linked to responsibility and the potential for blame (Power 2007; Luhmann 1993).

Removing probability from the expression of risk was defended because it is seen as impossible to estimate. In many cases, however, it is impossible primarily because of the link to responsibility. If one's obligation is to predict and prevent *every single incident*, then the difference between 0 and 1 incidents is enormous. The probabilities of many security risks are often low, at least for a single organization. The difficulty is not necessarily in finding that out, it is to be responsible *if* something happens.

This leads to the second part of the answer; that responsibility is linked to security. Søby Kristensen argues that risk within a national security domain introduces a conceptual instability (2008). Risk-based thinking makes security issues relative. It introduces a probabilistic logic where costs can be weighed against assumed benefits. This is diametrically opposed to the security message that '[e]very terrorist attack has a potential national impact' and must therefore be prevented (Søby Kristensen 2008, 74). Risk is relative, while security is not. The 'neutral' or balanced logic of anticipating risks lies in the ideal that all 'sides' should be treated equally. There is no precautionary thinking 'baked into' the risk calculation (Sunstein 2005). This is not, however, in line with the utopian ideal of security.

Downplaying probability, we argue, 'solves' the imbalance between risk and security through a subtle securitization move: Risks that are 'low' in a 2FA can be communicated as more important or 'higher', because probability – that which moderates the risk – is given less weight. Probability has two roles in a risk assessment: anticipating the future and moderating the risk. The securitization move lies in not explicitly moderating the risk through a judgement of probability. This can be interpreted as an attempt to increase the importance of security issues to increase resources and investments. Some of the quotes from interviewees certainly substantiate such an interpretation. The reference to hindsight judgements, however, suggests a more complex explanation.

A risk is only a risk *before* the incident. Hindsight judgements no longer judge the incident as a risk, where the degree of probability is relevant. M8 concludes that 'they are right when it goes wrong'. When something goes wrong, an approach that does not take probability into account corresponds, in M8 and other's experience, with the public's hindsight judgements. Prospective organizations of risks (risk assessment arrangements) are influenced by anticipated, retrospective actions and responsibilities in the future (audits and blame) (Hardy et al. 2020).

It is unclear what should replace probabilities. Some interviewees point to 'possibilities' rather than 'probabilities'. This could indicate complete overload, where 'decisions are taken on the basis of future possibilities, however improbable or unlikely.' (Amoore 2013, 12). Focus on the organization's perceived vulnerabilities and becoming resilient is another path, much in line with the 3FA approach. A third is a pragmatic approach of choosing some scenarios and ignoring others, which is expressed by several interviewees. There is little guidance in the 3FA, however, regarding how to reason on the dimension often represented by an expression of probability. This makes it prone to the dangers expressed by Amoore and others.

To take away probability from the risk assessment, or not openly discussing likelihood judgements, differs from suggested strategies from the risk literature on how to deal with uncertain and ambivalent risks. From this perspective, probability judgements should be supplemented with strategies such as qualitative strength of knowledge judgements and openness about uncertainties (Askeland, Flage, and Aven 2017; Aven and Renn 2020).

Arguably, the 3FA can be viewed as an attempt to 'have it both ways'. Risk assessment is an attractive tool in security management; it makes security fit into a larger world of risk management and brings in flexibility and an interpretive process (Wardman and Mythen 2016). However, the utopian element of security makes it difficult to fit into a larger world of risk management, which is marked by trade-offs and 'taking risk'. Downplaying probability makes it possible to use a risk based approach *and* take precautionary measures at the same time.

It is argued here that Power's three ideal models of risk management logics shed light on the case in question. They are condensed expressions of insights from risk research and the sociology of risk, including some of the debates mentioned initially in this article. To understand risk management practises in a security framework, however, we need to pay attention also to security, and especially how security influences and interplays with responsibility. The utopian ideal of security, understood as something that should be secured 'no matter what', brings in a challenging tension into the idea of, and potentially practise of, risk assessments.

It could be objected that tolerance for failure is low within risk governance too (Power 2014). Still, how security influences social processes investigated i.e. in securitization theory (Buzan et al. 1998) seems to be lacking both in Power's theory and in much risk research. Further investigation into the intersection between risk- and security, both as phenomena and management practices, could be useful.

To conclude, the article shows how security and risk professionals deals with risk assessments in a security context. For all the professionals, risk assessment in areas of zero or low tolerance for incidents introduces a discrepancy that is difficult to handle. On the one hand, security analysts are supposed to deal with threats as risks, implying scaling, comparing and level of acceptance. On the other hand, they are supposed to create security, which implies the opposite of scaling and risk acceptance. Probability is a moderating factor in a risk assessment. It 'makes' risks relative, which is challenging in a security setting, where there is little or no room for incidents. Risk assessments becomes difficult if there is little room for taking risk.

Within critical security studies, the introduction of risk in the security domain has been interpreted as deepening a problematic securitization process (Amoore 2013; Aradau and Van Munster 2007). The case investigated suggests that, seen from a risk perspective, the argument could be turned around. The quest for security can influence the framing of risk judgements (Battistelli and Galantino 2019). The utopian character of security, the idea that 'some things should be secured no matter what', is at odds with the 'riskiness' of risk.

Notes

1. Standard Norway is the Norwegian member of the European Committee for Standardization (CEN) and International Organization for Standardization (ISO).
2. The controversy became visible not least in Busmundrud et al. (2015), in blogposts and a few newspaper articles, but took mostly place in informal discussions among security- and risk professionals.
3. 'Value' is often translated as 'asset', but it has a more wide-ranging connotation of being what is valuable/critical to an organization. All translations are done by the author.
4. There is only one concept in Norwegian for both probability and likelihood ('sannsynlighet'), referring to both numerical and qualitative judgements. The term 'probability' is used for both.
5. Aradau refers to the difference between risk and danger; the distinction is not elaborated on in the present article (Luhmann 1993).
6. Securitization is linked to a claim of something extraordinary, and how the extraordinary, if accepted by the audience, legitimizes measures not otherwise acquiesced (Buzan, de Wilde, and Waever 1998).
7. Names of the 2014 interviewees are included in Busmundrud et al.
8. *Risk and Vulnerability Analysis*, The Emergency Planning College (NUSB) 24-26 September 2018, *Risk Assessment*, Norwegian National Security Agency (NSM) 18 September 2019, *Basic Preventive Security*, NSM 7-10 October 2019, *Security-Risk Analysis*, The Norwegian Business and Industry Security Council, 2-3 October 2019.
9. Anne-Kari Valdal, ProActima Bransjemøte sikring – Statens jernbanetilsyn 12. juni 2019, last accessed 14/10/2020.
10. There is a variety of perspectives, and for some probability should be estimated, but not expressed in the final risk assessment.
11. In practice, it depends on the assumptions and judgements conducted in the risk assessment. Some argue that a more precise value (asset) assessment reduces the scope and hence the risk.

12. The government had decided years earlier to implement certain physical security measures, but the decision had not been implemented. The case is none the less used as an example of the consequence of using probabilities in security risk judgements.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was supported by the Research Council of Norway and the Norwegian Ministry of Justice and Public Security.

References

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

Amundrud, Øystein, Terje Aven, and Roger Flage. 2017. "How the Definition of Security Risk Can Be Made Compatible with Safety Definitions." *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 231 (3): 286–294. doi:10.1177/1748006X17699145.

Ansell, Christopher, and Patrick Baur. 2018. "Explaining Trends in Risk Governance: How Problem Definitions Underpin Risk Regimes." *Risk, Hazards & Crisis in Public Policy* 9 (4): 397–430. doi:10.1002/rhc3.12153.

Aradau, Claudia. 2014. "The Promise of Security: Resilience, Surprise and Epistemic Politics." *Resilience* 2 (2): 73–87. Routledge: doi:10.1080/21693293.2014.914765.

Aradau, Claudia. 2016. "Risk, (in)Security and International Politics." In *Routledge Handbook of Risk Studies*, edited by Adam Burgess, Alberto Alemanno, and Jens Zinn. Abingdon: Routledge.

Aradau, Claudia, and Rens Van Munster. 2007. "Governing Terrorism through Risk: Taking Precautions, (Un)Knowing the Future." *European Journal of International Relations* 13 (1): 89–115. doi:10.1177/1354066107074290.

Askeland, Tore, Roger Flage, and Terje Aven. 2017. "Moving beyond Probabilities - Strength of Knowledge Characterisations Applied to Security." *Reliability Engineering & System Safety* 159: 196–205. doi:10.1016/j.ress.2016.10.035.

Aven, Terje. 2020. "Three Influential Risk Foundation Papers from the 80s and 90s: Are They Still State-of-the-Art?" *Reliability Engineering & System Safety* 193: 106680. doi:10.1016/j.ress.2019.106680.

Aven, Terje, and Seth Guikema. 2015. "On the Concept and Definition of Terrorism Risk." *Risk Analysis : An Official Publication of the Society for Risk Analysis* 35 (12): 2162–2171. http://dx.doi.org.ezproxy.uio.no/10.1111/risa.12518. doi:10.1111/risa.12518.

Aven, Terje, and Ortwin Renn. 2020. "Some Foundational Issues Related to Risk Governance and Different Types of Risks." *Journal of Risk Research* 23 (9): 1121–1114. doi:10.1080/13669877.2019.1569099.

Battistelli, Fabrizio, and Maria Grazia Galantino. 2019. "Dangers, Risks and Threats: An Alternative Conceptualization to the Catch-All Concept of Risk." *Current Sociology* 67 (1): 64–78. doi:10.1177/0011392118793675.

Bieder, Corinne, and Kenneth Pettersen Gould, eds. 2020. *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. SpringerBriefs in Applied Sciences and Technology. Cham: Springer International Publishing. doi:10.1007/978-3-030-47229-0.

Boholm, Max, Niklas Möller, and Sven Ove Hansson. 2016. "The Concepts of Risk, Safety, and Security: Applications in Everyday Language." *Risk Analysis: An Official Publication of the Society for Risk Analysis* 36 (2): 320–338. doi:10.1111/risa.12464.

Boustras, Georgios, and Alan Waring. 2020. "Towards a Reconceptualization of Safety and Security, Their Interactions, and Policy Requirements in a 21st Century Context." *Safety Science* 132: 104942. doi:10.1016/j.ssci.2020.104942.

Bowen, Glenn A. 2006. "Grounded Theory and Sensitizing Concepts." *International Journal of Qualitative Methods* 5 (3): 12–23. doi:10.1177/160940690600500304.

Busmundrud, Odd, Maren Maal, Jo Hagness Kiran, and Monica Endregard. 2015. *Tilnaerminger til risikovurderinger for tilsiktede uønskede handlinger*. Vol. 2015/00923. Norwegian Defence Reserach Establishment, Kjeller, Norway.

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

Charmaz, Kathy. 2017. "Special Invited Paper: Continuities, Contradictions, and Critical Inquiry in Grounded Theory." *International Journal of Qualitative Methods* 16 (1): 160940691771935. doi:10.1177/1609406917719350.

Ciută, Felix. 2009. "Security and the Problem of Context : A Hermeneutical Critique of Securitisation Theory." *Review of International Studies* 35(2): 301–326.

Dunn Cavelty, Myriam, Mareile Kaufmann, and Kristian Søby Kristensen. 2015. "Resilience and (in)Security: Practices, Subjects." *Security Dialogue* 46 (1): 3–14. doi:10.1177/0967010614559637.

Ezell, Barry Charles, Steven P. Bennett, Detlof von Winterfeldt, John Sokolowski, and Andrew J. Collins. 2010. "Probabilistic Risk Analysis and Terrorism Risk." *Risk Analysis : An Official Publication of the Society for Risk Analysis* 30 (4): 575–589. doi:10.1111/j.1539-6924.2010.01401.x.

Furedi, Frank. 2009. "Precautionary Culture and the Rise of Possibilistic Risk Assessment." *Erasmus Law Review* 2: 197–220.

Hacking, Ian. 1990. *The Taming of Chance*. Cambridge: Cambridge University Press.

Hardy, Cynthia, Steve Maguire, Michael Power, and Haridimos Tsoukas. 2020. "Organizing Risk: Organization and Management Theory for the Risk Society." *Academy of Management Annals* 14 (2): 1032–1066. doi:10.5465/annals.2018.0110.

Heng, Yee-Kuang. 2018. "The Continuing Resonance of the War as Risk Management Perspective for Understanding Military Interventions." *Contemporary Security Policy* 39 (4): 544–558. doi:10.1080/13523260.2018.1494670.

Høyland, Sindre Aske. 2018. "Exploring and Modeling the Societal Safety and Societal Security Concepts – a Systematic Review, Empirical Study and Key Implications." *Safety Science* 110: 7–22. doi:10.1016/j.ssci.2017.10.019.

Jore, Sissel H. 2019a. "The Conceptual and Scientific Demarcation of Security in Contrast to Safety." *European Journal for Security Research* 4 (1): 157–174. doi:10.1007/s41125-017-0021-9.

Jore, Sissel H. 2019b. "The Multifaceted Aspect of Uncertainty –the Significance of Addressing Uncertainty in the Management of the Transboundary Wicked Problem of Terrorism." In *Proceedings of the 29th European Safety and Reliability Conference(ESREL). 22-26 September 2019 Hannover, Germany*, edited by Michael Beer and Enrico Zio. 4044–4051. doi:10.3850/978-981-11-2724-3.0622-cd.

Jore, Sissel H. 2020. "Standardization of Terrorism Risk Analysis." In *Standardization and Risk Governance*, edited by O. Olsen, K. V. Juhl, P. Lindøe, and O. Engen. London: Routledge. doi:10.4324/9780429290817.

Klima, Noel, Nicholas Dorn, and Tom Vander Beken. 2011. "Risk Calculation and Precautionary Uncertainty: Two Configurations within Crime Assessment." *Crime, Law and Social Change* 55 (1): 15–31. doi:10.1007/s10611-010-9265-2.

Klinke, Andreas, and Ortwin Renn. 2002. "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies1." *Risk Analysis : An Official Publication of the Society for Risk Analysis* 22 (6): 1071–1094. doi:10.1111/1539-6924.00274.

Larsson, Sebastian, and Mark Rhinard, eds. 2020. *Nordic Societal Security. Convergence and Divergence* (1st ed.), London: Routledge.

Luhmann, Niklas. 1993. *Risk: A Sociological Theory. Soziologie Des Risikos*. Berlin: Wallter de Gruyter.

Maal, Maren, Odd Busmundrud, 2016. and, and Monica Endregard. "Methodology for Security Risk Assessments – is There a Best Practice?." In *Risk, Reliability and Safety: Innovating Theory and Practice*, Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016, Glasgow, Scotland, 25–29 September 2016, edited by Matthew Revie, Tim Bedford, and Lesley Walls. London: Taylor & Francis.

Manunta, Giovanni. 2002. "Risk and Security: Are They Compatible Concepts?" *Security Journal* 15 (2): 43–55. doi:10.1057/palgrave.sj.8340110.

McInnes, Colin, and Anne Roemer-Mahler. 2017. "From Security to Risk: Reframing Global Health Threats." *International Affairs* 93 (6): 1313–1337. doi:10.1093/ia/iix187.

Mueller, John, and Mark G. Stewart. 2014. "Terrorism and Counterterrorism in the US: The Question of Responsible Policy-Making." *The International Journal of Human Rights* 18 (2): 228–240. doi:10.1080/13642987.2014.889397.

Mythen, Gabe. 2018. "Thinking with Ulrich Beck: Security, Terrorism and Transformation." *Journal of Risk Research* 21 (1): 17–28. doi:10.1080/13669877.2017.1362028.

Mythen, Gabe, and Sandra Walklate. 2008. "Terrorism, Risk and International Security: The Perils of Asking 'What If?" *Security Dialogue* 39 (2/3): 221–242. doi:10.1177/0967010608088776.

NSM, PST, and POD 2015. *Terrorsikring. En veildning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger.*

Paté Cornell, Elisabeth. 2012. "On 'Black Swans' and 'Perfect Storms': Risk Analysis and Management When Statistics Are Not Enough." *Risk Analysis* 32 (11): 1823–1833. doi:10.1111/j.1539-6924.2011.01787.x.

Petersen, Karen Lund. 2012. "Risk Analysis – a Field within Security Studies?" *European Journal of International Relations* 18 (4): 693–717. doi:10.1177/1354066111409770.

Pettersen, Kenneth Arne. 2016. "Understanding Uncertainty: Thinking through in Relation to High-Risk Technologies." In *Routledge Handbook of Risk Studies*, edited by Adam Burgess, Alberto Alemanno, and Jens O. Zinn, 39–48. Abingdon: Routledge.

Pettersen, Kenneth Arne, and Torkel Bjørnskau. 2015. "Organizational Contradictions between Safety and Security – Perceived Challenges and Ways of Integrating Critical Infrastructure Protection in Civil Aviation." *Safety Science* 71, 167–177. doi:10.1016/j.ssci.2014.04.018.

Pouliot, Vincent. 2008. "The Logic of Practicality: A Theory of Practice of Security Communities." *Int Org* 62 (2): 257–288. doi:10.1017/S0020818308080090.

Power, Michael. 2007. *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

Power, Michael. 2014. "Risk, Social Theories, and Organizations." In *The Oxford Handbook of Sociology, Social Theory, and Organization Studies*, edited by Paul Adler, Paul du Gay, Glenn Morgan, and Mike Reed, 1st ed., 370–392. Oxford: Oxford University Press. doi:10.1093/oxfordhb/9780199671083.001.0001.

Reason, James. 1997. *Managing the Risks of Organizational Accidents*, Ashgate, Aldershot .

Salter, Mark B., Can E. Mutlu, and Oxford Handbooks Online 2018. "Methods in Critical Security Studies." In *The Oxford Handbook of International Security*, edited by Alexandra Gheciu and William Curti Wohlforth. Oxford: Oxford University Press.

Smith, Clifton, and David J. Brooks. 2012. *Security Science* (1st ed.). Butterworth-Heinemann. https://www.elsevier.com/books/security-science/smith/978-0-12-394436-8.

Søby Kristensen, Kristian. 2008. "The Absolute Protection of Our Citizens': Critical Infrastructure Protection and the Practice of Security." In *Securing "the Homeland": Critical Infrastructure, Risk and (in)Security*, edited by Myriam Dunn Cavelty and Kristian Søby Kristensen, 63–83. London: Routledge.

Standards Norway. 2012. NS 5830 Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi.

Standards Norway. 2008. *NS 5814 Krav til risikovurderinger*.

Standards Norway. 2014. *NS 5832 Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse*.

Stern, Jessica, and Jonathan B. Wiener. 2006. "Precaution against Terrorism." *Journal of Risk Research* 9 (4): 393–447. doi:10.1080/13669870600715750.

Stirling, Andy. 2010. "Keep It Complex." *Nature* 468 (7327): 1029–1031. doi:10.1038/4681029a.

Sunstein, Cass R. 2005. *Laws of Fear: Beyond the Precautionary Principle* (Vol. 6). The Seeley Lectures. Cambridge: Cambridge University Press.

Swedberg, Richard. 2018. "How to Use Max Weber's Ideal Type in Sociological Analysis." *Journal of Classical Sociology* 18 (3): 181–196. doi:10.1177/1468795X17743643.

Taleb, Nassim Nicholas. 2010. *The Black Swan : The Impact of the Highly Improbable*. Rev. ed. New York: Random House Trade Paperbacks.

Van Coile, Ruben. 2016. "Probability." In *Routledge Handbook of Risk Studies*, edited by Adam Burgess, Alberto Alemanno, and Jens O. Zinn, 27–38. Abingdon: Routledge.

Vedby Rasmussen, Mikkel. 2006. *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*. Cambridge: Cambridge University Press.

Wardman, Jamie K., and Ragnar Löfstedt. 2018. "Anticipating or Accommodating to Public Concern? Risk Amplification and the Politics of Precaution Reexamined." *Risk Analysis : An Official Publication of the Society for Risk Analysis* 38 (9): 1802–1819. doi:10.1111/risa.12997.

Wardman, Jamie K., and Ragnar Lofstedt. 2020. "COVID-19: Confronting a New World Risk." *Journal of Risk Research* 23 (7/8): 833–837. doi:10.1080/13669877.2020.1842988.

Wardman, Jamie K., and Gabe Mythen. 2016. "Risk Communication: Against the Gods or against All Odds? Problems and Prospects of Accounting for Black Swans." *Journal of Risk Research* 19 (10): 1220–1230. doi:10.1080/13669877.2016.1262002.

Zinn, Jens O., ed. 2008. *Social Theories of Risk and Uncertainty. An Introduction*. Hoboken: John Wiley & Sons, Ltd. doi:10.1002/9781444301489.ch1.

III

European Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/feus20

From prescriptive rules to responsible organisations – making sense of risk in protective security management – a study from Norway

Anne Heyerdahl

To cite this article: Anne Heyerdahl (2022): From prescriptive rules to responsible organisations – making sense of risk in protective security management – a study from Norway, European Security, DOI: 10.1080/09662839.2022.2070006

To link to this article: https://doi.org/10.1080/09662839.2022.2070006

EUROPEAN SECURITY
https://doi.org/10.1080/09662839.2022.2070006

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

From prescriptive rules to responsible organisations – making sense of risk in protective security management – a study from Norway

Anne Heyerdahl

Department of Sociology and Human Geography, University of Oslo, Oslo, Norway

ABSTRACT

Protective security management aims at protecting against malicious acts. It has, in a relatively short period, undergone substantial changes. One such change is the introduction of risk management. This article investigates a debate about a standard for security risk assessment (SRA) in Norway. It focuses on sense-making by security professionals, drawing on a unique interview material. The analysis utilises Michael Power's theory on risk governance, as well as insights from security studies. A central finding is that the SRA approach was introduced to create more analytical security management. The importance of analysing one's values (assets) makes it key to scrutinise the organisation's characteristics, goals and vulnerabilities, regarded as moving security management in the direction of corporate governance. The article investigates how understanding of risk assessment and security interplay, and identifies a tension between risk (assessment) and the goal of protection, which makes security management risk averse. A requirement of creating *sound security* is viewed as a potential for burdensome organisational responsibility and blame. The analysis identifies elements of what is often described as resilience (attention towards vulnerabilities), but without the political reading (neo-liberal abdication of the state), thus contributing to the literature on resilience.

ARTICLE HISTORY
Received 28 January 2022
Accepted 21 April 2022

KEYWORDS
Protective security; security management; sociology of risk; risk management; resilience; interpretation

Introduction

Protective security management consists of attempts to protect against malicious acts. Although it does have some expressions visible to everyone, such as safety zones around government buildings, security management is mostly invisible and "boring", far from the grand narratives of security, viewed as "a matter of 'high politics' and statecraft, not the 'low politics' of the domestic realm" (Bossong and Hegemann 2019, Neal 2019, p. 4). It works in the tension between the undramatic, tedious work of non-events and the perceived severe potential of malicious attacks. This invisibility, however, should not prevent us from seeing the importance of investigating "the politics of protection" (Huysmans 2009,

CONTACT Anne Heyerdahl ✉ Anne.heyerdahl@sosgeo.uio.no

Supplemental data for this article can be accessed online at https://doi.org/10.1080/09662839.2022.2070006.
This article has been corrected with minor changes. These changes do not impact the academic content of the article.

p. 14). Security is also "about everyday routines and technologies of security professionals" (Bigo 2002, Aradau and Van Munster 2007, p. 98).

In 2014, Standards Norway (2014) published a standard for security risk assessment (SRA) pertaining to when the risk stems from intentional undesirable acts (NS 5832), as part of a series of security risk management standards. During and especially after its publication, a controversy arose between security and risk professionals as well as civil servants, concerning the usefulness of this approach (Maal *et al.* 2016, Jore 2019, Heyerdahl 2022). The approach and ensuing discussions resonate with scholarly investigations into the risk–security nexus and the use of risk management in a security context (Amoore 2013, Dunn Cavelty *et al.* 2015).

This article builds on a study of the professionals' perspectives on and sense-making of risk management within the realm of security. The debate is used as a lens for understanding more general developments in the intersection between risk and security management. The SRA approach was introduced during a period of rapid, extensive changes in protective security. Part of the professionals' reasoning also relates to a new Security Act, which includes a requirement to have a risk-based approach (Norwegian Ministry of Justice and Public Security 2019, §4-2). The article asks: How do security professionals make sense of risk assessment and the SRA approach, and what does this sense-making tell us about the use of risk assessment in protective security management (PSM)?

The practices of interest are close to what is often linked to critical infrastructure protection (Dunn Cavelty and Søby Kristensen 2008, Bossong 2014). SRA, however, casts its net more widely; all "security risks" are relevant.

Security and defence studies have paid little attention to questions of management (Taylor 2012, Norheim-Martinsen 2016). Although practises of security professionals have been investigated, it is mostly related to expertise on an international level (Berling and Bueger 2015). When national practises are under scrutiny, it tends to focus on how agencies and professionals participate in transnational security practises (Bigo *et al.* 2010). Few investigations have been conducted on the reasoning and local sense-making of professionals. Security cultures are understood as "extremely difficult to penetrate or to participate in" (Salter and Mutlu 2013, p. 7). This article aims at being an exception, by contributing rare, extensive qualitative data on security professionals' reasoning. It prioritises extensive quotes, aiming to provide "thickness" on which to base the analysis (Alvesson and Sköldberg 2018).

Of particular interest to this article is the risk–security nexus. Although risk (management) shares with security (management) the perspective of potential negative futures, both traditions and academic disciplines stem from different backgrounds (Petersen 2012, Pettersen Gould and Bieder 2020); security from the aim of creating national security in an international environment, as well as criminal justice; risk from a wide number of fields, such as insurance and industrial safety. Security scholars have noted that (national) security has for some time been managed by tools and perspectives from risk management (Aradau and Van Munster 2007, Petersen 2012). Scholars have investigated the difference between viewing a (security) issue in terms of "risk" as opposed to "threat" (Corry 2012, Bengtsson *et al.* 2018). An alternative to accentuating the difference is to investigate how practices and discourses that have evolved in one, influence, merge and develop through interactions with the other, potentially influencing how we understand and manage both (Amoore 2013, Battistelli and Galantino 2019, Berling et al. 2021, Heyerdahl 2022).

Recognising the importance of risk management for the case at hand, we turn our attention to Michael Power's (2007, 2016, 2021) theory of risk governance, which builds on the sociology of risk, as well as organisational theory and management studies. We utilise Power's (2014) ideal models of risk management logics as sensitising concepts (anticipation, resilience, auditability), but also draw on Bigo's (2006, 2009) investigation into discourses on protection. The benefit of utilising Power is that he theorises risk management practises coming from auditing and risk governance, with the inside of organisations as a point of reference. His theory is thus closer to the details of organisational life and management than most security scholars investigating risk management.

In the article, we (a) describe how the SRA approach is perceived as a shift from prescriptive rules to a more analytical approach. We (b) discuss the notion that the approach is "value[asset]-centred", and the way in which this links PSM to (corporate) risk governance. Lastly, (c) the normative requirement for "sound security" is discussed.

The study contributes to the call for richer descriptions of "riskwork" (Power 2016), and to analyse "how security works in practise" (Nyman 2016, p. 823). It shows how risk assessment is given new meaning in the translation into a security setting (Berling et al. 2021), negotiated in a Norwegian, that is, local context (Ciută 2009). The article sees the SRA approach as an attempt to reduce the tension between the idea of creating security, linked to the state's role as protector, and risk management, building on assumptions of flexibility to optimise outcomes. It suggests that protection better conveys what is at stake than resilience. Lastly, the article investigates the perceived responsibilitisation of organisations, and how SRM thus becomes part of the overall governance in organisations.

Background

"Securing" in a national security context became high politics in Norway in 2011, after a right-wing terrorist killed eight people in Oslo in a bomb attack, then killed 69 people in a shooting massacre at a political youth camp. The attack severely damaged key government buildings, such as the Prime Minister's office. The subsequent inquiry criticised the government for the lack of protective security measures (NOU 2012, p. 14). Investigations, audits, parliamentary hearings and a new Security Act all placed protective security measures, and the perceived lack thereof, on the agenda.

Taking a step back, key changes in security management occurred after the Cold War in Norway as in other countries. A functional and broad "all-hazard" approach emerged, with a broad societal security perspective (NOU 2000, p. 24, Olsen *et al.* 2007, Larsson and Rhinard 2021). Security measures were supposed to address "problems related to the survival and recovery of vital societal functions" (Hovden 2004, p. 631). A distinction eventually arose between "safety", linked to natural disasters and accidents, and "security", linked to malicious acts (Jore 2019); PSM belongs to the latter.

A key milestone for PSM was an Act on Protective Security proposed by the Ministry of Defence (2001). The Act created a distinction between military intelligence and protective security (Prop.153L; Norwegian Ministry of Defence 2017). It regulated protective, defensive actions to reduce the risks of security threats from espionage, sabotage or terrorism (Norwegian Ministry of Defence 2001 §3-2).

The functional, broad security perspective was strengthened in a new Protective Security Act (Norwegian Ministry of Justice and Public Security 2019). Entities subject to the Act are those which "control information, information systems, objects or infrastructure which are of vital importance to fundamental national functions" (§1-3 b). The Security Act is not limited to the military. Increasingly attention in security governance is geared towards fundamental national functions in the civil domain (water, electricity, etc.).

The private standard subject to this study was produced by Standards Norway (SN 5832:2014).[1] It is built on a governmental guideline on terror protection (Norwegian National Security Authority *et al.* 2010). The standard targets all types of security risks. The interest in this article is on the perspectives and discourses pertaining to national security.

When the term SRA is used, it refers to the security risk assessment approach presented in the standard and terror protection guidelines mentioned above. SRA is one element in a larger system of security risk management (SRM). PSM is the area where the SRA takes place, here narrowed down to "national security".

Theoretical approach

This article utilises Michael Power's writings on risk governance as a theoretical lens. Power describes a shift, in a short period of time, from a discourse on risk assessment as a mainly technical discipline to calculate risk, intimately linked to science, engineering and insurance, to a logic concerned mainly with organisation and accountability (Power 2007). Concerns have been raised in the social sciences that technical risk approaches not only solve but also produce risks (Beck 1992). Similarly, Hutter and Power (2005) argue, organisations are agents in handling risk, but notably also potential producers of risk. Risk is a key feature in contemporary organising (Hardy *et al.* 2020). Risk governance not only acts on knowledge, it also shapes organisations and their actions.

Three ideal models of risk management logics

Power (2014) has argued that risk and risk management build on a complex and historically situated "apparatus of risk", divisible into three ideal models of risk management logics. The logics are not mutually exclusive, on the contrary, Power stresses, "any specific practice setting … will involve a combination of all three to varying degrees" (Power 2014, p. 387). The ideal models have been little used, even by Power, but are regarded as a heuristic tool and as sensitising concepts (Blumer 1954) aiding interpretation.

Anticipation

The first risk management logic is *anticipation*, building on the scientific aspiration to know and calculate the future, using past regularities (Power 2014). In this model, risk assessment is a technical discipline closely related to science and the specialised practices of experts. Power (2014) notes that the idea of anticipation does not depend on actual calculability, "although the promise remains in the background" (p. 383).

Resilience

The second risk management logic builds on the disappointments of the ambition to anticipate risks and is the logic of *resilience* (Power 2014). This logic accepts the existence of ignorance and uncertainty and builds on an understanding that it is impossible to anticipate future events in many cases. Instead, the focus is on creating resilience to unforeseeable events. Attention shifts from the character and severity of presumed, external threats to internal matters and whether the subject itself can mitigate and survive detrimental events (Dunn Cavelty *et al.* 2015). "The rise of resilience marks a significant shift from the predictable to the contingent" (Dunn Cavelty *et al.* 2015, p. 6), from "problems to responses" (Aradau 2017, p. 80). Emphasis is on matters such as identifying vulnerabilities, creating redundancy, robust organisational designs and recovery mechanisms (Power 2014, Rogers 2017).

Power sees resilience primarily in contrast to the idea of anticipation. The resilience concept has, however, a number of other notable connotations. It has been linked more generally to non-hierarchical, poly-centric and "organic" developments (Rogers 2017, Bourbeau 2018). In critical readings, resilience is often related to a "typically neoliberal social contract, where the state is allowed to withdraw at the expense of the community" (Brunner and Plotkin Amrami 2019, p. 233). Resilience as a security solution is seen as moving security-planning away from the political level of governments, "outsourcing" solutions to the individual or organisational level (Berling and Petersen 2021).

Accordingly, the concept of resilience has been much criticised as "a moving target" (Rogers 2017, p. 19), so diverse and contested that it has been asked whether it serves "more the role of cultural metaphor than … a well-developed scientific concept" (Jore 2020, p. 2). For our purposes, we retain the ideal model, at least initially, as it may help describe a potential shift in perspective. In the "dialectic of enlightenment" (Power 2014, p. 373), risk-taking is fundamentally a positive endeavour; you *take* risk because the potential gains outnumber the potential negative consequences. In the shift to resilience as a risk management logic, risk is not something you actively seek, it is something you hope to mitigate against and protect yourself from.

Auditability

The third ideal model of risk management logic is *auditability*. "The underlying feature of this logic is for risk management to be demonstrated and evidenced" (Power 2014, pp. 386–387). Power (2014) labels this a "regulator-driven conception of risk management" (p. 387). In a legal system, evidence of process is required. If there is no evidence of risk management, then according to this logic, risk management did not occur (Power 2014). It is thus necessary to produce an audit trail that "creates traceability between primary data and higher order representations of information" (Power 2007, p. 164). This is not so much a precision of calculation as of process (Power 2007).

The "governance" part of risk governance responds to concerns of legitimacy and transparency (Power 2007), a responsiveness to a broader community than that of just experts and managers, "a reflexive self-consciousness in regulatory regimes" (Ansell and Baur 2018, p. 401). The auditability logic is strongly linked to responsibility and governance. It is not easy to judge whether experts inside organisations are doing a good job. This is especially so with risks which are "complex counterfactuals about the distant future" (Pollack cited from Power (2007, p. 19)). Expert judgements are thus not directly "auditable". The management process that surrounds the expert judgements can, however, be audited (Power 2007). The possibility to hold organisations to account is thus made possible by a shift in attention from the "substantive" questions of risks to the process part of risk assessment and management.

Central to Power's (2021) theory is that auditing does not only "represent" pregiven facts; it constructs the reality or "facticity" of performance, creating the control systems and the reporting structures of the organisation. Performance is thus made "auditable" through the creation of auditable facts, amenable to observation and inspection (Power 2021). The audit trail has, Power (2021) argues, something very attractive to offer organisations. It externalises performance and gives it "facticity"; it helps organisations and actors "make sense of themselves and their performance in primary traces" (Power 2021, p. 16). The benefit is that performance is fully externalised and objectified and thus defendable.

Modes of disappointment

Power (2014) presents "modes of disappointment" within the different logics (see Table 1, p. 387). In the anticipatory logic, knowledge is striven for and an unexpected event would be a disappointment, since the event should have been predicted. The logic of resilience has the ambition of survival, and the mode of disappointment in this logic is thus disaster. The auditability logic has to do with responsibility and hence the mode of disappointment is a negative outcome within "your" area of responsibility, which can be blamed.

Method and data

This article presents a study of the reasoning of security professionals in relation to an SRA standard. The debate about, and understanding of, the standard are used as a "lens" to investigate broader developments in security and risk management. The analysis builds on a primarily abductive logic, where a "situational fit" between observed facts and theory is sought (Timmermans and Tavory 2012, Alvesson and Sköldberg 2018). We utilise a theory of ideal models as heuristic tools of a sensitising kind (Blumer 1954). The models cannot be "tested", but they guide us, and sensitises us, by "providing clues and suggestions" (Blumer 1954, p. 8).

Ideal models are ideal types in a Weberian sense and, as such, they are intimately linked to theory (Rosenberg 2016). The benefit is that they are condensed expressions of complex, theoretical insights. One potential shortcoming is that the models are created in a different context, risking us imposing understandings and becoming less context-sensitive (Ciută 2009). A key strategy is thus to be sensitive also to the possibility that the ideal models do not fit.

The study uses a combination of interviews, fieldwork and written material. The interview data consist of 40 interviews, 31 conducted by the present author in 2018–2021 and 9 in 2014 by Busmundrud *et al.* (2015). Interviewees were mainly security professionals and civil servants. Some were interviewed more than once, making the number of interviewees 34, from 19 different organisations (see Table 2). The interviews conducted by the

Table 1. Power's three logics of risk management.

Logic	Fact production	Mode of disappointment
Anticipation	Knowledge of the future	Unexpected events (surprise)
Resilience	Uncertainty and ignorance	Disaster
Auditability	Decision responsibility	Blame

author have been anonymised, as the interviewees do not speak on behalf of their organisations, and to encourage open dialogue.[2] Translations of interviews and texts, including citations from standards, are conducted by the author.

Interviewees were selected through a combination of strategic and snowball sampling, with the intention to gain insight into the questions raised and elicit multiple perspectives. The interviewees are influential or well-positioned advisors in terms of the relevant policy developments. The author has also conducted fieldwork at four courses for practitioners of risk assessment and security planning.[3] Written material, such as standards, guidelines, reports, laws and other administrative documents, has also been analysed.

The interviewees were asked mainly open questions about topics such as the development of PSM, the introduction of SRM and SRA, their views on approaches to risk assessment in a security context, why a different approach was developed to security risks and so forth. Transcribed interviews and notes from fieldwork were coded in Nvivo, using a combination of sorting-based (Tjora 2018) and analytical (Charmaz 2017) coding. The three empirical topics raised in this article are a result of primarily inductive, analytical coding, finding matters such as "values" and "sound security" to be important. Findings have been refined by engaging with theory in line with the abductive logic.

The author has a leave of absence from the Norwegian Ministry of Justice and Public Security, and a background of nearly 20 years as a civil servant in Norway, (see Supplemental material) for elaboration of formal arrangement and methodological implications.

From rules to anticipation and "sound security"

Risk assessment as reaction to rules

An important reference point for the discourse on SRA is the demarcation concerning what it is *not*. It is regarded as representing a shift away from the previous way of conducting PSM. In the national security context, PSM during the Cold War era is described as building largely on detailed, prescriptive rules. PSM consisted of following checklists, stencils or predefined frameworks. Detailed rules were supposed to ensure sufficient, sound security measures, often linked to military planning as shaped by NATO:

> A14: The security instructions were very NATO and NATO was very American. And the Americans delight in making detailed rules and they also have the people and money to deal with such matters.

Table 2. Interviews – key characteristics[a].

Type of institution	Interviews	Interviewees	Organisations	Education	Gender
Ministry	9	9	5	Social science 10	25 Male
Public Agency	17	15	7	Technical/practical 9	9 Female
Research Institute	3	3	2	Law 5	
Private sector/Standardisation	11	7	5	Military 4	
				Police 3	
				Humanities 1	
				Medical 1	
				Business 1	
Total	40	34	19	34	34

[a]When referring to interviews, M stands for ministry, A for agency, P for private/standardisation and R for research institute.

Interviewees seem to agree that protective security practice as it developed during the Cold War was not advanced analytically. “We lived a bit of a shadowy existence behind the instructions; the field was rather amoeba-like” (A10). Such prescriptively oriented rules, however, became challenging after the Cold War:

> A7: It was a rule-based regime, with a flimsy, professional foundation … where rules were used as well as people who mostly lacked an analytical way of thinking, while in charge of areas of the utmost importance. Perhaps this worked in 1980 because the world was so simple then that a rule-based approach could work. But as complexity has increased, this approach no longer cuts it …
>
> Much protective security has consisted of rules, rules, rules. This created a challenge in that the world moves much more quickly than protective security.

A rule-based system is thus not regarded as flexible enough to adapt to a fast-changing world. Predefined rules and “stencils” also do not lead de facto to security: “If you use stencils to choose solutions from, you don’t have control of anything, really … You have no connection with what is smart or sensible” (M4). According to this perspective, a “checklist” type of practice and mentality de facto abdicates from actively judging what a solid, holistic and sensible security arrangement would consist of.

An auditing system that paid attention to detail ran in tandem with these prescriptive rules:

> M8: I think their auditing has not been particularly risk-based. They’ve been obsessed with deviations. In many weird and low-risk areas. Counting some stamps here and some stamps there.

Summing up, PSM according to the “old” system is described as a fine-grained rule-oriented system, often with attention to detail in terms of rules and auditing.

SRA as analytical practice to anticipate risk

The SRA approach laid out in the standard was not the first attempt to produce a risk-based approach to security management, and not the only security practice using risk assessment.[4] Arguably, however, it represented the most articulate and clear-cut expression of a more general desire to break with a prescriptive, rule-oriented practice in PSM, at least in what is publicly known. It also spurred a public debate among security professionals for a while, the basis for this investigation (Heyerdahl n.d.).

Arguably, the standard’s main contribution was that it stated that security management should be conducted using tools from risk management. It also expressed the importance of using an approach tailored to security risks. Introducing risk management was perceived as a radical shift, as expressed by a senior civil servant:

> A12: It’s an important change when you go from a legal approach, where you have laws and regulations, and attention to how you should follow them. You also have … pretty specific ways of governing. Securing objects … is quite a technical, specific and detailed type of governance. This has characterised the field. And, now, shifting to having to think risk-based. It’s a pretty big change.

The content of the standard shares much in common with other risk assessment approaches, the most notable difference being the expression of risk (see Table 3).

Table 3. The SRA standard.

- The SRA standard defines risks as "the relationship between a threat against a given value and this value's vulnerability towards the specific threat" (NS 5832:14:4) This builds on routine activity theory within criminology and Manunta (Stranden 2019).
- A risk assessment consists of:
  - (a) a value judgement, where values should be identified and ranked (see Table 4)
  - (b) security goals being set, pertaining to "what is a desired or acceptable state of affairs for the values of the entity during or after an unwanted incident" (NS 5832:14:6)
  - (c) a threat assessment and choice of threat scenarios
  - (d) the vulnerability assessment uncovering to what extent the values are vulnerable in the scenarios chosen
  - (e) the risk assessment, based on the value-, threat- and vulnerability assessments
  - (f) judgements of uncertainties

The advocates of the SRA approach argue that risk assessment pertains to a thorough, systematic analysis that reveals, as far as possible, which risks are critical. There is a perceived need for more analytical, and often academic, knowledge:

> A9: There's a requirement now for more theoretical knowledge …
>
> I: What type of knowledge?
>
> A9: Often analysts. Often with political science backgrounds. When I look around, the proportion of academics in such organisations is increasing. Before, there were people like me; oldies from the police and military. Stomping about. Now their backgrounds are much more academic.
>
> I: And what do you think about this development?
>
> A9: I think it's utterly correct … It leads to the security measures being more conscious, more adapted to the actual threat.
>
> I: Do you think they conduct their analyses differently? That they think differently?
>
> A9: Yes … they start from the right end. They do it in the right way. Which risks are we actually facing? Questions, questions, questions. And these people are good at asking questions about why. That's what's important. And they know how to answer them. Before there was a consultant who said "you need to protect yourselves against terror and you have to do this and that; security bollards, barriers; you need to block off this whole quarter" … They were just crude judgements that could have been done much more elegantly.

In the SRA standard, a separate subchapter is devoted to the importance of critical thinking and analytical rigour (Standards Norway 2014). It underlines the importance of a systematic approach using standardised methods. It also notes the importance of securing the equivalent of data reliability and validity. Security propositions should be developed as hypothesis and tested (Stranden 2019). The subchapter conveys that security management as risk assessment requires skills in line with academic reasoning from (social) science.

A9's quote above conveys an "optimism" on what is possible with the right skills. Especially immediately after the publication of the standard, but also today to some degree, there is a confidence in SRA as a tool to anticipate security risks by many, but not all. Through rigorous analysis and strengthened analytical skills, an (academically oriented), knowledge-based security management system can be created. Several interviewees call for rigorous, in-depth analysis:

Table 4. Values.

A value is defined as "a resource which, if it is exposed to an unwanted impact, will result in a negative consequence for those who own, manage or have a benefit from the resource" (NS 5830:12 p. 4). Values can be material or immaterial, examples are life and health, physical objects, classified information, monetary values, infrastructure, reputation and "operative capability" (Standards Norway 2012, (Norwegian National Security Authority *et al.* 2015)).

Values may be interdependent. Something within one organisation may be valuable "upstream" to another organisation. This is most prevalent in digital chains. Value judgements thus need to take cross-organisational dependencies into account.

> P5: Many were of the opinion that the method should be simple enough even for your grandmother to follow it. But that's meaningless. This is a specialist area. If you don't understand the area, or the method and can't create content, it's just a waste of time. … If you make it so simple that even your grandmother can do it, it does not make sense. It does not help shed light on the decisions I am supposed to arrive at.
>
> I prefer that you do not conduct a risk assessment if it is a bad one. Then it might be wrong, but it makes you feel confident, and you just go ahead.

Thorough risk assessments based on professional methods and judgements are thus needed, or else the analysis will not help in making decisions and may even lead to a false sense of knowledge and security.

The SRA standard is also regarded as more academic than traditional security management in that key people who developed the approach had studied at British universities, often a practically oriented MSc.

The perspectives are notably *not* academic in the sense of interacting with, or using research from, academia.[5] There are very few references to academic knowledge and publications presented, especially given the aim of making security management more scientific (Busmundrud *et al.* 2015, Stranden 2019; fieldnotes).

Agreement, but also criticism

All the interviewees, from inside and outside of security management, regard risk assessment as meaningful. They support the idea that (security) risk assessments can provide insights which will help protect against, or prevent, future incidents. No-one regards it as a precise science. The focus on anticipating risks makes analytical skills key.

Although all interviewees agree that risk assessment is a useful tool, there are also disagreements and criticism of the SRA approach. We can mention only a few. One is about the level of abstraction and the usefulness of SRA on a more strategic level:

> A4: They [proponents of SRA] focus on protecting objects … many come from physical security … . The point of departure: I have a small area of responsibility, which I am supposed to protect. What should I prioritise within this area of responsibility? The approach is useful when you have an installation or maybe a company. But it is not useful on a societal level or a larger scale, where you must compare apples with pears. That's what risk management is about … And then the approach is utterly useless.

A4 regards risk management at a strategic or societal level as a pragmatic comparison, scaling different types of risk, not as an in-depth, detailed analysis to "find" the risks.

Another concern is the idea that organisations can, and should, conduct threat assessments. "You need a type of competence that actually lies with the PST [Police Security Agency] and E [Intelligence Service] … you may get some rather dangerous and scary judgements - built on a false premise" (A5). A5 and others regard threat assessments conducted by people outside the professional services as potentially dangerous, as threats may be exaggerated, with the potential for drawing false conclusions.

Summing up, the SRA approach and the change it represents are viewed as a break with a rule-oriented, former practice involving detailed, prescriptive rules. The standard introduces a perspective on security management that is geared more towards anticipating future risks through risk assessments. Some advocates convey an optimism about what can be anticipated from it, although the optimism has waned somewhat. People in favour of the approach often stress in-depth and thorough analysis, whereas critics regard the level of ambition when it comes to anticipation as unrealistic on a larger scale.

A value-centred approach

One notable characteristic of the security risk approach is that it is "value-centred". The first step of a SRA is a value judgement, where the organisation's values (assets) are mapped and ranked. The term "value" is linked to what is valuable to the organisation and thus has a wider connotation than "assets" (see Table 4). Values are in line with the idea of *objects at risk*, the key characteristic being that it is "*endowed with a value that is considered at stake*" (Boholm and Corvellec 2011, p. 177).

Characteristic of a value judgement is that it is not obvious what is worth securing before the assessment:

> P5: We conducted a real value assessment for the first time - what is valuable? Everyone indicated the basement full of highly classified information. But through the process we discovered that what was really valuable to the agency was delivering strategic alerts. The ability to say that "we may now be attacked". It means that the function of agency X, the operative capability of X, that's the most important. Not the basement full of "top secret" stuff.

The organisation assumed that classified information was its key value. By analysing the organisation's values, they came to realise that what was most critical, and thus worth securing, was linked to the goals of the organisation and its ability to deliver them.

According to this perspective, security management develops into, or merges with, (corporate) governance: "The link to the governance systems, the awareness of - why are we here? Which services do we really deliver? That's essential" (A6).

In its clearest expression, security management becomes detached from, or at least is not limited to, the traditional expressions of (or artefacts from) security, such as classified information and physical security measures. Human research management can in principle, if not in practice, become as important as secure locks and classified information.

Attending to values is not limited to a specific standard or method but is described as a shift in attention that goes beyond security management. A quote by an interviewee outside of the traditional security milieu describes this shift:

> A6: We have been highly incident-driven. Now we are becoming more and more value-orientated. You realise that security is value-centred. It's the values you are concerned about securing. The challenge then becomes that you must discuss what types of values do we really have, what is inside and outside of the Security Act and critical societal functions?
>
> I: It sounds like a development where the … [SRA] approach is becoming more and more important?

> A6: Yes, I see it first and foremost as a discourse.
>
> I: A discourse?
>
> A6: Yes, a discourse linked to values and threats.

The SRA approach is described above as a changing "discourse", the increased attention to characteristics about "yourself" and what is worth securing. "Understanding yourself" is not trivial. Indirectly, this change attention to what potentially may be harmful. It does not (only) have to do with the external world, it is also linked to characteristics about "yourself".

Values drive risk

Several interviewees expressed, whether directly or indirectly, that values often "drive" risk. What should be secured is at the heart of protective security:

> I: There are some buildings in the government quarter which were built recently [and are now regarded as insecure].
>
> A11: Yes, yes. But the question is which values do you have in these buildings - can you accept losing them? You can say "but we sit in those building, that is fine with us". The point is that you must make these value judgements.

When asked about the changing security assessment of the government quarter, A11 responded by asking whether there was a willingness to lose what was within those buildings; that is, lose the values.

P5 links this to uncertainty:

> P5: Greater uncertainty of course produces greater risk.
>
> I: You mean that if there is greater uncertainty, then the risk is also greater?
>
> P5: Yes, because then you don't know. But again, if you have the values, they often drive the result.

If the values are high, P5 reasons, the risk also becomes high, given the uncertainty. If you do not know (uncertainty) – what you (presumably) do know is the values. The clearest expression of giving values "absolute value" comes from A3: "There are some values that should be protected no matter what." A14 expresses this as an acceptance level: "You get kind of an acceptance level. If the value is low, then you can accept that the activity to protect it will also be low".

This reasoning poses a challenge. If low value implies low risk and high value implies high risk, and some values should be protected no matter what, this easily leads to an overload of (high) risks, with correspondingly high demands for security measures.

This troubling perspective may be the reason why conducting a thorough value judgement is regarded as key, to separate the important from the unimportant. Values must be sorted and scaled:

> A9: What do you really want to protect? Look at your values. How important are they to you? Why are they important? What harm and loss can you live with? Look at small bits at a time … .Make a judgement and sort values. It is extremely difficult but very, very important.

Through a thorough value judgement, A9 argues, key values can be discerned and prioritised. A key purpose of the value judgement is not only to identify everything valuable, but also to narrow down the critical value(s), so there is a distinction between (limited amount of) values needing security measures.

> M4: If you work in these professional processes, you'll actually discover that there are only these eight offices which have people performing critical societal functions … then it is the function [which is secured], that they should be able to sit safely and work even if something happens …

It is specific value judgements that are conveyed as the ideal: *these* eight offices, *that* power station, *this* microchip procurement. A prerequisite is the ability to distinguish between a limited number of "valuable" assets and less valuable ones that can be ignored in the risk assessment. The critical values may be foreseeable when it comes to offices. When it comes to matters such as digital value chains, however, which are often "complex, unclear, tightly connected and transnational" (DSB 2020, p. 8), identifying critical values is far more complicated and often unrealistic.

Summing up, values are key to the SRA, as the rest of the risk assessment takes them as its starting point. The SRA approach seems to represent a shift in attention and discourse in that more focus is directed towards internal matters. Values link the SRA to the general (corporate) governance, as security management becomes linked to key deliveries by the organisation. In case of uncertainty, some interviewees regard the values as "driving" the risk. To prevent overload, distinguishing between critical and less critical values thus becomes essential.

The normative judgement of sound (levels of) security

The SRA standard states that decision-makers should set an "acceptable security risk" (Standards Norway 2014, p. 7). Similarly, the Security Act pertaining to national security requires "sound" or "acceptable [levels of] security" (*forsvarlig sikkerhetsnivå*) (Norwegian Ministry of Justice and Public Security 2019, §4–3), hereafter called "sound security". What is to be achieved is thus not linked to a factual basis, to specific measures, but to a normative notion of "sound". It is abstract, open and normative.[6]

P3 expresses a sentiment shared by several interviewees about the introduction of "sound security" as a requirement:

> When the focus on risk-based security work increases, it will implicitly create more uncertainty … It creates more flexibility, but it also creates greater uncertainty when it comes to what is good enough … It's freedom with responsibility. You get more flexibility but it can also become a somewhat burdensome responsibility.

The flexibility is regarded as a positive, necessary development by some interviewees, enabling a targeted, sensible security approach. Others expressed frustration about the "soft", intangible character of the goal of "sound security". Linked to the Security Act, A14 sees the development as going from one hole (rule-based) to another:

> A14: We have come to a totally different place. But we have most likely got stuck in a different hole, too. If you look at the Security Act, it offers the hysterical solution that you say you need a … management system. That's ok … but then you [the government] has to describe where

> you want to go. You can call it a level of acceptance. You need to say something about how much security you want to have. The Security Act does not do that. It presents a functional demand labelled "sound security". It does not say anything about what sound security is. Then you're lost, you know. You never manage to grasp that concept … .
>
> I: What's the result then?
>
> A14: … It leaves a huge responsibility to each entity subject to the rules … . And they will end up giving different answers. Which means we will arrive at different levels of security. This is my most principled critique. The developers of the Act did not spend their time answering the question: How much security do we need?

A14 expresses frustration that what is considered to be sound security is not defined. This is left to each organisation to decide, giving "a huge responsibility" to the organisations subject to the Act. A14 also regards much responsibility being given to the security authorities, as they must express some kind of level of acceptance through their guidelines.

In the Security Act, much attention has been given to organising a structure of responsibility and auditing (NOU 2016, p. 19; Prop 153L (2016–2017)). The Act creates a top-down approach where the Ministries are responsible for pointing out fundamental national functions within their jurisdiction (§2-1 a) and designating entities subject to the Act (§1–3). The security authority (National Security Agency) is responsible for auditing, including auditing the Ministries and other auditing entities with security responsibilities (§3-1). The auditing is systems-oriented but can also use detailed recommendations from the security authorities as criteria when deemed appropriate.

The SRA standard arguably expresses a neutral position in the sense that "a high security risk can be accepted if the occasion, conditions, gain or costs indicate so" (Standards Norway 2014, p. 7) One can, in other words, choose to take high risk. However, as P3 said above, the responsibility for "taking risk" may become burdensome. M9 expresses a link between the normative requirement of "sound security" and the potential for blame:

> I: What does having "sound security" mean?
>
> M9: If something goes wrong, then you by definition have not acted "soundly". Then there's the guilt and shame and consequences and the full package.

To M9, "sound security" is linked to a potentially negative outcome, and the subsequent judgement of this outcome, which (s)he expects to be "blame".

Summing up, the requirement for "sound security" creates flexibility, but also responsibility. It is uncertain what is required, what is sufficient, with the corresponding potential for blame.

Discussion

The aim of anticipation

There is little doubt that interviewees perceive the changes since the turn of the millennium, and especially in the last decade, as profound, at least in terms of aspiration, tools and perspectives. The aim is a more analytical approach to PSM than a rule-based system. The attention given to analytical skills, academic qualifications, systematic method and to risk assessment as production of knowledge, all points to a discourse and aspirations resonating with Power's ideal model of anticipation.

The value-centred perspective also links it to anticipation, as identifying values in need of protection requires thorough analysis. Interviewees stress the need to pinpoint the most critical values, as everything cannot be valuable and in need of security measures. This again requires analysis of which objects are at risk, their criticality, interdependencies, etc.

Risk assessment is in part seen as about unpacking an objective, pregiven risk. By using the label "value", the SRA makes, however, explicit that it is also an *evaluation*. What is considered a risk depends on what is considered valuable. This challenges the distinction between analytical non-normative conduct (risk assessment) and normative choices, a tension well known to risk scholars (Lupton 2013). This study does not investigate actual evaluation processes. We may hypothesise, however, that the value-centric discourse conveys more directly risk as relational (Boholm and Corvellec 2011) and negotiated than when attention is on risk as an uncertain, external event (Aven and Renn 2010). The judgemental character is to some extent conveyed (i.e. A6 sees it as primarily a changing discourse), but also not, as much of the discourse links identifying "values" to analysis (unpacking, revealing, understanding).

Interviewees have argued that we need to anticipate our values ("ourselves") because they are what one can do something about. Whereas threats are uncertain and to some extent "destiny", one can, it is assumed, anticipate "oneself" and thus reduce vulnerabilities. Luhmann's (1993) distinction between "danger" (external, outside your decision making) and "risk" (internal, can be dealt with) is relevant. A value-centred approach, one may argue, internalises potential negative, future events, and makes them into risks in Luhmann's sense. The call to anticipate those things that one can do something about (oneself) is at the same time a "will to know" (anticipate) and a "will to decide and act" (Boholm and Corvellec 2011, p. 181).

The shift of attention towards values may reduce the importance of, and ambition to, anticipate the external world, the "enemy's actions".[7] It is a change in attention of the anticipation (more towards "oneself"), but it is still anticipation.

Resilience

When it comes to Power's understanding of resilience, the case partly resonates. In line with Power's perspective, attention is directed "inwards", towards one's values and vulnerabilities. At the same time, and contrary to Power's description, anticipation is, as described above, not given up.

A critical normative reading of resilience, often linked to an Anglo-American context, sees resilience as a neo-liberal withdrawal of the state (i.e. Brunner and Plotkin Amrami 2019), where security politics become a local and individualised matter (Berling and Petersen 2021). This understanding of resilience is not recognised in the case at hand. On the contrary, it is the burden of perceived (government) responsibility for creating security, not abdication, which is striking.[8] This may be seen both in view of the active role of the Norwegian state in general, but also in light of the 22 July 2011 terrorist attack. The attack put governmental responsibility for protective security measures on the political agenda, and made the domain of protection important and politicised.

The case also does not fit the polycentric and "organic" understandings of resilience (Rogers 2017, Bourbeau 2018). In the case at hand, the discourse is very much within the bounds of classical, hierarchical, top-down government.

Protection

To better understand what is at stake, and as an alternative to the diverse and contested concept of resilience, we propose to draw on the term "protection". Bigo (2002, 2009) has investigated discourses on and the etymologies of protection. One is linked to territory, to a clear-cut notion of inside/outside. Here, protection means excluding the enemy from the territory. Protection "involves someone else guaranteeing security and survival", but also the place defended "by a garrison" (Bigo 2009, p. 91). The enemy cannot infiltrate the safe garrison/territory because of protected borders (Bigo 2006, 2009). This links protection to the classical role of the state. Another protection discourse is more inward-looking, Bigo (2009) argues, and linked to vulnerability. Dangers are not clearly identified and thus it is best to reinforce protection by limiting the vulnerability of infrastructures. Here, a distinction is made between important and unimportant, and analysis is placed on the agenda.

In today's world, where the enemy is not clearly defined and the territory ceases to be demarcated, there is a development in the meaning of protection, Bigo (2009) argues, away from the idea of the state as a container, where society is enclosed by a territory, and contained by the state. The state as a defender of the territory struggles, as protection is no longer a battle, a fight. "Protection is about the capacity of the protector and not about the strength of the enemy … The real danger, if any, is inside" (Bigo 2009, p. 98). It is the performance of the protector which is at stake.

The role of the state as protector is precautionary and risk averse. In notions such as defence-in-depth security (Reason 1997), several layers of protective measures are implemented to create sufficient security. This creates a safe "inside", not of the country, but of the object at risk (building, infrastructure, ICT system).

A3's perspective that "some values should be protected no matter what" was referred to above, indicating strong levels of precaution and an unwillingness to take risk. We may note the "mode of disappointment" in Power's (2014) ideal model of resilience (valid also to protection), which is disaster. If disaster is at stake, there is little acceptance for risk-taking, for juggling different interests and norms, for cost–benefit judgements.

Bigo's description of protection can be viewed as an "idealised" version of protection as it unfolds in today's world. It sensitises us towards parts of the discourse on SRM that are linked to national security and the traditional role of the state as the guardian and defender of territory. It can also incorporate how this role is changing and struggling. As the state cannot (primarily) create security through traditional tools such as military defence, risk management becomes an alternative. But this poses a challenge, as there is an imbalance between security (protection) and risk (Søby Kristensen 2008). Protection is, at least in its idealised version, highly risk adverse. It is at odds with the "riskiness" of risk (Heyerdahl 2022).

In our case, attention to values and the risk-averse attitude resonate with the idea of protection. The potential disastrous consequences of insufficient security measures make PSM important in the perspective of the interviewees. It is however also daunting (how can we understand and secure everything critical in an interconnected and complex world)? The interviewees convey a mixture of hope (in risk management and professionalisation) but also great concern (difficulty, uncertainty and responsibility). In line with Bigo's description, it is the capacity of the protector to protect which is at stake and which troubles.

Summing up, the resilience concept is understood in a number of different ways, some of them intimately linked to an Anglo-American and neo-liberal political context. Our case may help differentiate and nuance by observing that parts of what is described as resilience may be developing (focus on vulnerabilities, survival, etc.), without the other interpretations (abdication of the state, non-hierarchical). We propose returning to ideas about protection as a core role of the state and regard this as a potential path for understanding how "security" may interact and shape SRM.

Auditability

Power's last ideal model of risk management logics is auditability. Does the case at hand resonate with this logic? Proponents of the SRA position it as a *reaction to* a rule-based and audit-oriented system. We may thus investigate whether and how the SRM resonates with the logic in different phases.

Auditability 1.0

As noted, traditional PSM was in many respects "audit-oriented". The "audit trail" was simple to identify and control. Matters were checked (was classified information stored in a certified safe?) and the answers were easy to interpret.

For many organisations, typically civil organisations with some national security functions, PSM was a limited affair. Rules regulated specific measures, and nothing more. Interviewees express that security management "lived" its life on the floor of the organisation, largely detached from the rest of the organisation. Consequently, security professionals often felt neglected, and security auditors felt they were not heard: "They [the leadership of organisations] thought we were totally irrelevant" (A2), a former security auditor says of the time before the terrorist attack in Norway of 22 July 2011. "No-one says that anymore", (s)he continues.

Although there was an "audit system", arguably it was not in line with a "logic of auditability" in Power's sense. Security management was not linked to something perceived as risk *to* the organisation. Unlike in Power's logic of auditability, the audit system originally had little transformative power in the organisations, at least the civil ones.

Auditability 2.0

If the ideal model of risk management as auditability is to resonate with the case at hand, this implies that auditing is a key organising principle. Although we cannot fully judge the question of the evolving PSM system pertaining to auditability, a few factors can be noted.

First, the focus on "values", we argue, links SRM with risk management in organisations at large. Investigating values invites self-examination and a need to make explicit what has often been implicit, unknown or taken-for-granted: What are we really delivering? What is critical to our goals? Do we understand interdependencies in our ICT systems? Power describes a need to "turn organisations inside out", linked to internal control

(Power 2007). Organisations cannot "just" "do their thing", they need to be able to express what is happening so the information can be externalised and judged. There is a similarity in the idea that one needs to know, express, evaluate and document one's values. Given the complexity and uncertainties relating to large organisations' whereabouts, deliveries and interdependencies, this is no easy task. It thus becomes important to analyse, express, document and make judgements about values. Given ambiguities, uncertainties and unknowns, and what is at stake, creating evidence of responsible conduct in auditable trails becomes, we may assume, important.

The value-centred approach, we argue, intimately links SRA with the management of the organisation at large. Security risks should no longer be something "for the security people"; they are a matter of strategic choice, leadership and goal achievement within the organisation itself. The link to the overall governance system of organisations is clearly reflected in the second Security Act described above, where a systems oriented, top-down auditing regime is implemented (Prop 153L (2016–2017)).

Second, Power expresses some key propositions regarding how "fast" the logic of the audit trail gains performativity (Power 2021). One is linked to the potential for blame: the "more … that organisational actors believe they face possible censure and blame, the more … they will embrace, elaborate, and amplify audit trails" (Power 2021, p. 22). After all, blame is the "mode of disappointment" for the auditability logic (Power 2014).

Creating (national) security is in general in the realm of potential blame. This has been clearly demonstrated in a Norwegian context in the aftermath of the terror attack in 2011, where much attention has been directed to questions of responsibility and blame (NOU 2012, Renå and Christensen 2020).

The requirement of the Security Act for organisations to define "sound security" is seen as offering additional potential for blame. There is an ambiguity in the meaning of "sound". Is it the judgement beforehand (prospective) that should be "sound", or the result retrospectively (Hardy *et al.* 2020)? The term "sound security" is Janus-faced, we argue, in that in the planning process, it implies flexibility and choice. It is not a requirement for security at any cost. The meaning may change, however, in the case of an incident: Something happened, "they" were responsible for sound security, eo ipso they did not do what they were supposed to have done. As M9 said above, a negative outcome is in itself not "sound". The normative requirement for sound security arguably implies that someone (a person, organisation, government) can always be regarded as responsible if something happens.

The Janus-faced nature of "sound security" makes it important, one may assume, to create an audit trail documenting a responsible process, as it can form a defence against blame if a disaster becomes the outcome.

Third, the difficulty involved in creating security may drive a process-focused, potentially audit-driven logic. Security requirements are often beyond the bounds of what is "reasonable" from all other perspectives other than that of security. It may thus become attractive, we may hypothesise, to "fulfil" the requirements of "sound security" through documenting the process and choose "doable" outputs as proxies for security (94% of our employees have taken the e-learning course on insider risks). The challenging characteristics of PSM, such as the requirement for "sound security", are thus, we may hypothesise, prone to "rituals of verification" (Power 1997).

Summing up, attention to values, a requirement of "sound security", and a systems-oriented auditing regime in a new Security Act, links SRM to governance systems at large and the responsibilities and accountability of organisations. Although we do not know how organisations will act on these requirements, we hypothesise that they facilitate an auditability logic.

Concluding remarks

Critical security scholars have discussed the value of security at length (Booth 1991, Buzan *et al.* 1998, Nyman 2016). The SRA approach comes prior to saying anything about what security is. It does not refer to anything outside of the evaluation, simply stating that the value (object at risk) is whatever is held to be of worth by the evaluator (Boholm and Corvellec 2011). It is a framework for analysis. Similarly, the notion of "sound security" lacks grounding in the concrete (we only know that it should be "sound"). When A14 describes going from one hole to a different one, s(he) describes going from over-specifying prescriptive rules) to under-specifying ("sound") security. Seen from the perspective of critical security theory, looking for normative implications of security policies, the approach is "empty". It does not say anything about what type of security (or society) one should aim at or what should be avoided. Drawing on the surrounding discourse and perceived aims of PSM, notable implications do, however, follow.

Initially, we asked how security professionals make sense of the SRA approach and what this can tell us about the use of risk assessment in PSM. We found that the professionals positioned the approach as more analytical than a prescriptive, rule-based system, with the aspiration to anticipate risk. The SRA discourse is thus intimately linked to the ideal model of anticipation, in its attention to analysis, systematic method and production of knowledge. It also resonates with the resilience model in the inward attention to values. The article suggests, however, that protection better conveys what is at stake than resilience. Lastly, the concept of "sound security" is interpreted as a burdensome responsibility for organisations with potential for blame, the mode of disappointment in the auditability logic.

Sensitising the case through the ideal models, two main conclusions may thus be drawn. One is the link to the role of the state as protector. This draws risk management in a risk-averse direction. Risk assessment as anticipation is in its classical form a "neutral" tool to juggle costs and benefits, where an incident is just an element in an undramatic calculation to optimise outcome. The SRA approach is as described above in one sense "neutral", but PSM has as its underlying premise that of creating protection. It is not neutral or indifferent if an incident occurs or not. On the contrary, it is potentially disastrous. The translation of risk assessment into the security context (Berling *et al.* 2021) attempts to take such security concerns into account. It is not clear what security is or should be, but it is risk-averse. This again could potentially lead to extensive security measures (Amoore 2013). One may argue that the discourse on the Norwegian SRA approach, not least through its value-centric perspective, makes a tension visible which will often be imminent in SRM; the tension between the idea of creating security, linked to the state's role as protector, and of risk management, creating flexibility to optimise outcomes.

The second conclusion is linked to responsible organisations and auditing. In this case, the requirement to create "sound security" makes responsible organisations the focal point of creating security. It is the organisation, or someone in the organisation, that makes the decisions on which security measures are deemed "sound". Sound security is not linked to concrete security measures. One does not know what is required in substance. This suggests that it is not concrete measures that can prevent blame, but an audit trail documenting a responsible process.

"Can we know the risks we face, now or in the future? No, we cannot; but yes, we must act as if we do" (Douglas and Wildavsky 1982, p. 1). Douglas and Wildavsky's chilling quote may give insight into a dilemma of relevance. The requirement of "sound security" may make organisations responsible for the future, although the future is unknown. "Responsibility" may be as important as "knowledge" in the management of risk.

The case shows the intricate and complex interplay between security and risk practices and discourses. Security studies may benefit from engaging with risk management literature, also the one leaning towards understanding "management" as much as "risk". Further investigation into the risk–security nexus, through interdisciplinary cross-fertilisation, is called for.

Notes

1. Standards Norway is the main standardisation organisation in Norway, a member of the International Organisation for Standardisation and the European Committee for Standardisation.
2. For the interviews conducted by Busmundrud *et al.* (2015), verified interview summaries were included in an appendix.
3. *Risk and Vulnerability Analysis*, The Emergency Planning College 24–26 September 2018, *Risk Assessment*, Norwegian National Security Agency (NSM) 18 September 2019, *Basic Preventive Security*, NSM 7–10 October 2019, *Security-Risk Analysis*, The Norwegian Business and Industry Security Council, 2–3 October 2019.
4. The Norwegian Defence Estates Agency and the Norwegian Defence Research Establishment both used risk-based approaches.
5. There are close links between security milieux/agencies and academia in other areas, such as physical security.
6. There are still a number of specific, prescriptive requirements in the Security Act on matters such as information security and personnel security (Norwegian Ministry of Justice and Public Security 2019).
7. Some interviewees see threat assessments as very important, but in general, more attention is directed towards values and vulnerabilities.
8. Discourses on resilience do exist in a Norwegian context (Berling and Petersen 2021), but not identified in the case.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Norwegian Research Council [grant number 271718]; Norwegian Ministry of Justice and Public Security.

References

Alvesson, M. and Sköldberg, K., 2018. *Reflexive methodology: new vistas for qualitative research*. 3rd ed. Los Angeles, CA: SAGE.

Amoore, L., 2013. *The politics of possibility: risk and security beyond probability*. Durham: Duke University Press.

Ansell, C. and Baur, P., 2018. Explaining trends in risk governance: how problem definitions underpin risk regimes. *Risk, hazards & crisis in public policy*, 9 (4), 397–430.

Aradau, C., 2017. The promise of security: resilience, surprise and epistemic politics. *In:* D. Chandler and J. Coaffee, eds. *The Routledge handbook of international resilience*. London: Routledge, 79–91.

Aradau, C. and Van Munster, R., 2007. Governing terrorism through risk: taking precautions, (un)knowing the future. *European journal of international relations*, 13 (1), 89–115.

Aven, T. and Renn, O., 2010. *Risk management and governance: concepts, guidelines and applications*: Berlin: Imprint: Springer.

Battistelli, F. and Galantino, M.G., 2019. Dangers, risks and threats: an alternative conceptualization to the catch-all concept of risk. *Current sociology*, 67 (1), 64–78.

Beck, U., 1992. *Risk society: towards a new modernity*. London: Sage.

Bengtsson, L., Borg, S., and Rhinard, M., 2018. European security and early warning systems: from risks to threats in the European Union's health security sector. *European security*, 27 (1), 20–40.

Berling, T.V. and Bueger, C., 2015. *Security expertise: practice, power, responsibility*. London: Routledge.

Berling, T.V., *et al.*, 2021. *Translations of security: a framework for the study of unwanted futures*. London: Routledge.

Berling, T.V. and Petersen, K.L., 2021. Designing resilience for security in the Nordic region: implications for strategy. *In:* S. Larsson and M. Rhinard, eds. *Nordic societal security*. London: Routledge, 131–153.

Bigo, D., 2002. Security and immigration: toward a critique of the governmentality of unease. *Alternatives*, 27, 63–92.

Bigo, D., 2006. Internal and external aspects of security. *European security*, 15 (4), 385–404.

Bigo, D., 2009. Protection: security, territory and population. *In:* J. Huysmans, A. Dobson, and R. Prokhovnik, eds. *The politics of protection: sites of insecurity and political agency*. London: Routledge, 84–100.

Bigo, D., Bonditti, P., and Olsson, C., 2010. Mapping the European field of security professionals. *In*: D. Bigo, S. Carrera, E. Guild, and R.B.J. Walker, eds. *Europe's 21st century challenge*. Farnham: Ashgate, 71–86.

Blumer, H., 1954. What is wrong with social theory? *American sociological review*, 19 (1), 3–10.

Boholm, Å and Corvellec, H., 2011. A relational theory of risk. *Journal of risk research*, 14 (2), 175–190.

Booth, K., 1991. Security and emancipation. *Review of international studies*, 17 (4), 313–326.

Bossong, R., 2014. The European programme for the protection of critical infrastructures – metagoverning a new security problem? *European security*, 23 (2), 210–226.

Bossong, R. and Hegemann, H., 2019. Internal security. *In:* D.J. Galbreath, J. Mawdsley, and L. Chappell, eds. *Contemporary European security*. Abingdon, Oxon: Routledge, 101–119.

Bourbeau, P., 2018. A genealogy of resilience. *International political sociology*, 12 (1), 19–35.

Brunner, J. and Plotkin Amrami, G., 2019. From the therapeutic to the post-therapeutic: the resilient subject, its social imaginary, and its practices in the shadow of 9/11. *Theory & psychology*, 29 (2), 219–239.

Busmundrud, O., *et al.*, 2015. *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger [Approaches to risk assessments for intentional adverse actions]*. Kjeller: Norwegian Defence Research Establishment.

Buzan, B., de Wilde, J., and Wæver, O., 1998. *Security: a new framework for analysis*. Boulder, CO: Lynne Rienner.

Ciută, F., 2009. Security and the problem of context: a hermeneutical critique of securitisation theory. *Review of international studies*, 35 (2), 301–326.

Charmaz, K., 2017. The Power of Constructivist Grounded Theory for Critical Inquiry. *Qualitative Inquiry*, 23 (1), 34–45.

Corry, O., 2012. Securitisation and 'riskification': second-order security and the politics of climate change. *Millennium*, 40 (2), 235–258.

Douglas, M. and Wildavsky, A., 1982. *Risk and culture: an essay on the selection of technical and environmental dangers*. Berkeley, Calif: University of California Press.

DSB (The Norwegian Directorate for Civil Protection). 2020. *Risikostyring i digitale verdikjeder. [Risk management in digital value chains]*.

Dunn Cavelty, M., Kaufmann, M., and Søby Kristensen, K., 2015. Resilience and (in)security: practices, subjects, temporalities. *Security dialogue*, 46 (1), 3–14.

Dunn Cavelty, M. and Søby Kristensen, K., 2008. *Securing 'the homeland': critical infrastructure, risk and (in)security*. London: Routledge.

Hardy, C., *et al*., 2020. Organizing risk: organization and management theory for the risk society. *Academy of management annals*, 14 (2), 1032–1066.

Heyerdahl, A., 2022. Risk assessment without the risk? A controversy about security and risk in Norway. *Journal of Risk Research*, 25 (2), 252–267.

Heyerdahl, A., n.d. Standardizing policy in a non-standard way – a public/private standardization process in Norway. *forthcoming*.

Hovden, J., 2004. Public policy and administration in a vulnerable society: regulatory reforms initiated by a Norwegian commission. *Journal of risk research*, 7 (6), 629–641.

Hutter, B. and Power, M., 2005. Organizational encounters with risk: an introduction. *In:* B. Hutter and M. Power, eds. *Organizational encounters with risk*. Cambridge: Cambridge University Press, 1–32.

Huysmans, J., 2009. Agency and the politics of protection. implication for security studies. *In:* J. Huysmans, A. Dobson, and R. Prokhovnik, eds. *The politics of protection: sites of insecurity and political agency*. London: Routledge, 1–18.

Jore, S.H., 2019. The conceptual and scientific demarcation of security in contrast to safety. *European journal for security research*, 4 (1), 157–174.

Jore, S.H., 2020. Is resilience a good concept in terrorism research? A conceptual adequacy analysis of terrorism resilience. *Studies in conflict & terrorism*. doi:10.1080/1057610X.2020.1738681

Larsson, S. and Rhinard, M., eds., 2021. *Nordic societal security: convergence and divergence*. London: Routledge/Taylor & Francis Group.

Luhmann, N., 1993. *Risk: a sociological theory*. Berlin: Wallter de Gruyter.

Lupton, D., 2013. *Risk*. 2nd ed. London: Routledge.

Maal, M., Busmundrud, O., and Endregard, M., 2016. Methodology for security risk assessments – is there a best practice? *In:* M. Revie, T. Bedford, and L. Walls, eds. *Risk, reliability and safety: innovating theory and practice*. London: Taylor & Francis, 860–866.

Neal, A.W., 2019. *Security as politics: beyond the state of exception*. Edinburgh: Edinburgh University Press.

Norheim-Martinsen, P.M., 2016. New sources of military change - armed forces as normal organizations. *Defence studies*, 16 (3), 312–326.

Norwegian Ministry of Defence. 2001. *Lov om forebyggende sikkerhetstjeneste [Security Act]*.

Norwegian Ministry of Defence. 2017. *Prop. 153L Lov om nasjonal sikkerhet [Security Act Proposal]*.

Norwegian Ministry of Justice and Public Security. 2019. *Lov om nasjonal sikkerhet [Security Act]*.

Norwegian National Security Authority, Norwegian Police Security Agency, and National Police Directorate. 2010. *En veiledning. Sikkerhets- og beredskapstiltak mot terrorhandlinger [Guideline to protective and preparedness measures against terrorism]*.

Norwegian National Security Authority, Norwegian Police Security Service, and National Police Directorate, 2015. *Terrorsikring. En veildning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger [Terror protection. A guideline in security- and preparedness measures against intentional unwanted actions]*.

NOU. 2000. *Et sårbart samfunn. [A vulnerable society]*. No. 24.

NOU. 2012. *Rapport fra 22. juli-kommisjonen [Report from the 22. July commission]*. No. 14.

NOU. 2016. *Samhandling for sikkerhet [Cooperation for security]*. No. 19.

Nyman, J., 2016. What is the value of security? Contextualising the negative/positive debate. *Review of international studies*, 42 (5), 821–839.

Olsen, O.E., Kruke, B.I., and Hovden, J., 2007. Societal safety: concept, borders and dilemmas. *Journal of contingencies and crisis management*, 15 (2), 69–79.

Petersen, K.L., 2012. Risk analysis – a field within security studies? *European journal of international relations*, 18 (4), 693–717.

Pettersen Gould, K.A. and Bieder, C., 2020. Safety and security: the challenges of bringing them together. *In:* C. Bieder and K.A. Pettersen Gould, eds. *The coupling of safety and security: exploring interrelations in theory and practice*. Cham: Springer International Publishing, 1–8.

Power, M., 1997. *The audit society: rituals of verification*. Oxford: Oxford University Press.

Power, M., 2007. *Organized uncertainty: designing a world of risk management*. Oxford: Oxford University Press.

Power, M., 2014. Risk, social theories, and organizations. *In:* P. Adler, P. du Gay, G. Morgan, and M. Reed, eds. *The Oxford handbook of sociology, social theory, and organization studies*. Oxford: Oxford University Press, 370–392.

Power, M., 2016. Introduction. *In:* M. Power, ed. *Riskwork: essays on the organizational life of risk management*. Oxford: Oxford University Press, 1–25.

Power, M., 2021. Modelling the micro-foundations of the audit society: organizations and the logic of the audit trail. *Academy of management review*, 46 (1), 6–32.

Reason, J., 1997. *Managing the risks of organizational accidents*. Aldershot: Ashgate.

Renå, H. and Christensen, J., 2020. Learning from crisis: the role of enquiry commissions. *Journal of contingencies and crisis management*, 28 (1), 41–49.

Rogers, P., 2017. The etymology and genealogy of a contested concept. *In:* D. Chandler and J. Coaffee, eds. *The Routledge handbook of international resilience*. London: Routledge, 13–25.

Rosenberg, M.M., 2016. The conceptual articulation of the reality of life: Max Weber's theoretical constitution of sociological ideal types. *Journal of classical sociology*, 16 (1), 84–101.

Salter, M.B. and Mutlu, C.E., 2013. *Research methods in critical security studies: an introduction*. London: Routledge.

Søby Kristensen, K., 2008. 'The absolute protection of our citizens': critical infrastructure protection and the practice of security. *In:* M. Dunn Cavelty and K. Søby Kristensen, eds. *Securing 'the homeland': critical infrastructure, risk and (in)security*. London: Routledge, 63–83.

Standards Norway, 2012. *NS 5830 Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi [Societal security. Protection against undesirable intentional actions. Terminology]*.

Standards Norway. 2014. NS 5832 Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse [Societal security. Protection against intentional undesirable actions. Requirements for security risk analysis].

Stranden, R., 2019. *Sikring: en innføring i teori og praksis. 1. utgave*. Oslo: Gyldendal.

Taylor, T., 2012. The limited capacity of management to rescue UK defence policy: a review and a word of caution. *International affairs*, 88 (2), 223–242.

Timmermans, S. and Tavory, I., 2012. Theory construction in qualitative research: from grounded theory to abductive analysis. *Sociological theory*, 30 (3), 167–186.

Tjora, A., 2018. *Qualitative research as stepwise-deductive induction*. London: Routledge.