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

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 e*valuation.* 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 – meta-governing 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.