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 (2021): Risk assessment without the risk? A controversy about security and risk in Norway, Journal of Risk Research, DOI: 10.1080/13669877.2021.1936610

To link to this article: https://doi.org/10.1080/13669877.2021.1936610

Published online: 14 Jun 2021.

JOURNAL OF RISK RESEARCH
https://doi.org/10.1080/13669877.2021.1936610

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.