FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme / specialisation: Risk analysis and Governance	Spring semester, 2023 Open access

Author:

Filip Ærø Haugesten

Supervisor at UiS:

Frederic Bouder

Thesis title:

Threat communication grounded in science: Bridging the gap between Intelligence public threat communication and Risk science

Credits (ECTS): 30

Keywords: Public Risk Communication, Risk Science, Intelligence, Threat Communication, National Security, The Norwegian Police Security Service, Politiets sikkerhetstjeneste, PST, The Norwegian Intelligence Service, Etterretningstjenesten, NIS	Pages: 73 + appendix: 1 Stavanger, *28.08.2023*

University
of Stavanger

Filip Ærø Haugesten

Threat communication grounded in science

Bridging the gap between Intelligence public threat communication and Risk science

Risk Analysis and Governance, Master’s thesis

Faculty of Science and Technology

Stavanger 2023

Acknowledgement

I would like to express gratitude to my supervisor, Frederic E. Bouder. Other than being a kind and welcoming person, your critique has been thorough and concrete. Your flexibility has gone way beyond what one could expect, working around my day job and family life. I would also like to express my appreciation to my wife because my studies has occupied time we could have spent together. Thank you for supporting me and, most of all, pushing me when it was needed.

As I am writing these last words of my thesis, I realise that I stand as a slightly different man than when I started the master's programme in 2020, not only because of the new insights and wonderful people at the university, but also because I have gotten the privilege to become a father along the way.

Tuva, your smile and presence has been a most appreciated digression throughout this process. I look forward to not only invest time into my own learning, but also more time into your learning.

Abstract

In recent years, Norwegian intelligence agencies have communicated intelligence to the public as part of their threat communication programme. After several terrorist acts, the public discourse has raised concerns regarding the success of the intelligence threat communication. Because the field of public threat communication is a rather new intelligence practice, this thesis aims to compare the contemporary approach to the risk communication field. The data were collected by triangulation of observation, collection of online communication and qualitative interviews. The interviews were carried out with four intelligence employees in the Norwegian Police Security Service and the Norwegian Intelligence Service, in addition to two journalists from national news media. The contemporary intelligence approach gives little weight to uncertainty and supportive evidence because of the need to protect their sources, capabilities and methods. Furthermore, a dissented practice on whether probability should be communicated to the public was found. When probability was communicated, this was done in an inconsistent and ineffective manner, promoting ambiguous interpretations by the recipients. This thesis presents several recommendations for bridging the gap between the contemporary intelligence approach and risk science. The risk science approach gives more weight to uncertainties, portrays probability in a more consistent manner and suggests a deeper understanding of how the intended audience perceive the risks.

List of contents

List of Abbreviations

PST – The Norwegian Police Security Service

NIS – The Norwegian Intelligence Service

9/11 – Terrorist attack in New York City on September 11th 2001

NATO –The transcontinental military alliance *North Atlantic Treaty Organization*.

OSINT – Intelligence collection discipline known as *open source intelligence*.

HUMINT – Intelligence collection discipline known as *human intelligence*.

List of Figures and Tables

1 INTRODUCTION

> The task of communicating Intelligence to decision makers involves a great deal of judgement and a high degree of emotional detachment and honesty on the part of the Intelligence Community. Assumptions must be made explicit. The quality and freshness of the information must be revealed. Limitations in collection and analysis must be outlined. Conclusions must be well supported and well reasoned. (Kennedy, 2008, p. 124)

The above quote highlights many of the challenges in communication of intelligence to the intended receiver. The intelligence community has historically held a position of secrecy (Phythian & Gill, 2013), and this is perhaps why some of the more known examples of intelligence communication is the failures that lead to public interest and scandals. In the early 2000s, the intelligence agencies in the United States were under public scrutiny after the terrorist attacks in New York in 2001 (9/11) (Hatlebrekke, 2021). One of the identified intelligence failures leading up to 9/11 was the lack of communication between intelligence agencies and decision makers. The problematic 'need to know' culture prohibited the important flow of information that could have given decision makers better knowledge prior to the attack (Hatlebrekke, 2021). The communication phase of the intelligence process is called *dissemination* and is often seen as the Achilles' heel of intelligence (Hatlebrekke, 2021, p. 219; Herman, 2009, p. 45). The 9/11 example represents one aspect of dissemination, which includes communication with a decision maker, policy regulator, or other branches of government. Another aspect of dissemination is the newly taken path of *public* intelligence communication. The audience is no longer a national security decision maker but rather laypeople from all walks of society. Furthermore, in what way is the Achilles's heel of intelligence affected when the intended audience is without sector-related knowledge and experience?

Increased public openness and transparency of the intelligence community is an evident trend in Norway (Evalueringsutvalget, 2020). Both the Police Security Service (PST) and the Norwegian Intelligence Service (NIS) have released a public version on their annual threat assessment from 2004 and 2011, respectively. However, several recent events have brought forth a discussion as to the success of such public communications. On August 10, 2019, a solo-terrorist killed his sister and preceded to drive to a nearby mosque in Bærum, Norway, where he opened fire. The perpetrator was quickly overpowered by people from the mosque, leaving no further casualties. According to himself, he was motivated by a prior right-wing terrorist attack in Christchurch, New Zealand (Evalueringsutvalget, 2020). Prior to the Bærum attack, the government intelligence agency responsible for assessing domestic threats (PST) had assessed right-wing terrorist threats to have increased after the events in Christchurch. Consequently, the assessed probability for a right-wing attack was raised from ‘unlikely’ to ‘even chance’. However, the increased probability was not communicated to relevant groups in society and the public (Evalueringsutvalget, 2020). PST was criticised on multiple aspects, first for the presentation of probability judgements to lay people. It was argued that the audience had few prerequisites to interpret the full meaning of linguistic expressions such as ‘Highly unlikely’ (Evalueringsutvalget, 2020, p. 85). Second, there was found to be a lack of targeting relevant audiences in their public communication (Evalueringsutvalget, 2020, p. 12). Questions concerning the success of the current risk communication approach of PST was raised again after yet another presumed[1] solo-terrorist attack in Oslo in the summer of 2022. The director of the PST stated that *threat communication* is an area they find especially demanding and wanted the mandated commission to address this issue (25. juni-utvalget, 2023, p. 181). The following commissions report addressed several aspects of communication, but few seemed to ask if some of the answers can be found in risk science. Certain scholars in risk science, such as Aven (2020), have also criticised intelligence services for their public risk communication in events such as terrorist attacks. Aven’s reasoning was based on the notion that the public is not given the proper explanation regarding the background knowledge the judgements are based on. Aven argued that successful risk communication is hard to achieve when such crucial aspects of the risks are withheld (2020, pp. 151-152).

The Norwegian intelligence community has recent published articles, doctrines, assessments and information about their methodology. This gives us a better picture of their approach and the conditions surrounding their work. However, there is inadequate research as to the fundamental principles of what the intelligence-based public threat communication is founded on. Though public risk communication seems as a fairly new strategy for intelligence agencies, these issues has been under steady development over the last 40 years in risk science (Balog-Way et al., 2020; Bouder, 2015; Fischhoff, 1995; Leiss, 1996). The present

[1] The attack is still pending investigation at the time of writing this thesis.

thesis will therefore aim to compare the contemporary intelligence approach with the risk science approach. The objective of the present thesis is to investigate the following:

> *How does the public risk communication approach in the National Police Security Service and the Intelligence Service conform or depart from risk science?*

1.1 Limitations and terminology

The theoretical foundation for the present thesis is within the scope of risk science with a specific focus on developments within risk communication. The broader scope of communication, such as literature on communication strategy, psychology, marketing and so forth are not specifically addressed in the current thesis due to thesis limitations.

Risk communication and *threat communication* are two terms that will be referred to throughout the present thesis. This thesis takes the risk science view, meaning that threat is defined as a specific type of risk source (see Aven, 2020; SRA, 2018b). In this view, *risk* communication and *threat* communication have a similar meaning with the distinction that risk can be applied in a broader context, whereas threat is delimited to deliberate actions with malicious intent (see Jore, 2017). Therefore, the present thesis will mostly use the term *risk communication*. The intelligence practitioners—and the public discourse surrounding them—apply the term *threat communication.* Therefore, this term will also be applied in contexts of statements from informants or times when contemporary intelligence practice is addressed.

1.2 Thesis outline

In chapter two, there will be a literature review to outline the key aspects of risk science, as well as a presentation of the Intelligence field. A best practice approach to public risk communication, founded in risk science, will be presented and justified. In chapter three, the thesis research design and data collection will be presented, followed by discussion of reliability, validity and research ethics. The results of the study will be thematically presented according to the respective data collection method in chapter four. In chapter five, the results will be discussed based on the presented literature review, bridging the gap between the contemporary intelligence approach and the risk science approach, including recommendations and limitations. In chapter six, the present thesis will conclude the study by outlining the deviating and conforming nature of the intelligence approach in relation to risk science, and how this can be further applied.

2 LITERATURE REVIEW

The field of risk analysis has been under steady development throughout the recent years, shedding new lighting on issues such as how risk can be understood and applied in relation to the aspect of uncertainty (see. e.g. Aven, 2020). This theoretical section will start with the fundamentals of risk science, followed by academic literature and empirical descriptions of intelligence. The last part will concentrate on public risk communication, thematically divided into elements of best practice principles according to Bouder (2009).

2.1 Risk science

> The risk science covers risk understanding, risk assessment, risk characterization, risk communication, risk management, risk governance, and policy relating to risk, in the context of risks which are a concern for individuals, public and private sector organizations, and society at a local, regional, national or global level (Aven, 2020, p. 34).

There is an ongoing discussion to recognise the field of risk analysis—or rather risk science—as a scientific field and separate science discipline (Aven, 2020, p. viii). However, scholars such as Terje Aven have argued that the systematic developments, including publications, professorships and so forth, in the risk field over the last 40 years deem it necessary to recognise the field as a new science (Aven, 2018, 2020; Thekdi & Aven, 2021). The present thesis adopts the view of Aven that the risk field can be seen as a distinctive science, so the term *risk science* will be further applied throughout the thesis.

Aven (2020) stated that risk science activities can produce two separate types of knowledge. Type A knowledge relates to how risk science is applied in specific areas. This could be how a risk assessment is conducted within a certain field or how a certain sector handles risks. Type B knowledge relates to how risk science can be used to form universal methods, definitions, frameworks and so forth. Type B knowledge is often derived from Type A knowledge and seeks to enhance development of concepts and fundamental understandings for further applications (Aven, 2020, pp. 29-35).

In risk science there is a distinction between the terms *safety* and *security.* The two fields are generally viewed as two separate disciplines when it comes to research and the development of managerial tools and viewpoints (Jore, 2017; Piètre-Cambacédès & Bouissou, 2013). According to Jore (2017, p. 160), security issues relate to deliberate actions with malicious intent, whereas safety issues relate to matters that are unintentional, such as accidents. Jore (2017) argued that malicious intent is the essential factor in security related issues, and this is why security organisations often find themselves within typical governmental jurisdictions (e.g., criminal acts, terrorist attacks etc.) (Jore, 2017). The safety field has had more research and development throughout the past 20 years, so the degree of transferrable methods has been rather one-sided with practitioners from the security field adopting methods from safety (Piètre-Cambacédès & Bouissou, 2013). Piètre-Cambacédès and Bouissou (2013) argued that there is a bigger potential for a more collective methodology between the disciplines and that the safety field can also learn and adopt methods from security, despite their different natures.

The variations as to how the concept of risk is understood and described has implications for risk analysis and, subsequently, how risks are managed by decision makers (Aven, 2020, p. 63). Jore (2017) stated that safety issues often relate to an organisation's ability to balance risks and profit. Research within safety shows a close link to organisations and production of certain products that are often produced under hazardous conditions such as the oil and gas industry or nuclear energy. There are more observable and/or historical data contributing to making the risks more predictable and stable because most hazards relate to the production line (e.g., component failure, gas leak, etc.) (Jore, 2017). On the other hand, risks and threats relating to security are affected by factors outside organisational control, thus being more unpredictable and less controllable. Unknown threats can emerge at any given time with intent to cause harm (Jore, 2017; Piètre-Cambacédès & Bouissou, 2013). Facing threats such as criminality, terrorism and cyber-attacks, one must often rely on knowledge gained through intelligence services (Jore, 2017).

Within risk science, there are arguably different ways of understanding *risk* and its components. Over the past 30 years, the predominant way of defining risk has been to view it as merely a combination of probabilities and consequences, and in many ways, this is still a dominating viewpoint among lay people (Aven & Ylönen, 2018; Hrudey et al., 2011, p. 6). Many attempts have been made to give risk a unified definition, and there remains a broad consensus for a single definition (Aven, 2020, p. 147). However, there are certain components to risk that has a broad acceptance within the risk science field. Aven (2020, pp. 57-59) referred to *the risk concept,* highlighting that risk is based on two main components. The first component is *consequences* (linked to something we value), and the second is *uncertainty* (possibility or potential), often relevant to an activity or event. Hence, the risk concept can be described as follows: A (activity), C (consequences) and U (uncertainties) (Aven, 2020, p. 58). According to *the risk concept*, there will always be uncertainties when dealing with risk, and one must consider how big or small the uncertainties linked to a specific risk are (Aven, 2020).

In its broadest sense, the concept of *threat* in risk science is viewed as simply a risk source that is most commonly applied in security related settings (Aven, 2020; SRA, 2018b, p. 7). Other scholars such as Meloy and Hoffmann (2014, p. 3) emphasised a more narrow view of threat as ‘the perceived possibility of harm’ and also links threats to the malicious intent to harm someone or something of value. With reference to the field of security, we understand *security risk management* as ‘assessing and reducing the likelihood and consequences of possible attacks with various types of risk-reducing measures, for example, through critical infrastructure protection and by building organisational and societal resilience’ (Jore, 2017, p. 170).

2.2 Intelligence

The use of intelligence dates far back into human history and written text, and scholars noted that intelligence collection dates back as far back as the writing of the Bible, where, in Numbers 13, we can read about Moses, who dispatched spies to investigate the Canaans’ strengths and weaknesses (Gill & Phythian, 2018; Stenslie et al., 2019). Within the last decade, the development of intelligence has seen a rapid development not only in methodology, but also in the use of intelligence networks and structures across international borders. This development is the result of several wars and conflicts dating from World War I to the ‘war on terror’ in the early 2000s (Gill & Phythian, 2018).

There remains a consensus, both in academia and practitioners, regarding how intelligence should be defined (Stenslie et al., 2019; The Norwegian Armed Forces, 2021). However, for the present thesis, we will use the definition of intelligence used by the NATO military alliance:

> Intelligence is the product resulting from the directed collection and processing of information regarding the operating environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision makers (The Norwegian Armed Forces, 2021, p. 18).

There is little empirical evidence as to how most intelligence agencies view concepts such as risk and threat. However, PST openly discussed their understanding of a set concepts in their annual threat assessment. PST stated that they view risk as a combination of *assets*, *threats* and *vulnerabilities* as shown in Figure 1 (PST, 2023). This view on risk corresponds with the NS 5832-standard called '*National security risk management in relation to protection against intentional undesirable actions'* (NS 5832:2014). This conceptual understanding of risk and threat is commonly applied in security contexts (Aven, 2020).

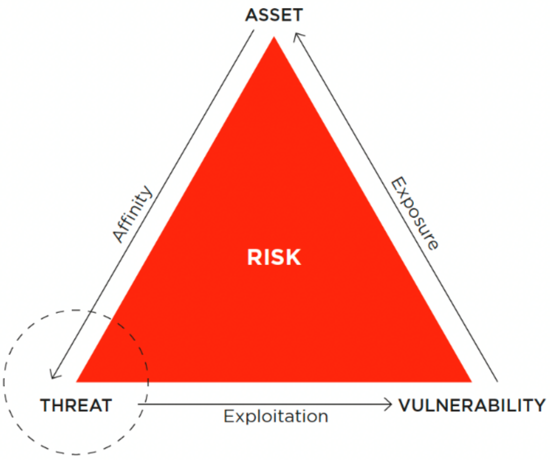


Figure 1. Visualisation of threat in relation to risk. Reprinted from PST (2023, p. 2)

Much of intelligence analysis focuses on threats and is based on the work of Davis Singer (Vandepeer, 2011). Singer published a model for threat analysis in 1958 in his article 'Threat-Perception and the Armament-Tension Dilemma', which he called a 'quasi-mathematical' model (Singer, 1958, p. 94): *Threat-perception = Estimated capability x Estimated Intent*. Stinger's model has been predominant for the past 60 years within threat analysis in the intelligence sector (Vandepeer, 2011), even though some intelligence agencies have later added *freedom of action* as being a third component of threat perception (The Norwegian Armed Forces, 2021, p. 71).

Vandepeer (2011) stated that there has been a notable shift of focus within the national security branch and intelligence agencies. Before the Cold War, the primary focus of strategic intelligence was threats posed by other states. Since then, the threats of nonstate actors has also risen to be a strategic priority in national security. For instance, this could be the terrorist groups and/or individuals targeting critical infrastructure or planning mass causality attacks. In particular, the terrorist attack on 9/11 has led to extensive development in intelligence gathering and management of nonstate threats in Western societies (Vandepeer, 2011).

2.2.1 Intelligence as a cyclic process

The definition of intelligence is understood and referred to as a cyclic process, known as the *intelligence cycle*. The intelligence cycles of Western society organisations are generally in accordance with each other in terms of process and key aspects, even though there are some variations as to how many steps the cycle has (see, e.g., Davies et al. (2013, pp. 58, 63, 64); Phythian (2013, pp. 1-4); Stenslie et al. (2019, p. 23); The Norwegian Armed Forces (2021, p. 42)).

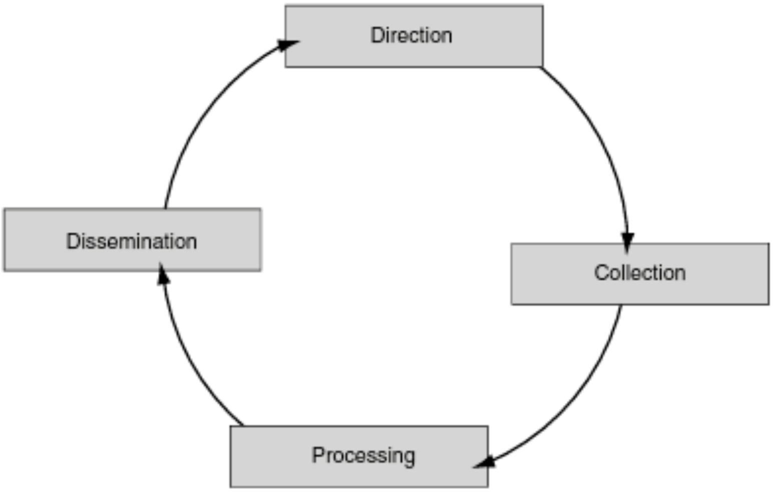


Figure 2. Traditional generic intelligence cycle. Reprinted from Davies et al. (2013, p. 58)

(1) The **direction** phase is the basis for the intelligence cycle. The 'customer' (e.g., decision maker) requests intelligence on a certain target or topic and gives direction on the type of decision support that is needed (Buckley, 2013; Phythian, 2013). The following phase is where information and data are **collected** (2). This is collected from different sources, commonly known as various 'INTs'. One example of such INTs is *open source intelligence* (OSINT), which is information that is publicly accessible, such as information on the internet

(Gill & Phythian, 2018). Another example is *human intelligence* (HUMINT), which is information gathered by someone gaining access to documents or photographs, information gained through informants, or information from other personnel (Gill & Phythian, 2018). (3) The **processing** phase is where the information is sorted and processed and then later analysed (Phythian, 2013).[2] (4) The **dissemination** phase is where the finished product is delivered to the decision makers who ordered the intelligence product (Phythian, 2013). In this phase, the product is communicated and distributed to people who can utilise the intelligence (Buckley, 2013; The Norwegian Armed Forces, 2021).

2.2.2 Intelligence communication of probability and uncertainty

> The most consequential decisions leaders make… are mired in uncertainties not only reflecting what is unknown but also what is unknowable, such as the intentions of others who may not have made up their own minds (Mandel & Irwin, 2021, p. 1)

One of the early pioneers of intelligence analysis, Kent Sherman, laid the ground work for today's practise regarding the presentation of judgements on uncertainties and probabilities in intelligence (Mandel & Irwin, 2021). Sherman highlighted that the use of terms such as *certain* or *almost certain* are judgements or estimates made by the analyst and, therefore, reflect probability and uncertainty. Furthermore, Sherman (1964) made the case for putting these judgements in a systematic categorisation. Mandel and Irwin (2021) stated that most methods for uncertainty communication in modern day intelligence use a variant of Sherman's model, where there is a linguistic judgement on certainty/probability, combined with a numeric probability interval (see Figure 3).

[2] Some organisations, for example the FBI (Buckley, 2013) have divided this phase into two separate phases, making the distinction between *processing* and *analysis*.

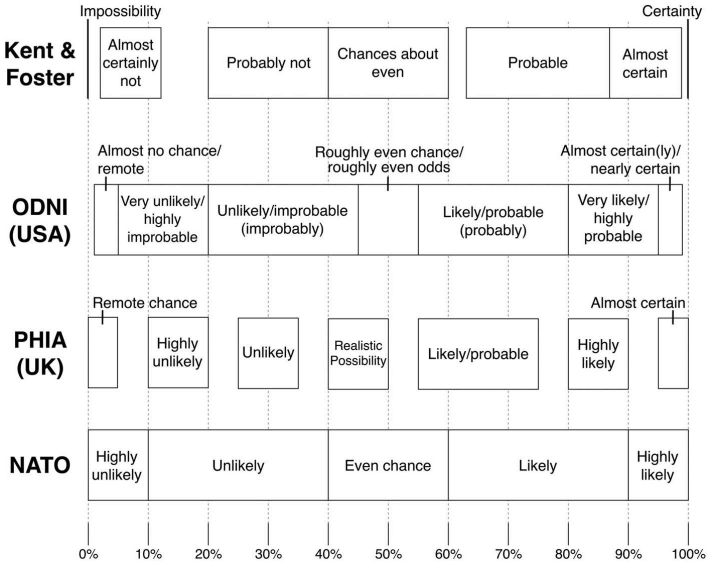


Figure 3. Various models for communicating judgements on probability/certainty. Reprinted from Mandel and Irwin (2021, p. 560).

In Norway, the official institutions that deliver intelligence (such as PST and NIS) use the NATO variant, and this has been implemented as a national standard (Evalueringsutvalget, 2020, p. 85). The purpose of using the standardised probability terms is to reduce the level of uncertainty to the reader (The Norwegian Armed Forces, 2021). Mandel and Irwin (2021) criticised the contemporary approach of utilising these types of probability models, specifically how it is utilised to communicate probability and uncertainty to decision makers. Mandel and Irwin (2021, pp. 561-563) argued that linguistic probability expressions are vague and full of implicit meanings. Numeric probability, on the other hand, is easier to understand and is less affected by personal interpretations and context. Hence, an alternative model for communicating probability to decision makers has been suggested, where there is given a numerical probability interval along with a written explanation (Mandel & Irwin, 2021).

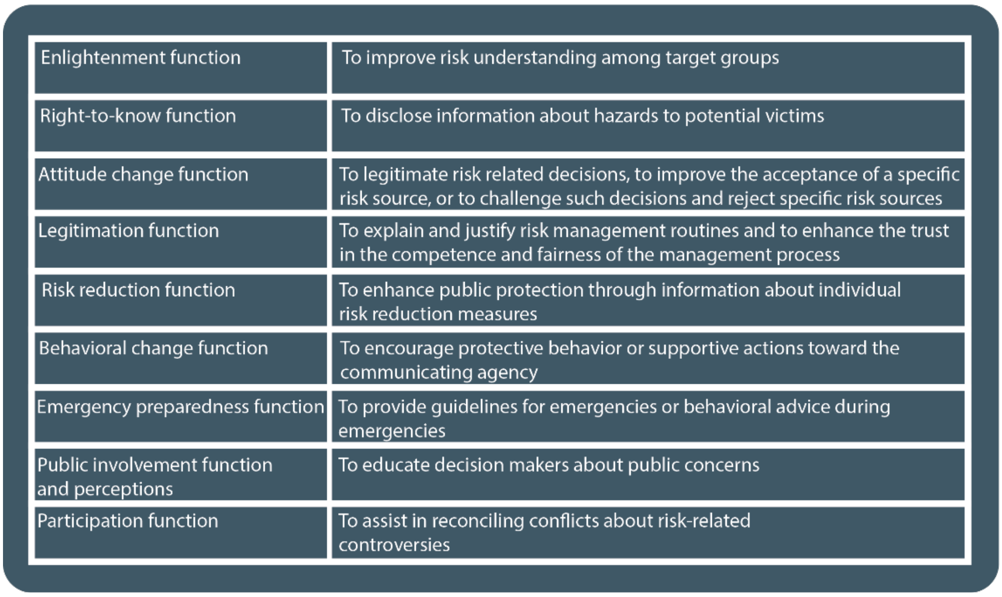
2.2.3 The purpose of intelligence

In a security risk management setting, intelligence can have multiple purposes. Omand (2010, p. 24) highlighted the fact that intelligence can improve the decision-making process by reducing the level of uncertainty for the decision maker and that this can be done in three different ways. For one, intelligence can enhance the decision makers' *situational awareness*. This gives relevant information about the characteristic of a certain situation, providing background knowledge and insights to questions such as who, what, where and when (Omand, 2019). This type of intelligence can provide both facts and information with various degrees of uncertainty, for instance, gathered from intelligence operators (Omand, 2019). The second type of decision support intelligence can provide is of an *explanatory* nature. This includes giving the receiver a reason for why the situation is at its current state, hence assessing and provide sensemaking to why some things are happening. For instance, if we have a sudden decreasing crime rate in a certain area, this could mean several things. It could be the result of decreasing police activity in that area, providing less police (self-)reported crime. It could also be the result of a decreasing trust between the residents and police, resulting in less reported crime from the public. Third, the police activity in that area could have given the incentive for criminals to shift their criminal activity to some other area. Omand (2019, p. 36) described that the intelligence must interpret what we are seeing and be based on the information available. In that sense, intelligence analysts have been weighing multiple hypotheses against each other. Further, Omand (2019, p. 36) stated that the third way of reducing uncertainty with intelligence is with the provision of *prediction.* This gives the decision maker a prediction of how the situation will evolve and will often include probability judgements on certain scenarios (Omand, 2019).

2.3 Risk communication

Ortwin Renn stated that ‘effective communication has to be at the core of any successful activity to assess and manage risks’ (2008, p. 201). We can define risk communication as ‘the flow of information and risk evaluations back and forth between academic experts, regulatory practitioners, interest groups and the general public’ (Leiss, 1996, p. 86). When communicating risk science, the terms and challenges presented are often of a technical or industry specific nature (Covello et al., 1986). When communicating risks in such a technical field, one can face challenges when trying to reach a common understanding, which is one of the main barriers in risk communication (Fischhoff, 2013). The goal of risk communication is simply not for all parties to agree on the most suitable decision but rather to find common ground as to relevant facts, risks and possible cost/benefit. Risk communication seeks to enlighten the intended recipient about the risks so that they understand the supporting evidence and can make a balanced decision (Fischhoff, 2013; OECD, 2002; Renn, 2008, 2010). Renn and Levine (1991) stated that there are several different functions risk communication can fill, as seen in Table 1. Hence, an evaluation of risk communication must be seen in conjunction with the intended function (Aven & Thekdi, 2021; Renn & Levine, 1991)

Table 1. Risk communication functions, reproduced from Renn and Levine (1991, p. 178)



Enlightenment function	To improve risk understanding among target groups
Right-to-know function	To disclose information about hazards to potential victims
Attitude change function	To legitimate risk related decisions, to improve the acceptance of a specific risk source, or to challenge such decisions and reject specific risk sources
Legitimation function	To explain and justify risk management routines and to enhance the trust in the competence and fairness of the management process
Risk reduction function	To enhance public protection through information about individual risk reduction measures
Behavioral change function	To encourage protective behavior or supportive actions toward the communicating agency
Emergency preparedness function	To provide guidelines for emergencies or behavioral advice during emergencies
Public involvement function and perceptions	To educate decision makers about public concerns
Participation function	To assist in reconciling conflicts about risk-related controversies

As shown in Figure 4, Frederic Bouder (2009) developed five procedural principles for public risk communication. The principles are based on 40 years of risk communication research (Bouder, 2015, p. 10) and represent a collection of best practices. The development of the principles were with contributions from leading scholars and practitioners within the field and had the backing of the *UK Government Office for Science*, as well as *the Economic and Social Research Council* and *the Risk and Regulation Advisory Council* (Bouder, 2009, p. 3). The principles can serve as a framework for public risk communication, and the present thesis has adopted the view where the principles are seen as a holistic approach to public risk communication and are applicable across multiple fields where risks are communicated to the public.

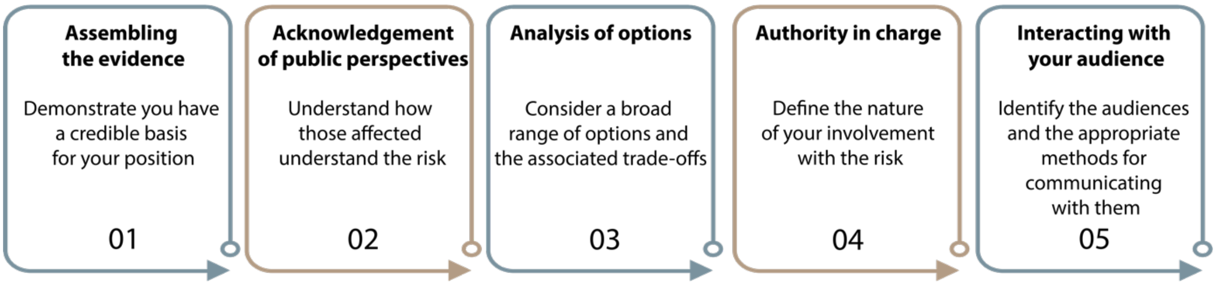

Assembling the evidence
Demonstrate you have a credible basis for your position
01
Acknowledgement of public perspectives
Understand how those affected understand the risk
02
Analysis of options
Consider a broad range of options and the associated trade-offs
03
Authority in charge
Define the nature of your involvement with the risk
04
Interacting with your audience
Identify the audiences and the appropriate methods for communicating with them
05

Figure 4. Key elements of public risk communication, reproduced from Bouder (2009, p. 4).

2.3.1 Assembling the evidence

Assembling the evidence means that there has to be sufficient collection of data and evidence to understand the risks, the associated uncertainties and possible hazards that can emerge

(Bouder, 2015). The goal is to demonstrate that the risks are understood and that decisions are based on sufficient evidence (Bouder, 2015). The background knowledge is an expression for the underlying data and presuppositions used in the analysis, such as historical data, knowledge of phenomena and assumptions made (Flage & Aven, 2009, p. 11). *Uncertainties* is an expression for the *lack* of knowledge, either linked to the activity itself or the consequences it may have (Flage & Aven, 2009, p. 11). For instance, if we are given the task of assessing the risks linked to a new food additive, the potential consequences could range from a great deal of public health issues, on the one hand, to no reported issues, on the other hand. There are uncertainties linked to the new food additive that influence our decision making. This could be that the additive has never been tried on humans before in a large scale, short-term versus long-term implications and so forth.

Bouder (2009, p. 2) stated that risks that affect the public (e.g., disease, climate change, etc.) impose implications for policy making and regulation. Moreover, if public risks are neglected and miscommunicated by government, an increase in distrust between the public and regulators may arise. The BSE[3] scandal in the UK is an example of such faulty risk communication (Bouder, 2009; Jensen, 2004; Löfstedt, 2005). The risk of BSE being transmittable to humans was not communicated to the public, even though there was signs of possible cross-species contamination (Löfstedt, 2005). The BSE case is interesting in evaluations of risk communications because it highlights several complications that can arise in risk management. First, the underlying risk assessments were unclear and ambiguous regarding the probability of BSE being transmittable to humans (Jensen, 2004). There was a great deal of uncertainties not properly addressed. For instance, the probability was reported in terms like 'remote', but there were also recommendations for precautionary measures (Jensen, 2004). Second, the designed risk communication based on the risk assessment further amplified the short comings of the risk assessment, failing to communicate information about the uncertainties (Jensen, 2004; Miles & Frewer, 2003).

Addressing uncertainties in risk communication has a wide consensus among scholars in risk science (Aven, 2020; Flage & Aven, 2009; Frewer et al., 2002; Renn, 2008, p. 252). However, Johnson and Slovic (1998) highlighted that uncertainty can be challenging to communicate to laypeople in a way that does not cause confusion. Frewer et al. (2002) found

[3] Bovine spongiform encephalopathy, commonly known as 'mad cow disease.'

that people prefer to be informed about the uncertainties linked to risks. Moreover, the study found it to be more acceptable when the uncertainties were because of the scientific process rather than lacking action or interest by the government. As a result, Frewer et al. suggested that risk communication should focus on 'what is being done to reduce the uncertainty' (2002, p. 363). Bouder (2015) stated that regulators tend to act in a precautionary manner when conflicting evidence or hazards occur, yet they often fail to re-evaluate precaution when reassuring evidence is put forth. This demonstrates that the assembling of evidence has to be a dynamic process, where risk descriptions are articulated accordingly (Bouder, 2009). Highlighting uncertainties and knowledge allows for a broader understanding of risk where additional factors are taken into account in the aim to describe, address and eventually apply risk measures (Aven, 2020; Aven & Ylönen, 2018).

2.3.2 Acknowledgement of public perspectives

Acknowledging public perspectives addresses the intended audience and attempts to understand their concerns and perspectives on the risks involved (Bouder, 2015). Studying public risk perceptions can provide insights and predictions to peoples reaction to new risks (Renn, 2010). Risk perception refers to 'a person's subjective judgement or appraisal of risk, which can involve social, cultural and psychological factors' (Aven, 2020, p. 138; SRA, 2018a, p. 4). Cognitive understandings of risk and the factors influencing risk perception have been highlighted often within research on risk communication (Bouder, 2015).

Risk perception is subjective, meaning that one person may perceive the same risk as being higher or lower than another person. Slovic (1987) stated that the risk perception of lay people is highly reliant on intuition, and this intuition can be influenced by factors such as our past experiences, media, culture, other people and so forth. Our intuition could also be subject to faulty heuristics (mental shortcuts), biases or emotions (Bouder, 2015; Skagerlund et al., 2020). Kahneman (2011) suggested that people generally make decisions by what he referred to as thinking according to the brains: *system 1* or *system 2.* These two thinking processes differ, where system 1 is quick and intuitive and system 2 is slow and analytic. The simultaneous use of the thinking processes is a necessity, but it can also lead to faulty conclusions because of heuristics (Kahneman, 2011). Under conditions of uncertainty, people are vulnerable to many heuristics that can influence their judgements (e.g., understanding probability, representativeness, availability and adjustment/anchoring heuristic) (Tversky &

Kahneman, 1974). Personal attributes can dictate the terms of how we interpret the message from the sender (Kaufmann & Kaufmann, 2015).

Starr (1969) found that the degree of voluntariness linked to an activity plays a central role in accepting risks. Examples could be the voluntary activity of driving a car versus involuntary activities posed by other controlling bodies (e.g., nuclear power plants). Starr's results indicated that people generally accept risks 1,000 times greater when it is a voluntary imposed risk (Starr, 1969, p. 1237). When compared with risk experts, laypeople tend to focus more on hazard characteristics, for example, the potential for catastrophic outcomes (Slovic, 2000b). Other influential factors are the degree of familiarity, controllability and level of understanding (Covello, 2009; Slovic, 2000b).

When people face situations of risk, a number of factors influence decision making; this is often referred to as *risk behaviour* (Sitkin & Pablo, 1992). Sitkin and Pablo (1992) described a three-clustered division of relevant factors that influences the decision makers in the decision between different risky choices. First, there are the **individual characteristics** of the decision maker, including risk perception and *risk propensity*, the latter meaning the 'cross-situational tendency to engage in behaviours with a prospect of negative consequences such as loss, harm, or failure' (Zhang et al., 2019, p. 153). Some people are more prone to focus on the positive aspect of risk, hence seeking riskier situations, while others focus on the negative aspects of risk and, therefore, seek options that are perceived as 'safer' (Dohmen et al., 2019; Sitkin & Pablo, 1992).

There are also **organisational characteristics** that influence risk behaviour (Sitkin & Pablo, 1992). These factors refer to the organisation itself, where the decisions are made. The research within this field highlight the importance of factors such as company safety policy and/or training (Man et al., 2021) or company-induced stress because of production pressure (Guo et al., 2016). Organisational culture is also a factor within this category and, by many researchers, is seen as a major influence on human behaviour and decisions (Reniers et al., 2011; Schein & Schein, 2017). In other words, there are practices and relations within the organisation or one's team/group that influences how decisions are made.

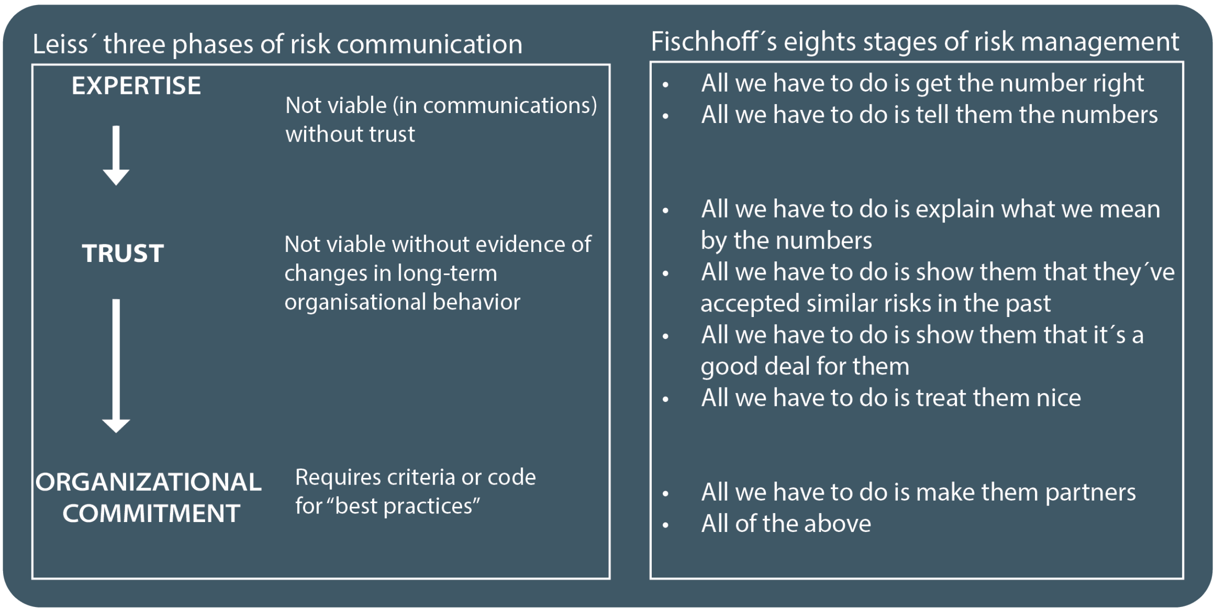
The third cluster of risk behaviour revolves around the **problem characteristics** (Sitkin & Pablo, 1992), emphasising the factors of the problem at hand. One example is how the problem is framed, whether it is in a positive or negative manner (Sitkin & Pablo, 1992). Different framing of the same choice could give effects on decision making, leading to inconsistent risk preferences (Kahneman & Tversky, 1979). Linden and Löfstedt described how regulators could have intent to either reassure (positive framing) or frighten (negative framing) as one of several 'highly questionable interpretation and communication practices' (2019, p. 11). Another factor is the level of experience the decision maker has towards the presented problem. A more experienced decision maker could use past experiences selectively to solve presented problems (March & Shapira, 1987; Sitkin & Pablo, 1992). Other research has indicated a propensity to underestimate the risks attached to one's own activities or past experiences, such as smoking (Slovic, 2000a) or natural disasters (Halpern-Felsher et al., 2001), as opposed to people who do not engage in the same activities or have the same experiences.

An understanding of public perspectives gives the opportunity for designing the right communication (Bouder, 2015; Renn, 2010). Learning from the failing communication strategies linked to the MMR vaccine, Bouder (2015) highlighted that the insights gained through knowing people's concerns could help form a strategy for when conflicting or un-scientific evidence becomes socially amplified.

2.3.3 Analysis of options

Analysis of options is where different choices are laid out and balanced. This implies being open about the different trade-offs and the weighing of potential costs and benefits (Bouder, 2015). One of the objectives is to demonstrate how the analysis of options is conducted and, thereby, how the risks are managed, providing transparency for the recipient (Bouder, 2009, 2015).

Several scholars have categorised the historical developments of risk communication practice. The most known are the three historical phases of risk communication by Leiss (1996), and the eight stages of risk management by Fischhoff (1995). Both categorisations complement one another, as shown in Figure 5.



Leiss´ three phases of risk communication

EXPERTISE

Not viable (in communications) without trust

TRUST

Not viable without evidence of changes in long-term organisational behavior

ORGANIZATIONAL COMMITMENT

Requires criteria or code for "best practices"

Fischhoff´s eights stages of risk management

- All we have to do is get the number right
- All we have to do is tell them the numbers
- All we have to do is explain what we mean by the numbers
- All we have to do is show them that they´ve accepted similar risks in the past
- All we have to do is show them that it´s a good deal for them
- All we have to do is treat them nice
- All we have to do is make them partners
- All of the above

Figure 5. Stages in development of risk communication, reproduced from Fischhoff (1995, p. 138) and Leiss (1996, p. 94)

Taking the view of the three historical phases of Leiss (1996), the first phase was characterised by a top-down communication. The focus was one-sided communication mainly directed at the general public, usually in a persuasive manner (Covello et al., 1986; Renn, 2008). The challenge in this phase was the lack of trust, in which the recipients were left with a notion that the risk experts were arrogant (Leiss, 1996). The second historical phase aimed to improve the communication and trust between the parties, hence focusing on clear messaging, credibility and communications, often imposing techniques inspired by marketing (Leiss, 1996). The third historical phase gave weight to the social context of the risk management process and emphasised the meaning of building relations and trust over time rather than utilising persuasion techniques. Each phase is built and developed on the underlying phase, thereby not completely replacing, but rather complimenting or correcting, certain aspects of the previous phase (Leiss, 1996). The development has led to further emphasising the importance of debate and two-way communication (Leiss, 1996; Renn, 2008).

What risk regulators deem as an acceptable risk can be hard to justify to the public eye; therefore, Renn (2010) emphasised that openness to public interests and stiving to communicate can be a way of remedying the effects of risk management decisions. In recent years, regulators' and agencies' *transparency* has been viewed as a factor affecting trust (Coglianese, 2009; O'Neill, 2002; Viola et al., 2022), and laypeople tend to want information about both supporting and ambiguous evidence to support personal decision making (Wiedemann et al., 2011).

According to Coglianese (2009), there are both positive and negative aspects to transparency. On the one hand, transparency can enlighten the public and serve as prevention to abuse of power by regulators. One the other hand, transparency can also create a fear of making mistakes in decision making and, therefore, less effective decisions. Total transparency can also be problematic in the collaboration with private actors who wish to keep certain business-related secrets from the public (Coglianese, 2009). Coglianese (2009) distinguished between *fishbowl transparency* and *reasoned transparency*. The former refers to releasing information and raw data providing transparency to their activities (e.g., on websites). Reasoned transparency is when governmental officials provide explanations as to why they have acted in a certain way.

Regulators tend to focus more on fishbowl transparency, by putting information and raw data on their websites, rather than reasoned transparency (Bouder, 2015; Curtin & Meijer, 2006; O'Neill, 2002). Publishing information on the internet is an easy and cheap process for being transparent but has had little shown effects in terms of countering the declining level of trust (O'Neill, 2002). For instance, Curtin and Meijer (2006) argued that the EU's fishbowl transparency could work against its intent because there has been very little interest by ordinary citizens to search in the online archives. Hence, such transparency could lead to damaging EU's reputation because of media or other people wishing to exploit disclosed information (Curtin & Meijer, 2006).

2.3.4 Authority in charge

Authority in charge is about defining the role of an organisation's involvement. For a governmental institution, this could mean clarifying its role in risk management and identify distinctions of responsibility between other institutions, private sector and so forth (Bouder, 2009). Trust is essential in the exercise of authority in risk communication (Bouder, 2009; Covello, 2009). Moreover, Löfstedt stated that 'Trust provides us with the lubrication to ease inherent frictions between society and its regulators' (2005, p. 6). According to Löfstedt (2005), there has been a decline in the levels of trust in Western modern societies recently. This decline in trust is because of a number of factors such as societal differences and access to higher education and general information (e.g. media, internet). These factors can generate scepticism among the general public. Löfstedt (2005) noted that a decline of public trust can reduce the efficiency of risk management and that the tools of risk management can sometimes have the opposite effect: increasing distrust. An example of how decreasing levels of trust materialise in modern day society was given by Larsson (2010); he pointed out that these societal changes have altered the practice of several professions with a historically high degree of societal authority, such as policing and teaching. As opposed to few decades earlier when authority was naturally given, such professions now find themselves in a position where they have to negotiate their own authority (Larsson, 2010).

With reference to risk management, Löfstedt (2005, p. 6) saw trust as a measurement for how willing the public is to accept decisions or risk judgements without questioning the underlying reasoning, stating that trust is something risk regulators should stive to obtain. Hence, it is paramount to understand the three underlying dimensions of trust. **Fairness** refers to the process of being impartial, ensuring that relevant actors and participants have been heard and that the outcome is objective and fair. **Competence** refers to how the public perceives the risk regulators competence in the face of issues linked to the case. **Efficiency** refers to the public perception of how the regulators execute their work and how they manage the recourses they are given (Löfstedt, 2005, pp. 7-8). Risk regulators tend to act on assumptions of public trust instead of testing the level of trust (Löfstedt, 2005). The latter could give insights into the best suitable communication method and, therefore, is an important part of designing risk communications (Balog-Way et al., 2020; Bouder, 2015; Löfstedt, 2005).

According to Löfstedt (2005, p. 5), there are three issues that pose a challenge for risk regulators in modern day society. First, trust is easily lost and much harder to regain after losing it. Second, distrust turns the public towards other sources of information, and they tend to perceive these sources as more reliable than the information provided from public risk regulators. Third, the 24/7 access to information through the internet and other forms of media create an independence to information given by governmental officials, policy makers and so forth. In turn, this contributes to a public with more knowledge but also more scepticism (Löfstedt, 2005). Renn (2008, pp. 254-255) stated that trustworthiness is achieved by exchanging and sharing information. This can be done by being open about technical information, hazards, risk assessments and results and avoiding a strategy where hazardous information is given in ‘fine print’ (Renn. 2008).

2.3.5 Interacting with your audience

Interacting with your audience is where the communication takes form by interacting with the intended audience using the selected method. An essential part of designing risk communication is to acknowledge that different audiences' calls for different communication methods (Bouder, 2009; Renn, 2010). Despite the various ways communication takes shape, there is a *sender*, a *message* and a *receiver* (Bråten, 2011; Kasperson et al., 1988; Renn, 1991). This can be one-way communication where the sender gives the message to the receiver or two-way communication where the message is given back and forth between the sender and receiver (Bråten, 2011). Proactive regulation likely increases the level of public trust. This means taking action before a certain crisis, as opposed to 'fire-fighting' after the crisis has occurred (Löfstedt, 2005, p. 12). According to Löfstedt (2005), the communication strategy should differ depending of the level of trust. Trusted agencies should engage in top-down communication and not partake in a wide deliberative process with interest groups on policy. If there is already established distrust, one must take measures to understand why there is distrust by looking at the three components of trust. This means considering a deliberative process (Löfstedt, 2005).

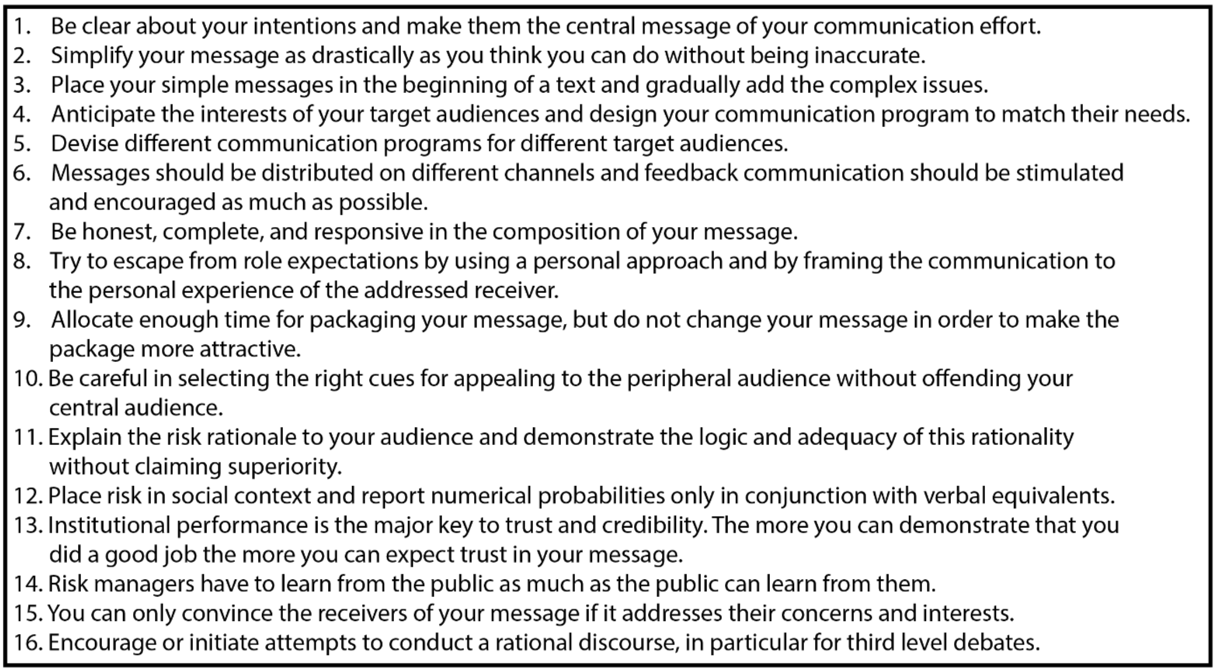
According to Aven (2020, p. 147), a risk communication involving the mere communication of likelihood judgement without addressing the underlying knowledge can be misleading. Many organisations apply probability judgements by referring to numerical and/or linguistic value. The use of both has been widely discussed in risk science and several findings have provided guidance towards designing risk communications. Similar to Mandel and Irwin's (2021) comments to the intelligence approach, Budescu and Wallsten (1985) also noted that numerical probability is a precise form, whereas linguistic probability (e.g., *unlikely*) is more vague and implies larger uncertainties.

Using probability to display uncertainty should be applied with careful consideration because it can also cause confusion, especially with lay people (Dieckmann et al., 2012). Even in cases where an interpretation table was given, much like Figure 3, interpretations were found to be inconsistent (Budescu et al., 2009). Budescu et al. (2012) argued that the use of precise probability can produce a falsified understanding by the recipient because it may imply a higher degree of consensus among experts and a higher precision of the estimates than what is really the case. In the opposite case where there is used qualitative linguistic estimates, the problematic nature relies on the reader's interpretation (Budescu et al., 2009; Budescu et al., 2012). Teigen et al. (2013) illustrated the latter in his study, where he found that the linguistic probability expression *unlikely* in a practical sense gave an association of near 0% chance as opposed to the intended interval of 10–30%.

Jenkins et al. (2018) studied four applications of probabilistic information and the level of success in risk communication: (1) numerical, (2) linguistic, (3) numerical and linguistic and (4) linguistic and numerical. The results indicated what they called the *extremity effect*, which means that the first presented expression was given the most weight. This effect was the least present in the numerical and linguistic variant (3), so this option gave the most consistent and accurate result. Several other scholars also recommend using both numeral and linguistic probability, including Budescu et al. (2009) and Ho et al. (2015), who also noted that this provides more flexibility if the numerical is not locked to a certain interval. For instance, if the term *likely* has a standardised probability interval of 70–90%, then the communicator could adjust the numerical to fit the risk at hand based on the evidence (e.g., 80% likely).

Renn (2008, pp. 251-271) developed a number of guidelines for how to effectively communicate risks, and Bouder (2010) further aggregated these guidelines into a list of 16, as shown in Table 2.

Table 2. 16 guidelines on how to communicate risks effectively, reprinted from Bouder (2010, pp. 283–284)



1. Be clear about your intentions and make them the central message of your communication effort.
2. Simplify your message as drastically as you think you can do without being inaccurate.
3. Place your simple messages in the beginning of a text and gradually add the complex issues.
4. Anticipate the interests of your target audiences and design your communication program to match their needs.
5. Devise different communication programs for different target audiences.
6. Messages should be distributed on different channels and feedback communication should be stimulated and encouraged as much as possible.
7. Be honest, complete, and responsive in the composition of your message.
8. Try to escape from role expectations by using a personal approach and by framing the communication to the personal experience of the addressed receiver.
9. Allocate enough time for packaging your message, but do not change your message in order to make the package more attractive.
10. Be careful in selecting the right cues for appealing to the peripheral audience without offending your central audience.
11. Explain the risk rationale to your audience and demonstrate the logic and adequacy of this rationality without claiming superiority.
12. Place risk in social context and report numerical probabilities only in conjunction with verbal equivalents.
13. Institutional performance is the major key to trust and credibility. The more you can demonstrate that you did a good job the more you can expect trust in your message.
14. Risk managers have to learn from the public as much as the public can learn from them.
15. You can only convince the receivers of your message if it addresses their concerns and interests.
16. Encourage or initiate attempts to conduct a rational discourse, in particular for third level debates.

Bouder (2015) further recommended considering the pros and cons of utilising modern technology such as the internet. Instead of merely ‘one-size-fits-all communications’ such as press releases, modern technology can be used to create a more interactive process between the parties like audience feedback and dialogue (Bouder, 2015, p. 13). As earlier addressed in the present thesis, there must be an approach to risk communication where the design is fit to meet the audience. This may include a variety of visualisations, details and complexity according to the audience’s level of understanding (Bouder, 2009; Hallgreen et al., 2016; Renn, 2010). However, the essential message must be kept consistent across the board (Bouder, 2009).

3 METHODOLOGY

In social sciences, the methodology describes the tools for gathering information and how the information should be analysed to make sense of the world we are investigating (Johannessen et al., 2010). The present thesis has utilised a triangulation of evidence and of qualitative methods, as shown in Figure 6. All research should be conducted in a way that promotes *transparency*, *methodic-ness* and *adherence to evidence* (Yin, 2016), and in this chapter, I present the methodical techniques and choices applied to answer the research question.

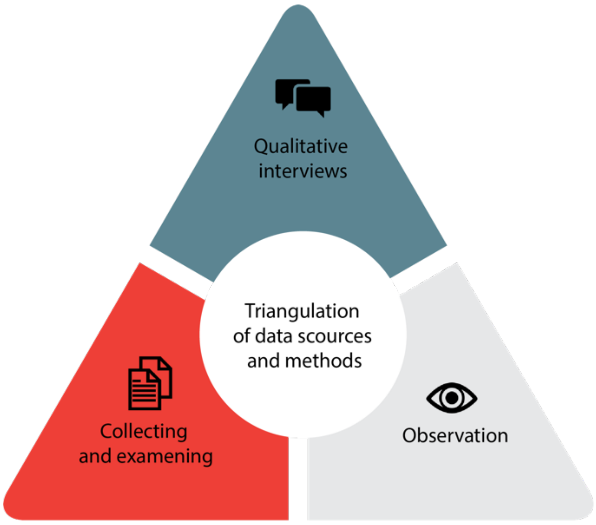


Figure 6. Triangulation of data sources and methods in this thesis

3.1 Research design and methods

As one of two research strategies, qualitative methods are based on social interactions or phenomenon and individual actions (Johannessen et al., 2010; Ringdal, 2013). According to Johannessen et al. (2010), qualitative methods are especially suitable where there is a low degree of prior research or knowledge and where the objective is a thorough understanding. The intelligence communities have a long history of secrecy compared with other governmental institutions (Phythian & Gill, 2013), and Vandepeer (2011) argued that, hence, the intelligence methodology has received little critique and research. Therefore, qualitative methods can be useful tools for investigating the intelligence field. For the following part of this section, I will go into each of the adopted methods. Finally, I will give details regarding how the data were coded and used in the analysis.

3.1.1 Data set one: Qualitative interviews

There is little research on intelligence risk communication, so qualitative interviews are a good way to gain new insights. Yin (2016, pp. 142-148) described such interviews as not being constricted to a strict protocol but rather the result of open-ended questions leading to a conversational communication between the interviewer and subject. For a holistic approach, both the sender and receiver of public risk communication participated in the interviews. I started with what Yin (2016) described as *purposive selection*. I contacted representatives for the intelligence services and journalists from the national media whom I knew had a role in receiving public risk communication from the intelligence services. I also utilised what Yin (2016) described as *snowball selection*, where I asked for participants both through my own network and the network of the already selected people for the study. The use of snowball selection provided me with a suitable selection because the intelligence agencies especially have an element of secrecy attached to their job descriptions. The selection left me with a total of six interviews: two from NIS, two from PST and two journalists from national media. Figure 7 illustrates the informants for the qualitative interviews and their role/relevancy.

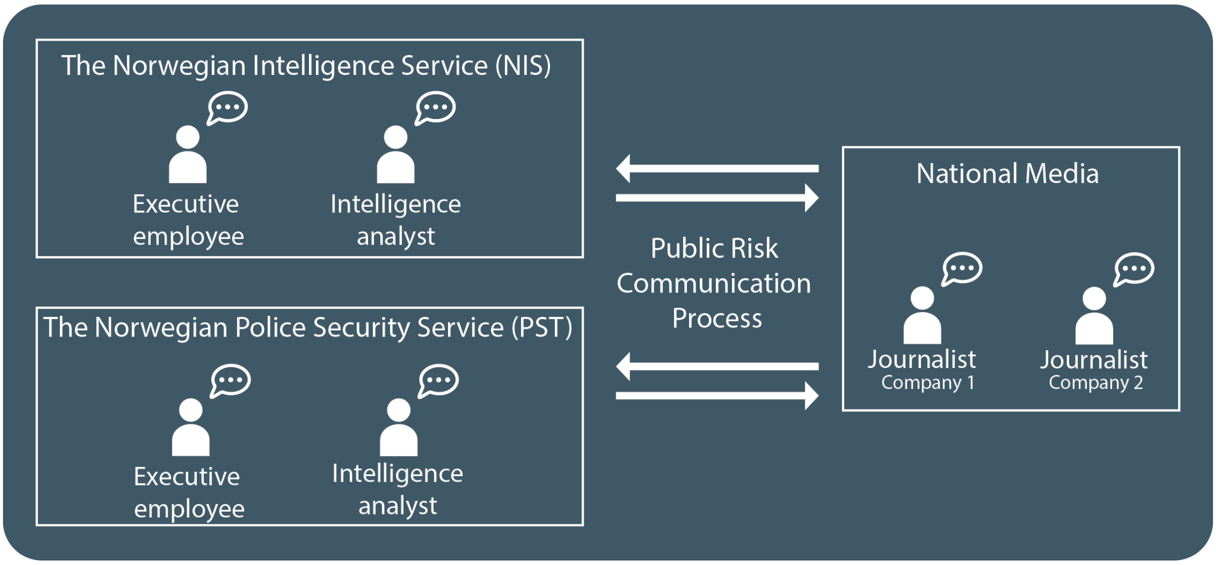


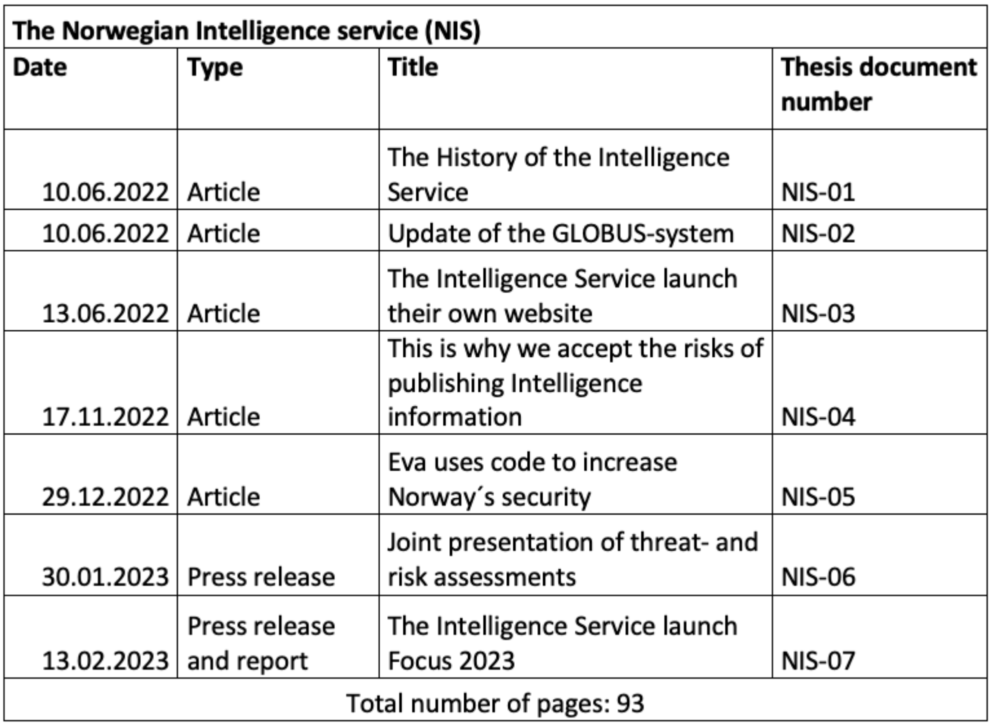
Figure 7. Visualisation of interview participants and their role in public risk communication

In accordance with Yin (2016), the interview guide was formed to reflect the literature review and contained 9 questions, in which the intended goal was to start a conversational thought process back and forth between both parties. The interviews were conducted one on one at a location of their choosing.

3.1.2 Data set two: Collection and examination

When conducting a study, there will often be a number of objects, such as documents, website information, artefacts and so forth, that are relevant to analyse in addition to other data. Yin (2016) highlighted that qualitative interviews can cause *reflexivity* related issues, where the effect of the interview setting can give a slightly different result compared to a normal conversation. A complimentary collection of objects is one way to reduce reflexivity (Yin, 2016). Both agencies have their own websites where they publish certain reports, press releases and other information about risks, how risk is managed and so forth. To give the data collection a broader dimension, the content of the agencies' communication on their websites over a span of one year was coded and analysed.[4] The goal of such data collection is not only to reduce reflexivity issues, but to provide evidence for the public risk communication practices with objective data. The time frame was set from of 1 March 2022 to 1 March 2023; a full list of content is listed in Tables 3 and 4. In addition to the publications, both websites contain multiple resources giving explanations to their work, how to understand intelligence and so forth. The majority of this information was looked through, but not directly addressed, in the analysis because of time and resource limitations.

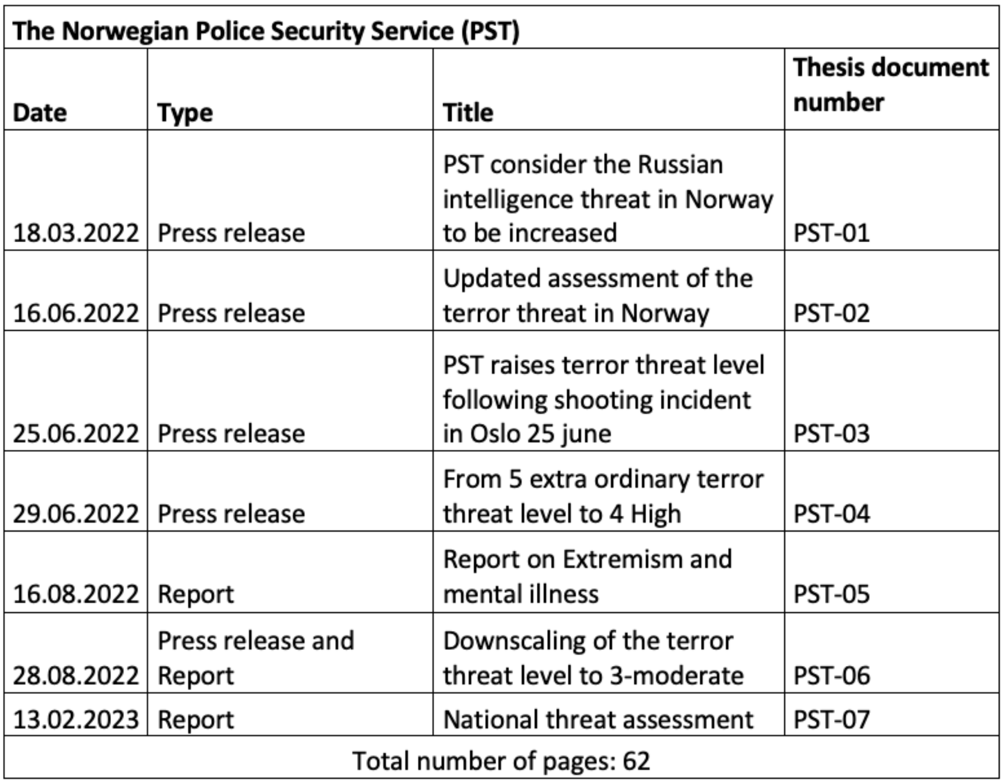
Table 3. Publications from the Intelligence Service from March 2022 to March 2023.



The Norwegian Intelligence service (NIS)			
Date	**Type**	**Title**	**Thesis document number**
10.06.2022	Article	The History of the Intelligence Service	NIS-01
10.06.2022	Article	Update of the GLOBUS-system	NIS-02
13.06.2022	Article	The Intelligence Service launch their own website	NIS-03
17.11.2022	Article	This is why we accept the risks of publishing Intelligence information	NIS-04
29.12.2022	Article	Eva uses code to increase Norway´s security	NIS-05
30.01.2023	Press release	Joint presentation of threat- and risk assessments	NIS-06
13.02.2023	Press release and report	The Intelligence Service launch Focus 2023	NIS-07
Total number of pages: 93			

[4] Certain documents were excluded because they were not deemed relevant for public risk communication. Most publications were in Norwegian, and these titles, shown in Tables 3 and 4, have been translated from Norwegian to English by the author.

Table 4. Publications from PST from March 2022 to March 2023



The Norwegian Police Security Service (PST)			
Date	**Type**	**Title**	**Thesis document number**
18.03.2022	Press release	PST consider the Russian intelligence threat in Norway to be increased	PST-01
16.06.2022	Press release	Updated assessment of the terror threat in Norway	PST-02
25.06.2022	Press release	PST raises terror threat level following shooting incident in Oslo 25 june	PST-03
29.06.2022	Press release	From 5 extra ordinary terror threat level to 4 High	PST-04
16.08.2022	Report	Report on Extremism and mental illness	PST-05
28.08.2022	Press release and Report	Downscaling of the terror threat level to 3-moderate	PST-06
13.02.2023	Report	National threat assessment	PST-07
Total number of pages: 62			

3.1.3 Data set three: Observation

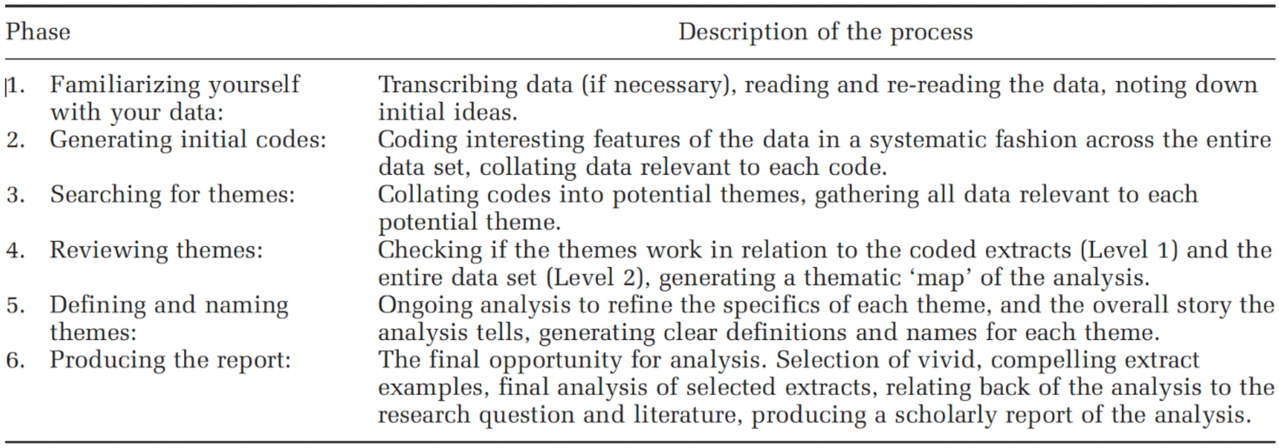
The qualitative method of observation is when the researcher is present and records situations relevant for the study that are based on the experience of seeing and hearing the actual event (Johannessen et al., 2010). One can utilise observation as a supplement to other methods to gain a new viewpoint into a specific area of interest (Johannessen et al., 2010; Yin, 2016). In a joint event each February, both NIS and PST, together with a third governmental agency, present their annual public threat assessment. The event is live streamed on government websites and on several national news media. Furthermore, the stream is recorded and published on the government's website.[5] Representatives from national news media are invited and can follow up with questions after the agencies have presented the key aspects of their reports.

The joint presentation of 2023 was utilised for the present thesis. The event was 59 minutes long and was transcribed to ensure that the analysis would capture the entirety of public risk communication.

[5] https://www.regjeringen.no/no/aktuelt/trusselvurderinger23/id2961017/

3.2 Analysing the data

The current thesis has adopted the use of both *primary evidence,* meaning data collected by the thesis author, as well as *secondary evidence*, meaning data collected or produced by others (Ringdal, 2013; Yin, 2016). To analyse the data, *thematic analysis* was utilised for coding and analysis. This is a widely applied method for analysing data developed by Braun and Clarke (2006). Thematic analysis was chosen because it has proven to be good for cross-data analysis, for example, data from interviews, documents and so forth to identify reoccurring patterns (themes) (Braun & Clarke, 2006). The method consists of six different phases.



Phase	Description of the process
1. Familiarizing yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes:	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

Figure 8. Phases of thematic analysis, reprinted from Braun and Clarke (2006, p. 87)

During data analysis, I implemented the use of phases one to five. To ensure a systematic approach, themes were repeatedly re-evaluated. Phase six (the results) will be presented in chapter four. These results will be the foundation for the discussion in chapter five.

3.3 Reliability and validity

My motive for methodical triangulation has been to strengthen the sources of evidence and ensure that the research question is viewed from multiple angles as objective and unbiased as possible. In relation to my data collection, it is relevant to comment on its *reliability* and *validity.* Although most evident in quantitative methodology, these factors are important in qualitative research (Ringdal, 2013; Thagaard, 2018). In qualitative research, reliability refers to the manner of how the research is conducted, that is, if the process seems reliable and credible. The overall thought is that the results can be reproduced by further research (Thagaard, 2018). Validity refers to the results and interpretation of data, along with the accuracy in the interpretation of evidence (Thagaard, 2018; Yin, 2016). Scholars such as Yin (2016) have argued that the use of triangulating evidence can strengthen the credibility because multiple sources of evidence can be put up against each other in comparison. Utilising this logic, one could argue that methodical triangulation increases the reliability of the study because it utilised multiple methods to gather different sorts of evidence. Furthermore, objective interpretation of data has been my priority throughout the process to further increase the validity.

3.4 Research ethics

Ethical challenges arise within aspects of qualitative interviews because it relies on personal descriptions later to be analysed and published (Kvale & Brinkmann, 2015). The present study contained personal data by recording, transcribing and analysing information from the interviewees. The project was viewed and approved by SIKT[6] to be in accordance with GDPR.[7] All participants were given information about the project, anonymity and personal data handling, and subsequently gave their participation consent. All records were transcribed, anonymised and then later destroyed after the analysis. When interviewing employees in the intelligence sector, I was attentive to the fact that most of their job was classified by law. The interview guide was given to all interviewees in advance. For the intelligence personnel, this gave them the option to identify potential answers/themes bound by classification issues. One intelligence informant did not consent to being recorded because of agency regulations. This interview was therefore substantially longer to ensure good notetaking. This informant later approved a written summary as his statement.

[6] Norwegian agency for shared services in education and research

[7] *General data protection regulation (GDPR*). Regulation of personal data handling within EU/EEA

4 RESULTS

This section provides the empirical evidence from interviews, relevant collected documents and observation. The results are displayed in a thematic fashion based on the questions in the interview guide, also corresponding with Bouder's (2009) framework for public risk communication. Content from the method of *collection and examination* is referenced with the thesis document number according to Tables 3 and 4 in the methodology chapter (e.g. PST-01, NIS-01 etc).

4.1 The understanding of risk and threat

Qualitative interviews

Based on the assumption that the intelligence agencies would view the terms *risk* and *threat* as two separate phenomena, all the interviews started with a clarification on how the terms risk and threat have been applied in the present thesis. This means viewing *risk* in a broad sense, where *threat* is a specific risk source with intentional malicious intent.

All four of the informants from the intelligence agencies made the clear distinction that their mandate was to mainly assess *threats*. *Risk* tended to imply implementing measures, often based on the threat assessment. For instance, the PST informants noted that their threat assessments often served as the basis for implementing measures in other governmental institutions such as the police force. The NIS informants commented that risk, in their context, would generally be the mandate of others such as the Norwegian National Security Authority (NSM). All four of the intelligence informants were clear that they used the term *threat communication*, where the interview guide stated *risk communication*. In contrast to the PST's model (Figure 1) for understanding *risk* in relation to *threat*, the two informants from the NIS noted that they understood and utilised *threat* in an everyday fashion without a specific model for distinguishing *risk* and *threat*.

Collection and examination

Of the collected material from PST, the concept of risk was only explained in PST's annual threat assessment: 'Risk can be defined in several ways. In this context, risk is discussed as a combination of assets, threats and vulnerability, and the national threat assessment is intended to be used as a resource to inform decisions about potential risks' (PST-07, p. 2).[8] Although the report was concentrated on threat, risks were addressed several times. For instance, they explained that their standardised probability model serves the purpose of creating '..a more uniform description of probability in the assessments and thereby to minimise the *risk* that they are unclear or to be misunderstood' (PST-07, p. 3). Another example is their belief that '…Russia may be willing to accept higher *risk* in respect of its intelligence activities in Norway' (PST-07, p. 9). The term *threat* was mentioned numerus times in the collected documents. It was defined to the extent of being one of the three factors making up risk, as earlier mentioned (PST-07, p. 2). NIS did not provide a definition to the terms *risk* or *threat*, but both terms were widely applied in their publications.

Observation

Both *risk* and *threat* were mentioned several times in the annual threat assessment presentation but not specifically defined. For instance, the Minister of Defence stated, 'Today, Russia is the biggest threat to Norwegian and European security'.[9] The Minister of Justice stated, '… every single one of us should be attentive to the risk of spreading false information or influence operations'.[10]

4.2 The goal of communicating risks to the public

Qualitative interviews

The two journalists both perceived the goal of the agencies' risk communication to be raising awareness, thereby seeking to prevent the described threats. One of the journalists noted that he perceived such communication to be a part of a culture of openness in which seemed to be a trending communicational strategy. Both journalists had for the most part collaborated with PST and also found them to be more outreaching and open. One of them noted, 'For some reason, they (PST) are more conscientious about reaching the common people' [11] (Informant #2, journalist).

[8] There might be a translation issue here because the Norwegian version of this document stated a different meaning to the last partial sentence: '…der den nasjonale trusselvurderingen gir beslutningsstøtte til vurdering av trusselen'. In English this corresponds to: '… the national threat assessment provides decision support to assessing the threat'.

[9] Translated original: 'Russland utgjør i dag den største trusselen mot norsk og europeisk sikkerhet'.

[10] Translated original: '...hver og enkelt av oss bør være oppmerksom på risikoen for spredning av falsk informasjon eller påvirkningsoperasjoner'.

[11] Translated original: 'Av en eller annen grunn så har de (PST) et mer bevisst forhold til å nå ut til allmuen'.

All four informants from the intelligence agencies stated that the main objective was to raise awareness to threats to society so that people could reflect on how this affects one's own life and workplace. The intended audience ranged from the common man in the street to people holding executive positions in government or other public and private organisations. Most informants highlighted the importance of openness towards citizens regarding what the agencies deemed as threats to society. One informant from NIS illustrated this by saying that the threats they presented to the public were the same threats they presented to the country's decision makers, though in a less detailed fashion. Both informants from PST stated that the most important message to the 'common man' was information on how to detect people who were in the process of radicalisation towards extreme ideology.

Both informants in executive positions, one informant from each agency, also noted that an additional purpose of risk communication was to build public trust and their institutional reputation.

Collection and examination

In the collected material from PST, the purpose of their public risk communication was only expressed in the annual threat assessment: 'It is intended to create awareness of the most serious threats facing Norway and to provide decision-making support in connection with the important preventive security measures for which enterprises are responsible' (PST-07, p. 2). It is later stated that the threat assessment should prompt the reader to perform a risk assessment to ensure that proper security measures are in place.

In the collected material from NIS, there was a less defined expressed purpose for public risk communication. However, NIS had one website posting where they explained their reason for launching their own website. NIS linked openness and transparency to being important to build and maintain trust while explaining why they must exclude certain details in communication with the public (NIS-03). NIS also published an article where they explained that one reason for their risk communication was to share their situational understanding as a contribution to the public discourse (NIS-04).

Observation

The annual threat assessment presentation had several references to the purpose of public risk communication. The Minister of Defence stated, 'The assessments presented today gives decision makers and our society knowledge and prerequisites that are of great importance for our security'.[12] Likewise, the Minister of Justice stated that the public assessments contribute to the understanding of the threats to society and that 'one can reflect upon one's own risks and assess possible preventive measures one should apply'.[13]

4.3 Demonstrating a credible basis for their position

Qualitative interviews

Both journalists expressed that the intelligence agencies were sparing in terms of giving details on the quality of supporting data or knowledge and pointing out uncertainties. 'That's where it stops. We receive little else information other than the preprogrammed sentences they wish to say something about, in which we simply have to accept'[14] (Informant #2, journalist). However, both journalists expressed understanding as to why such details were withheld from the public and saw this as a matter of trust and credibility. Both PST and NIS were seen as competent and trustworthy by the two journalists.

In terms of how probability was presented, one of the two journalists knew PST used certain probability expressions. However, this journalist did not know how many expressions they used or the equivalent percentage interval (e.g., the expression *highly likely* is defined to have more than 90% probability) and, hence, did not know the probability model to its full extent.

> I haven't related to any numeric value because I haven't really gotten an answer as to how the probability model is build up other than the expressions. That it's *likely* that people with mental illness will conduct violent acts with consequential death is

[12] Translated original: 'De vurderingene som presenteres her i dag gir beslutningstakere og samfunnet som sådan, kunnskap og forutsetninger som er svært viktig for vår egen sikkerhet'.

[13] Translated original: 'Det gjør at man kan tenke gjennom sin egen risiko og vurdere eventuelle forebyggende tiltak som en bør gjøre'.

[14] Translated original: 'Nei der stopper det jo. Så det får vi ikke vite noe særlig om, mer enn de forhåndsprogramerte setningene de ønsker å si noe om, som vi bare må akseptere'.

> something one has heard, but I don't know who calculated this or how the calculation looks like. This is something that can be clarified.[15] (Informant #2, Journalist).

The other journalist was not aware that any standardised probability expressions were used by the agencies at all.

All informants from the intelligence agencies made it clear that giving supportive information on the background knowledge, data and uncertainties linked to the data was problematic and impossible to implement in their public risk communication. This was because of the need to protect their sources and capabilities. The two intelligence analysts, one from each agency, also noted that a display of uncertainties linked to their supporting evidence could lead the audience to ambiguous interpretations. This is a point where the public risk communication differed from their risk communication to other decision makers and collaborating partners who had the need for—and clearance to receive—classified information. These audiences would also get more information about the supporting evidence. One of the informants referred to this as 'the food chain of threat communication'[16] (Informant #5, PST). In terms of their public risk communication, they could only give general information. This could, for instance, be stating that they utilised a set of specialised data collection methods.

The informants from PST agreed that there was generally higher degree of uncertainty in assessing their nonstate actors as opposed to state actors. The threat of nonstate actors (e.g., solo terrorists) was more dynamic and unpredictable. One of the informants noted the following:

> It is important to keep the threat communication at a steady pace, especially when it comes to nonstate actors because of the fleeting changes … There is a lot we don't know as a security service, and we constantly try to uncover what we don't know—and that's known as intelligence blind spots.[17] (Informant #5, PST)

[15] Translated original: 'Jeg har ikke egentlig forholdt meg til noen tallverdi for jeg har ikke egentlig fått helt svar på hvordan den sannsynlighetsskalaen er bygd opp annet enn ordene. At det er sannsynlig at folk med psykiske lidelser vil begå voldelige handlinger med døden til følge, det er noe man hører men jeg vet ikke hvem som har regnet seg til frem til dette og hvordan regnestykket ser ut. Så det kan godt tydeliggjøres'.

[16] Translated original: 'Næringskjeden i trusselkommunikasjon'.

[17] Translated original: 'Spesielt når det kommer til ikke-statlige aktører så er det å holde trusselkommunikasjonen jevn (viktig) fordi det endrer seg så flyktig... som en sikkerhetstjeneste er det så mye vi ikke vet. Vi prøver hele tiden å avdekke det vi ikke vet – og det kalles *etterretningshull'*.

Both intelligence informants in executive positions, one informant from each agency, emphasised the meaning of public trust in relation to the lack of supporting data transparency. As one of them noted, 'In a situation where PST have a poor reputation and low public trust, the public will be less inclined to believe us when we say: *This is the threat*. Because we will never be able to present the complete basis for why we set the threat level to a certain level'[18] (Informant #6, PST).

PST and NIS differed greatly in terms of reflections on—and application of—the standardised probability model. Both agencies utilised the model for risk communication, but only PST utilised this model for *public* risk communication. NIS abstained to protect their sources and because they did not find it useful from a pedagogical viewpoint for strategic reports such as their annual threat assessment. Despite whether the model was applied, all but one of the intelligence informants found the model to be problematic in terms of communicating risks, as shown by the following quotes:

> My experience is that it creates a lot of frustration and extra work because it's a statistical expression of something that is qualitatively assessed … So my experience is that, especially the use of probability expressions, is something that's always found controversial for some. It rarely resonates as well as our intentions. This is because we sometimes are so disagreeable internally about what level or probability expression that should be used. So I think it is a bit problematic as a communicational tool.[19] (Informant #5, PST)
>
> The model is in itself problematic. Take 40%, for instance, which is the crossing between *unlikely* and *even chance*. If someone told me that something was *unlikely*

[18] Translated original: 'Hvis PST har et svært dårlig omdømme og vi har lav tillit i befolkningen, så vil befolkningen i mindre grad tro på oss når vi sier at: Det er dette som er trusselen. Fordi vi vil aldri kunne presentere det komplette grunnlaget for hvorfor vi mener at trusselnivået er det eller det'.

[19] Translated original: 'Men jeg opplever at den skaper mye frustrasjon og merarbeid fordi det er en statistisk angivelse på noe som er en kvalitativ vurdering...Så opplever jeg at spesielt bruken av sannsynlighetsord er noe som hele tiden er litt kontroversielt for enkelte, treffer sjeldent så godt som vi ønsker, fordi vi også internt er så uenige noen ganger om hvilket nivå som er riktig eller hvilket sannsynlighetsord som er riktig. Så er den nok litt problematisk som kommunikasjonsverktøy'.

> and the reality was 40%, then I would be exasperated if this was an important issue. When it is hard for me, how is it then for a nonspecialist?[20] (Informant #4, NIS).

Collection and examination

Analysis of the collected material from PST and NIS indicate that they generally did not provide information regarding the supported evidence to their assessments, for example, the source of information or methods used to collect certain information. Uncertainties, either linked to the data or to the given probability, were not displayed. Examples include the following: 'It is **unlikely** that Russia will carry out an act of sabotage on Norwegian territory in 2023' (PST-07, p. 4) and 'Beijing thinks long term and is positioning itself for opportunities that may arise later, when Russia's need for investments are likely to increase' (NIS-07, p. 45). A few cases were found with both agencies, where they expressed some prior knowledge leading to their assessment of expected development, for example, 'Since the propaganda is being produced by sympathisers to an ever-greater extent, it is expected that terrorists will increasingly be inspired by local factors …' (PST-07, p. 30) and 'The expulsion of Russian diplomats has considerably restricted Russian security and intelligence services' freedom of action in Europe. Russia is therefore expected to …' NIS-07, p. 17).

Uncertainty was brought up a few times in the collected material from PST, mostly in short implicit statements like 'unresolved situation' (PST-03; PST-04), indicating high uncertainty. In a short press release where PST scaled the threat level down from 4-High to 3-Moderate, they additionally stated that 'PST's threat assessment is based on the information PST possess at any given time and will always be encumbered with a certain degree of uncertainty'[21] (PST-06, p. 1).

Both agencies used probability expressions in their texts. In the case of NIS, it remains unclear regarding the use of the standardised probability model because the probability expressions were incorporated in the text. In the case of PST, it was stated very clearly that the standardised model was implemented in their annual threat assessment. The probability expressions were utilised throughout this entire document and on all the presented themes. In

[20] Translated original: 'Ta 40%, som er skjæringspunktet mellom *lite sannsynlig* og *mulig*. Hvis noen hadde sagt til meg at noe var *lite sannsynlig* og det i realiteten lå på 40% så ville jeg vært sur hvis det hadde vært en viktig sak. Når det er vanskelig for meg, hvordan er det da for en ikke-spesialist'.

[21] Translated original: 'PST's vurdering er basert på den informasjonen PST til enhver tid besitter, og vil alltid være beheftet med en viss grad av usikkerhet'.

the presentation of probability, the expression was written in bold and underlined. The equivalent percentage was not presented. For instance, ‘PST believes there is an **<u>even chance</u>** that right-wing extremists will attempt to carry out terrorist acts in Norway in 2023’ (PST-07, p. 31). However, this application was not consistent throughout the collected material. In a press release (PST-02), the probability expression was not in bold or underlined but put in capital letters and followed by the equivalent percentage: ‘UNLIKELY, below 40% probability …’.[22] In cases where a probability expression and/or threat level was given, an interpretation table of the probability model and/or threat scale was presented near half of the cases.[23] Both agencies occasionally also used other probability expressions such as ‘most likely’ (PST-07;NIS-07) and ‘less likely’ (NIS-07).

Observation

Information regarding the supporting evidence was not given in the annual threat assessment presentation, either from NIS or PST. PST gave several probability estimates in their presentation, derived from PST-07, in accordance with the standard probability model. Both agencies—though more predominant with NIS—used other expressions that can indicate a form of probability. For example, ‘It is expected that terrorists increasingly will be inspired by local surroundings …’[24] (Director PST). ‘We can therefore expect a somewhat downplayed rhetoric and less offensive economic means of action’[25] (Assisting director NIS).

4.4 Acknowledging how lay people understand the presented risks

Qualitative interviews

The interviewed journalists both felt that the message from PST and NIS was constructed in a way that was clear and easy to understand. Both journalists wished they were given additional information, such as details and examples of how the threats could materialise. However, they understood why the agencies withheld parts of the information. One informant noted the following:

[22] Translated original: ‘LITE SANNSYNLIG, I underkant av 40 % sannsynlighet ...’.

[23] An explanatory table was presented in: PST-02, PST-07 and partially in PST-06. It was not presented in: PST-01, PST-03 and PST-04. PST-05 was a report not relevant for this issue and therefore left out of this specific analysis.

[24] Translated original: ‘...ventes det at terrorister i økende grad vil bli inspirert av lokale forhold’.

[25] Translated original: ‘Vi kan derfor forvente en noe nedtonet retorikk og mindre offensiv virkemiddelbruk’.

> That's the way it is with secret services. You can't ask for access to all the information you want. They must withhold something. Then it's our job as journalists to dig and try to extract information where we can.[26] (Informant #1, Journalist)

On the question of how they acknowledged public perceptions, the informants from PST and NIS all weighted the use of a clear message. *Public* risk communication was a challenge in the sense that the choosing of words and sentences were more important. The message should promote an unambiguous interpretation. If it were communication internally in the organisation or to other collaborating actors, then there would generally be more abbreviations and other worded formulations that required a deeper understanding of intelligence. Several intelligence informants referred to this as 'tribal language'. Both agencies also used '*Klarspråk*', which is a set of best practice principles from the Language Council of Norway, as a guide in designing their reports. The message would generally be based on their annual threat assessment with some customisation according to the audience.

> We pluck out our 'tribal language' to the best of our ability. The tribal language often contains a lot of probability expressions and abbreviations… This is something we try to take down to an understandable level.[27] (Informant #3, NIS).

The PST informant in the executive position stated that they found it challenging to reach the audience of boys in the age range of 17 to 21 years old. He knew the advertising business also found this target group to be challenging to reach. He noted that they knew little about how their message resonated with the audience, so there was an ongoing discussion in PST whether they should prioritise research on this issue. There would also be a reoccurring internal discussion from time to time regarding the possible negative consequences of their communication, making the public scared or at unease. However, the informant meant that their job was to describe the threat and that other institutions should take the position of reassurance towards the public. The informant stated that this was well illustrated after the terrorist attack in Oslo in 2022, where three different press conferences were held:

[26] Translated original: 'Sånn vil det være med hemmelige tjenester. Du kan ikke be om innsyn på alt du lurer på. De må holde tilbake noe. Så blilr det vår jobb som ournalister å grave og prøve å hente det ut der det er mulig'.

[27] Translated original: 'Vi plukker ut stammespråk så godt vi kan blant annet. Og i det stammespråket så vil det være ofte mye sannsynlighetsord og bokstavforkortelser ... Den prøver vi å ta ned og gjøre forståelig.'

> PST had a press conference where we tried to describe the threat picture, as well as we could and looked at possible consequential (terrorist) acts that could follow. … Then, Oslo Police District elaborated on the status in town ... and came with the '*don't be afraid, we have control*' type messages. And then, the Prime minister stood there with the executive '*we as a society cannot let this break us*' type message.[28] (Informant #6, PST)

4.5 Displaying risk management options

Qualitative interviews

Both journalists had received little information about how the agencies balanced different options in their risk management. However, they both expressed an understanding as to why such information was a scarcity.

> The secret services can't reveal the tools in their toolbox. In a way, that's their dilemma. How much should they reveal? How much do you keep for yourself? This is a point where I experience a difference between PST and the Intelligence Service, where PST are more open. Although they (PST) also keep their cards close to their chest.[29] (Informant #1, Journalist)

All the intelligence informants were clear on the fact that displaying risk management options to the public was something that they could not do. The two informants from NIS stated that they could loosely say something about the superior lines. One of them stated that an example would be the thematic of cyber incidents. In these cases, they could refer to it being handled by the joint cyber coordination centre. An informant from PST stated that this was something they were cautious about: '… We don't want the actors we are set to handle to know the content of our toolbox, or what we prioritise, and how we prioritise to use it … We are

[28] Translated original: 'Da står PST på en pressekonferanse og prøver så godt vi kan å beskrive trusselbildet vi ser og hvilken effekt vi tror dette terrorangrepet kan ha for eventuelle følgehandlinger...Også står Oslo politidistrikt og forteller hva som er status i byen... og kommer med de «ikke være redd, vi har kontroll» budskapene. Også står Statsministeren der etterpå og tar de overordnede «vi som samfunn må ikke la oss knekke av dette» type budskap'.

[29] Translated original: 'De hemmelige tjenestene kan jo ikke avsløre alle verktøyene de har i verktøykassa si heller. Og det er jo på en måte deres dilemma da, hvor mye skal de gå ut med? Hvor mye skal du holde for deg selv? Så der opplever jeg en forskjell mellom PST og Etterretningstjenesten spesielt da, og PST er mer åpne enn Etterretningstjenesten. Selv om de også holder mange kort tett inn til brystet'.

dependent on that our toolbox, the deepest and darkest part of it, remains unknown'[30] (Informant #5, PST).

The answers from the intelligence informants present an understanding that their purpose in public risk communication should mostly be centred around describing the threat as opposed to discussing risk management options. Their mandate would mostly be confined to descriptions of a threat actors; modus operandi, capacities, intentions, enemy stereotypes, target selection and so forth.

Collection and examination

The collected material indicate that PST and NIS did not give any information regarding their risk management options. In the case of PST, the extent of risk management options was limited to superior statements such as, 'The situation after the attack in Oslo on the 25th of June is now further clarified and a number of measures are put in motion'[31] (PST-06, p. 2) or 'There is a continuous preventive-focused job against potential threat actors'[32] (PST-06, p. 2).

Observation

Some references to risk management options were given at the annual threat assessment presentation. These references, however, were found in the introduction where the political elected ministers give some statements as to their governments focus and implemented measures. For instance, 'The government has focused on the day-to-day emergency readiness and operations, presence and vigilance, and strengthened contingency defence supplies'[33] (Minister of Defence).

[30] Translated original: 'Vi ønsker ikke at de aktørene vi skal håndtere er klar over vår verktøykasse eller hva vi prioriterer og hvordan vi prioriterer å bruke det ... Vi er også helt avhengige av at vår verktøykasse, at den dypeste og mørkeste delen av den, ikke er kjent'.

[31] Translated original: 'Situasjonen etter angrepet i Oslo den 25.juni er nå ytterligere avklart og en rekke tiltak er iverksatt'.

[32] Translated original: 'Det pågår et kontinuerlig forebyggende arbeid rettet mot potensielle trusselaktører'.

[33] Translated original: 'Regjeringen har lagt vekt på daglig beredskap og operasjoner, tilstedeværelse og årvåkenhet, og styrket beredskapsbeholdningen'.

4.6 Defining the nature of agency involvement

Qualitative interviews

Both journalists felt there was a clearly defined mandate and area of jurisdiction for each of the two intelligence agencies. One of the journalists indicated that this division of mandates would not be as clearly defined for 'the common man'.

> I know that after the 'Frode Berg case,'[34] for instance, the work of PST has become harder even though it was the Intelligence Service who fu**ed up. That's because people don't separate between the two and think that the secret services are the same.[35] (Informant #1, Journalist)

Both journalists had high trust towards both services and thought this also would apply for the public. Public trust was seen as a virtue the agencies should stive to achieve. In terms of transparency, PST was the agency that was seen as the most transparent agency.

Most intelligence informants noted that the public and media often were confused about the mandate and jurisdiction of their agency. This could be because they either were given questions of a political nature or relating to the jurisdiction of another agency. NIS operated with external threats, whereas PST operated with internal (domestic) threats.

All intelligence informants valued public trust and saw it as essential in their risk communication. In the case of NIS, one of the informants stated that the organisation tested for institutional reputation and knew the results indicated high public trust. The test was conducted by their superior organisation, the Norwegian Armed Forces, but the informant was uncertain as to the frequency or if NIS was addressed specifically. The other NIS informant was not aware of any such testing. In the case of PST, both informants stated that they knew the institutional reputation was tested and that the results indicated high public trust. In terms of test frequency, one of the informants knew this to be an annual testing, whereas the other informant was not sure.

[34] A case where a Norwegian army retiree was arrested in Russia in 2017 and later convicted by Russian authorities for espionage. The case brought much scrutiny and media coverage in Norway at the time and is often referred to as a NIS scandal.

[35] Translated original: 'Jeg vet for eksempel at etter Frode Berg-saken, selv om det var etterretningstjenesten som fu**et opp der, så har det på en måte gjort arbeidet til PST mye vanskeligere. Fordi folk skiller ikke mellom de og tenker at de hemmelige tjenestene er det samme'.

Transparency was something all four of the intelligence informants felt was hard for achieve. First, there were laws and regulation constricting transparency. Second, information had to stay hidden to ensure that sources were protected. One of the informants from NIS stated that the goal was to be '… as transparent as possible, without being irresponsible'[36] (Informant #4, NIS). This could include publishing information on their website, having background conversations with central news editorials or explaining why certain details had to be kept secret.

One of the PST informants noted that PST seemed more transparent recent years, at least to the public eye. However, the reality of this issue was that it was only their availability that had changed over the years:

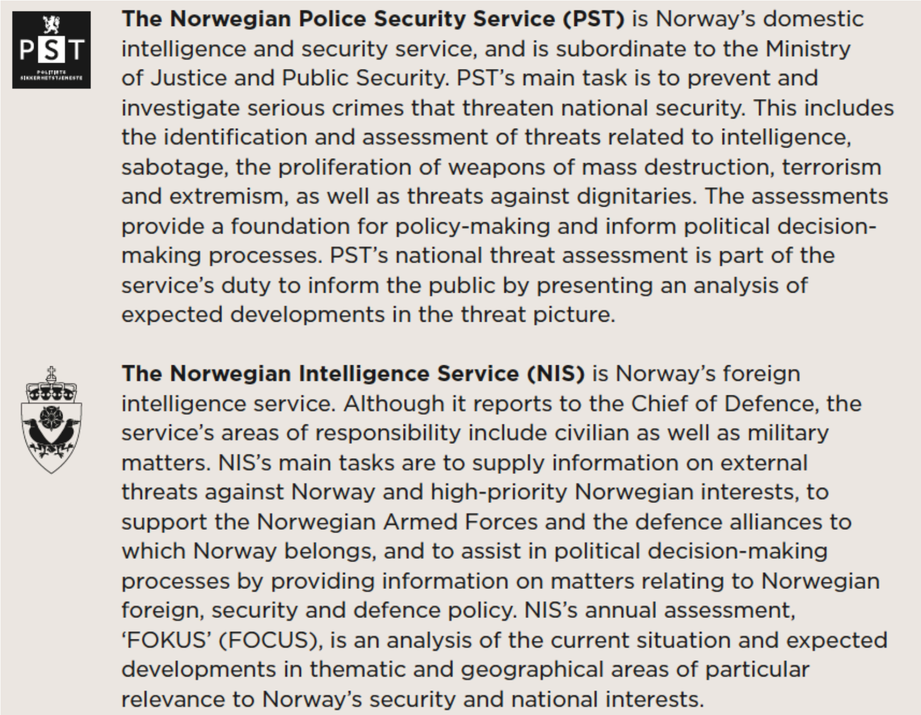
> … PST is surrounded by the same legal restrictions today as we were 10 years ago in terms of openness. Nevertheless, PST is perceived to be a lot more open today, without this actually being the case. We don't give more information today if openness is seen as the actual content of the information, but availability is a keyword in this regard. We are available on another level compared with earlier.[37] (Informant #6, PST)

Collection and examination

The two agencies both had a preliminary statement in their annual threat assessment (PST-07;NIS-07) where the mandate and jurisdiction was presented. This text was the same for each of the documents and explained the agencies distinctive nature.

[36] Translated original: '... så transparent som mulig uten å være uforsvarlig'.

[37] Translated original: 'PST er omringet av de samme juridiske begrensningene i dag som for 10 år siden, hva gjelder åpenhet. Likevel blir PST oppfattet som mye mer åpen enn vi var før, uten at vi egentlig er det. Altså hvis åpenhet er reelt informasjonsinnhold så gir vi ikke ut så veldig mye mer informasjon i dag enn vi gjorde før, men jeg tror et nøkkelord her er tilgjengelighet. Vi er tilgjengelige på en helt annen måte enn vi var før'.



The Norwegian Police Security Service (PST) is Norway's domestic intelligence and security service, and is subordinate to the Ministry of Justice and Public Security. PST's main task is to prevent and investigate serious crimes that threaten national security. This includes the identification and assessment of threats related to intelligence, sabotage, the proliferation of weapons of mass destruction, terrorism and extremism, as well as threats against dignitaries. The assessments provide a foundation for policy-making and inform political decision-making processes. PST's national threat assessment is part of the service's duty to inform the public by presenting an analysis of expected developments in the threat picture.

The Norwegian Intelligence Service (NIS) is Norway's foreign intelligence service. Although it reports to the Chief of Defence, the service's areas of responsibility include civilian as well as military matters. NIS's main tasks are to supply information on external threats against Norway and high-priority Norwegian interests, to support the Norwegian Armed Forces and the defence alliances to which Norway belongs, and to assist in political decision-making processes by providing information on matters relating to Norwegian foreign, security and defence policy. NIS's annual assessment, 'FOKUS' (FOCUS), is an analysis of the current situation and expected developments in thematic and geographical areas of particular relevance to Norway's security and national interests.

Figure 9. Presentation of PST and NIS, reprinted from PST-07, p. 1.

The content of the NIS threat assessment and PST threat assessment can be viewed as having a degree of overlap. Both documents assessed foreign states, such as Russia and China, but with the distinction that PST assessed their activity in Norway whereas NIS assessed their overall capabilities, intentions and so forth.

Observation

Overlap was also seen in the annual threat assessment presentation. For instance, both agencies referenced the ongoing war between Russia and Ukraine, as well as talk about state actors such as Russia and China.

4.7 Audience interaction

Qualitative interviews

Both journalists acknowledged that the communication had a different nature based on the situation. There would be situations where there would be top-down communication, such as the presentation of their threat assessments, and other times, it would be a two-way dialogue. Both journalists felt their communication was better with PST but also noted that this was the agency they had the most communication with. One of the informants pointed out that he had used PST's podcast quite a bit and found it both informative and as a good way of reaching out to the public. The other journalist emphasised that the agencies' communication was tightly governed, hence leaving him with little room for conducting journalism: 'It is a presentational form you kind of just accept. There is no point in arguing the form or content because it is their message—what they have to offer'[38] (Informant #2, journalist).

In the case of NIS, one of the informants noted that their communication was governed. Their role was often to describe the backdrop, meaning the development outside Norwegian borders that could influence national threats. The other NIS informant noted that there was two-way dialogue, mostly with journalists. They also focused on communicating through other channels such as interviews, radio and so forth.

In the case of PST, one of the informants emphasised that they had recently been focused on participating in multiple arenas. They had increased the number of meetings and presentations to a variety of audiences. Both PST informants explained that they had incorporated a strategy where they would also send people from the lower ranks of the organisation to communicate with certain audiences. One of the informants explained that this was a strategy to lower the perceived balance of power, based on the presupposition that it would seem more disarming and increase the chances of a good dialogue.

One of the PST informants also highlighted that one of their challenges in public risk communication was their interdependency to the mass media for further spreading of their message:

> … and the media need news flashes, news angles and something fresh … If you have a press conference and do interviews and figure on the news channel, then you reach a very large portion of Norwegian residents. But when it's told, then they won't run that news two times or three.[39] (Informant #6, PST)

In terms of choosing the right method, both agencies formed a strategy depending on the indented audience. For instance, NIS had featured on 'Supernytt', a news programme

[38] Translated original: 'Det er jo en presentasjonsform som man bare aksepterer på en måte. Det er ikke noe vits i å krangle på form og innhold på det fordi det er deres budskap, det de har å tilby'.

[39] Translated original: '...og mediene de må ha nyhetspoenger, nyhetsvinklinger, og det må være noe nytt...hvis du har en pressekonferanse, du stiller opp i nettintervjuer, er på Dagsrevyen, ja så når du en veldig stor del av Norges befolkning. Men når den er fortalt så vil de jo ikke kjøre den nyheten to ganger eller tre'.

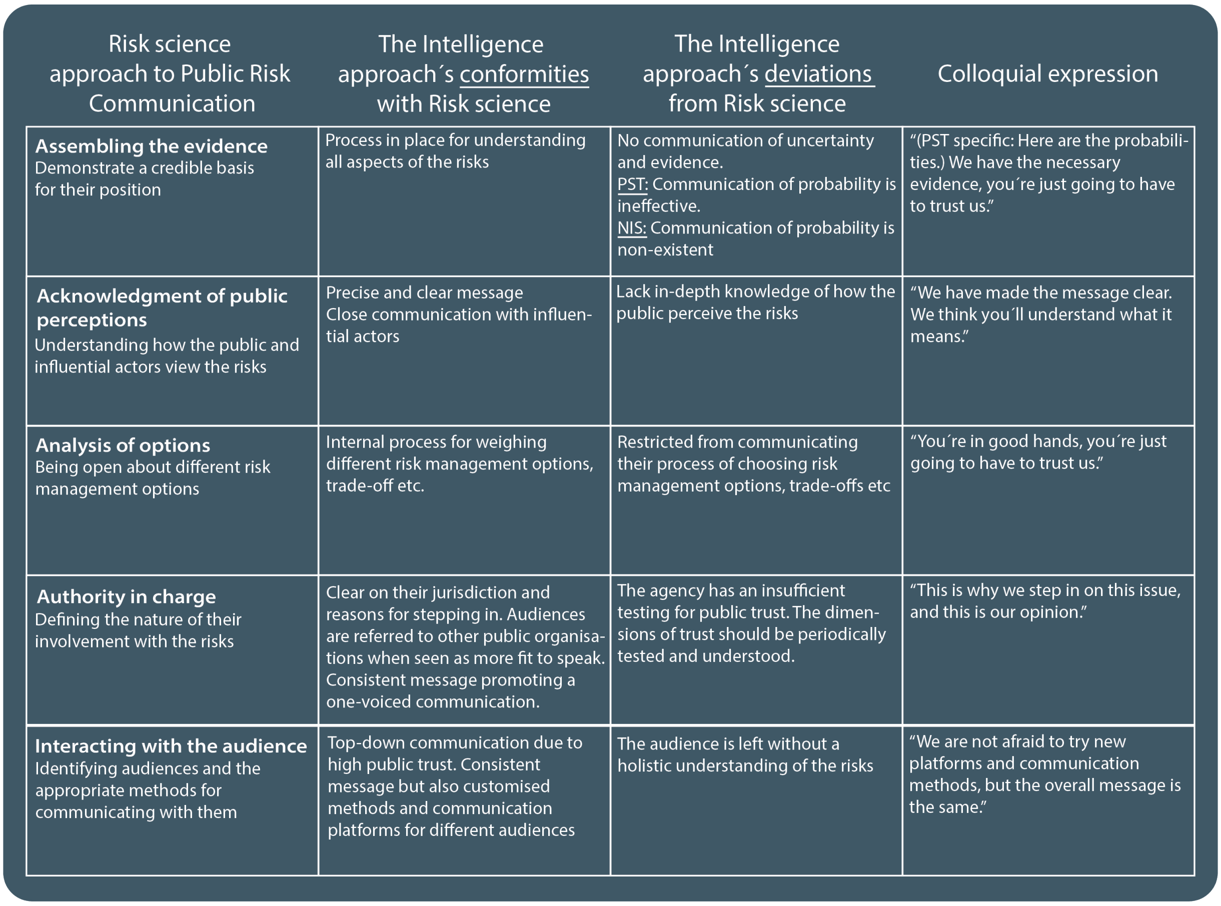
intended for children. Prior to their appearance, they had a reference test group of children on whom they tested how their message resonated and evaluated the level of success.

5 DISCUSSION

The objective of the present thesis has been to see how the public risk communication approach in the National Police Security Service and the Intelligence Service conformed or departed from risk science. Furthermore, the aim was to evaluate their approach from a risk science point of view.

As shown in Table 5, the data suggest that the public risk communication approach of PST and NIS had a great deal of similarities but differed on certain central aspects, such as the approach to communicating probability. Compared with public risk communication best practice, the data suggest areas of both a conforming and deviating nature. The agencies greatly restricted public access to details of the underlying data, as well as the internal discourse of risk management options. The analysis identified organisational trait-related issues as a key factor for the areas where there has been deviating practices.

Table 5. Visualisation of the main findings



Risk science approach to Public Risk Communication	The Intelligence approach´s conformities with Risk science	The Intelligence approach´s deviations from Risk science	Colloquial expression
Assembling the evidence Demonstrate a credible basis for their position	Process in place for understanding all aspects of the risks	No communication of uncertainty and evidence. PST: Communication of probability is ineffective. NIS: Communication of probability is non-existent	"(PST specific: Here are the probabilities.) We have the necessary evidence, you´re just going to have to trust us."
Acknowledgment of public perceptions Understanding how the public and influential actors view the risks	Precise and clear message Close communication with influential actors	Lack in-depth knowledge of how the public perceive the risks	"We have made the message clear. We think you´ll understand what it means."
Analysis of options Being open about different risk management options	Internal process for weighing different risk management options, trade-off etc.	Restricted from communicating their process of choosing risk management options, trade-offs etc	"You´re in good hands, you´re just going to have to trust us."
Authority in charge Defining the nature of their involvement with the risks	Clear on their jurisdiction and reasons for stepping in. Audiences are referred to other public organisations when seen as more fit to speak. Consistent message promoting a one-voiced communication.	The agency has an insufficient testing for public trust. The dimensions of trust should be periodically tested and understood.	"This is why we step in on this issue, and this is our opinion."
Interacting with the audience Identifying audiences and the appropriate methods for communicating with them	Top-down communication due to high public trust. Consistent message but also customised methods and communication platforms for different audiences	The audience is left without a holistic understanding of the risks	"We are not afraid to try new platforms and communication methods, but the overall message is the same."

The rest of this chapter will focus on discussing the findings relevant for the research question.

5.1 Factors influencing intelligence-based public risk communication

As described by Phythian and Gill (2013), intelligence agencies has historically had an inherent element of secrecy attached to methodology and practice. Intelligence seeks to find information about an organisation, group, individual or country. The purpose is to create a situational awareness, explain certain phenomena and predict how the situation will evolve (Omand, 2019). Furthermore, intelligence gives decision support to leaders on how to tackle the presented issues. The results of the present thesis indicate that most of the intelligence information must remain secret to protect the sources, methods, capabilities and limitations. This concrete issue is a good example of the inherent difference between safety and security. *Malicious intent,* as highlighted by Jore (2017), implies that someone has the intention to harm something. Extending this, it means that a total transparency of the data, for example, stating what areas they have large quantities of information and those areas they have little information, would be contra-effective. This would leave the intelligence agency vulnerable for exploitation. Revealing too much information could create a situation where the counterpart, for example, a terror organisation, could adjust their methods or targets according to the information they knew the intelligence agency possessed. The need for confidentiality also restricts the open discussion on different risk management options. Consequently, such underlying information would only be communicated in risk communication to recipients and decision makers who had the clearance and need for such information. This was both expected and understood by the two recipients of public risk communication. These circumstances differ greatly from, for example, public risk communication in the food sector, where one can more openly discuss underlying knowledge and uncertainty.

In risk science, assembling the evidence consists of two partials. For one, there is the need to collect sufficient information so that the risks and associated uncertainties are understood and that possible hazards and consequences are assessed (Bouder, 2015). Second, the evidence needs to be communicated to the audience in a fashion where the underlying factors, such as uncertainties, are made clear (Aven, 2020; Flage & Aven, 2009; Renn, 2008).

The intelligence informants stated that they had a process that could address the quality of the underlying evidence. This implies that they had internal processes for collecting information and assessing the quality, possible hazards, ambiguous information and so forth. However, such information could not be communicated to a public audience because confidentiality is needed. From a risk science perspective, Aven (2020) argued that such information generally should be communicated to the recipient for them to make a risk-informed decision. Hence, risk communication and the scientific quality of the underlying data cannot be separated.

The exclusion of information on supporting evidence was also highly reflected in the collected material because there was little notion of where there could be discrepancies, alternative explanations and so forth. From a risk science perspective, this became a challenging position because uncertainties generally can be viewed as a central component of risk. Furthermore, one can argue that security issues will generally have a higher degree of uncertainty (Jore, 2017; Piètre-Cambacédès & Bouissou, 2013), amplifying the need to communicate the extent of the uncertainty. In the case of PST and NIS, there are generally situations where there would be a relatively high degree of uncertainty, which is most evident in assessing nonstate actors as opposed to state actors because of the nonstate actors' more unpredictable nature.

Vandepeer (2011) argued that the intelligence agencies' use of models such as Singer's model for threat analysis is not applicable in the same way for nonstate actors, as opposed to the traditional state actors, because of the nonstate actors' unpredictability. States generally have stabile characteristics where there is a history, culture and clear military and political hierarchies (Vandepeer, 2011, p. 57). Furthermore, Vandepeer argued that, through these characteristics, we can largely understand how a state operates. Nonstate actors, on the contrary, are more individualistic, group and/or network based. They are more undefined, unclear and less understood than state actors (Vandepeer, 2011).

A methodology discussion on applying Stinger's threat analysis is outside the scope of the present thesis. However, the notion that nonstate actors produce judgements of higher uncertainty is important because of its relevance for risk communication. The data suggest that the agencies make no obvious distinction in how they present state actors (e.g., threat of foreign state activity in Norway) and nonstate actors (e.g., threat from right-wing extremists) in terms of reflections on uncertainty. This is the case even though several intelligence informants agreed that nonstate actors would imply a more fleeting and dynamic situation. Utilising the logic from Vandepeer, one can argue that the current practice may cause misinterpretations. For instance, when PST presented probability judgements for both state and nonstate actors in the same fashion, without explaining their distinctive nature, this could leave the reader with an understanding that the judgements would have a higher degree of certainty (especially with nonstate actors) than what the reality is.

There is an argument that the use of a lower probability expression or interval, for example, *even chance 40–60% probability*, would imply higher degree of uncertainty. One might then say that uncertainty is in fact reflected in their public risk communication. However, such an argument might be viable when the audience is intelligence professionals or others with an in-depth knowledge of the intelligence field, but it would doubtingly be the same for lay people. Lay people can find it difficult to interpret and understand uncertainty correctly in these types of settings (Dieckmann et al., 2012), e.g. because of faulty heuristics that influence risk perception (Bouder, 2015; Skagerlund et al., 2020; Slovic, 1987)

The results have further shown that the standardised probability model (the NATO variant in Figure 3) is utilised by both NIS and PST but only by PST for *public* risk communication. In the case of PST, the communication of probability is not consistent. Their most dominant way of communicating probability is by stating the verbal expressions (e.g., *Likely*) without stating the equivalent percentage interval. From a risk science perspective, these types of assessments are complex. There is little statistical data, and one must rely on information gathered from different qualitative sources. This may not be inherently problematic, but when combined with the notion that uncertainties and supporting evidence are to be left out of the public risk communication, it becomes a challenging starting point.

There are both pros and cons of expressing probability in numerals and linguistic values. However, many scholars have suggested a combination where both verbal and numeral probability is given to the reader (Bouder, 2010; Budescu et al., 2009; Ho et al., 2015; Jenkins et al., 2018; Renn, 2008) and where the numerical is given first (Jenkins et al., 2018). A discussion of how applicable the intelligence probability model is outside the scope on the present thesis, but it is important to note that such a model will always be a simplification of the reality. From a risk science perspective, this model must be explained in further detail. In this sense, the model becomes a tool for further understanding and interpretating information. When the model is utilised without proper explanation, the communication may become ineffective and not resonate as well as the communicator's intention. The observed event is one such example where linguistic probability was presented without numeric values or an explanatory table of what the linguistic probabilities relate to. The risk of an unsuccessful probability understanding was further illustrated in the present thesis in the case of the two nonintelligence informants; both had been given a written explanatory table (in document PST-07) as to the equivalent percentage interval of the probability expressions, but this failed to resonate with them. Hence, this result replicates the results in the study of Budescu et al. (2009). This means that, when the term *likely* was applied, the recipient did not have a unified understanding of how the term should be interpreted. The consequence would be a randomised interpretation of probability according to their own subjective risk perception, as described by Slovic (1987) and Teigen et al. (2013).

Three out of the four intelligence informants stated that the probability model was problematic in terms of communicating probability. First, there was the challenge of calculating the right probability. There was mostly qualitative information in which they had to conform to a probability model of a quantitative nature. Furthermore, as one of the informants noted, a 40% probability is the point where *unlikely* goes over to *even chance* as a probability expression. When the complexity of the situation makes it hard to place the threat in a single probability category, the crossing of probability expressions may seem like big leaps.

Based on the results, the intelligence agencies did not demonstrate a credible basis for their position from a risk science perspective. This is mainly because the underlying evidence was not addressed at all. For instance, their written material seemed to not systematically separate assumptions from evidence. An example is as follows: ‘It is unlikely that Russia will carry out an act of sabotage on Norwegian territory in 2023’ (PST-07, p. 4). The recipient did not know if this assessment was based on evidence that Russia would not conduct sabotage operations in Norway or if this was an assumption based on prior history, assessments of Russia’s intentions and so forth. The same is illustrated in NIS’s material, though less frequent, for example, ‘Beijing thinks long-term and is positioning itself for opportunities that may arise later, when Russia’s need for investments are likely to increase’ (NIS-07, p. 45).

NIS gives no definite probability, leaving the notion that the probability is less relevant to the message they want to communicate. The NIS informants highlighted a clear message and emphasised the meaning of a simplistic description of how they viewed the world, free of ‘tribal language’. From a strict risk science perspective, such an approach could be deemed unsuccessful because the recipient is not left with the full understanding of the risks involved.

PST’s approach attempts to remedy this by also communicating probability, mostly in the form of presenting linguistic probability. One can clearly argue that this approach communicates a levelling of probability. For instance, *highly unlikely* has an intuitively lower probability than *unlikely*. However, it falls short of effectively and consistently communicating probability from a risk science perspective. This is because of how probability is expressed and applied. An approach where both linguistic and numerical probability is presented would be more in line with the research in risk science.

In both NIS’s and PST’s cases, the lack of portraying underlying knowledge and uncertainties represent a deviation from risk science. The distinct nature of intelligence agencies and the terms for how their work must be conducted strongly limits their opportunity to conform with this principle in risk science. That being said, the present thesis argues that there are measures that can partially counteract this. This will be presented in section 5.4

5.2 Communicating the message

The results of the analysis have highlighted that the intelligence agencies weighted the importance of semantics in their public risk communication, utilising the guiding principles from ‘*Klarspråk*’ to form their message. Many of these leading principles corresponded to several of the guidelines of Renn (2008) and Bouder (2010) from Table 2. These include identifying the audience, stating your most important message at the beginning and forming a clear and precise sentence (The Language Council of Norway, n.d). It was also clear that the message was perceived to be clear and easy to understand for the two nonintelligence informants, indicating success on this point.

However, there were few reflections on how the message resonated with the audience. One informant from PST noted that they had discussed if they should preform tests on how their communication could give negative emotions such as fear or unease. The informant meant that their job was to communicate the threat, regardless of how scary the message may be.

In risk science, much effort has been made to emphasise the importance of knowing how the risks are perceived by the public (e.g. Bouder (2015); Renn (2010); Sitkin and Pablo (1992)). This includes understanding the audience's risk perception, risk behaviour and other factors that influence both how the audience interprets the message but also how these factors influence decision making. Such knowledge can help risk communicators to design the right communication method, here by knowing the focal points that needs to be explained in detail or framed in a certain way (Bouder, 2015; Renn, 2010).

It could be argued that the intelligence agencies failed to understand the public's perspectives, at least to the fullest extent. Creating a clear message based on best practice principles is a well-grounded method of writing. However, the risk science perspective suggests getting a deeper understanding of the message implications going beyond the semantics. Taking the view of Sitkin and Pablo (1992), one should ask what sort of characteristics might be relevant and what implications this has for the public risk communication. For instance, one could make the argument that intelligence as a phenomenon and methodology has a quite distinctive nature. NIS and PST deal with risks on a broad spectrum, ranging from terrorist attacks with catastrophic potential to human lives to unwanted intelligence activity from foreign states. The problem characteristics differ greatly from, for example, the risk linked to a new food additive. The risks intelligence agencies deal with are often outside the audiences' control and degree of familiarity and, therefore, may lead to a public less inclined to accept the risks, according to the logic of Starr (1969). Likewise, the individual characteristics could generally differ according to the audience. One could easily make the case that boys in the age range of 17 to 21 years old, which was the audience the executive PST informant noted was hard to reach, needs a different communication approach than the audience of men in their 50s. Sitkin and Pablo (1992) argued that the characteristics affect how decisions are made. If the objective would be to communicate to the public for them to make better decisions, then risk science would suggest a more advanced understanding of these factors.

The results have indicated that both NIS and PST were in a position of high public trust. This is because both nonintelligence informants held them to be highly trusted and because the agencies received an annual 'organisational reputation' test in which they received a high score. In risk science, recommendations are to periodically test organisational trust (Bouder, 2015; Löfstedt, 2005; Renn, 2010). Trust is essential for public risk communication because it relates to how willing the public is to accept decisions or judgements on risk without questioning reliability of their assessment (Löfstedt, 2005).

One can argue that a good organisational reputation generally will corelate to an agency being highly trusted. One can further make the argument that the fact that these agencies have these tests indicates a conformity with risk science on this notion. However, none of the intelligence informants knew further details about this test other that their organisational reputation was high. As one of the informants noted, it could be fruitful to also understand more details relating to public trust. Furthermore, to understand why those who report low trust do so. Löfstedt (2005) referred to three dimensions of risk: *fairness*, *competence* and *efficiency*. To increase trust, one must know in which dimension of trust the organisation scores low. Such information is paramount to form a strategy to increase trust.

The distinctive nature of being an intelligence agency, as discussed in section 5.1, strongly affected the ability to be transparent. This view was also accepted from the nonintelligence informants, who had little expectations of transparency from the intelligence agencies. Risk science favours *reasoned transparency,* where information is explained, as opposed to *fishbowl transparency,* where raw data are published without explanation (Coglianese, 2009). Although one could probably state that both types of transparency would be present in all cases, multiple views on transparency can be taken in the case of NIS and PST. A strict risk science perspective would deem them not transparent because they only publish a fraction of data on their websites. They further offer few explanations on their judgements or actions. Taking a more nuanced view, where we acknowledge the potential negative consequences of revealing too much information, a slightly different argument can be made. One could argue that the fact that all the information they release to the public eye is thoroughly gone through, assessed and weighed indicates that their transparency is a governed process lining up with reasoned transparency. Their transparency, however scarce, is by no means randomly selected or the result of an 'archive upload' on their websites.

On the presupposition that both NIS and PST generally have high public trust, a strategy of top-down communication is an appropriate one for public risk communication (Löfstedt, 2005). Most of the analysed written material were of a neutral and clear manner, or what Bouder would refer to as 'one-size-fits-all communications' (2015, p. 13). The reason for this approach is, as the intelligence informants described, to create a written foundation for their further public risk communication. The annual assessments of both agencies, hence also the observed event in the present thesis, represent the general extent of content they want to communicate. From that point on, they would participate in debates, conferences, meetings or different platforms where they could adjust the communication approach and focal points according to the audience. From a risk science perspective, having a common baseline for public risk communication is something that can promote a unified and consistent message in public risk communication for members of the organisation. However, the common message needs to be further adapted towards different audiences (Bouder, 2015; Renn, 2010). There were several examples of both PST and NIS to utilise new platforms and methods to reach different audiences. NIS also performed trail and mini experiments on how the message resonated with certain target groups before the actual event to evaluate the degree of communication success. PST further held the strategy to use people from lower ranks in the organisation in public risk communications to level the balance of power, thereby promoting two-way communication. This indicates that the intelligence agencies strived for a good dialogue in their public risk communication, which conforms with risk science practice.

One challenging view is that most of the information available online and through media is ‘one-size-fits-all’ communication. This would include threat assessments, press releases, intelligence reports and so forth. These types of communications offer little to no further explanations on how these products are to be interpreted and utilised. The most obvious objection would be the possible misinterpretations on probability and uncertainty, as discussed earlier.

5.3 Concluding discussion—The aim of the message

Because the present thesis aimed to compare contemporary approaches in intelligence to risk science in terms of public risk communication, a reflection on comparability is needed. Is ‘intelligence threat communication’ even comparable to the field of risk communication? I would say this is certainly the case, even though the aspect of confidentiality challenges this view. Intelligence undisputedly deals with a wide range of societal risks, where the risk source is threats with malicious intent. The intelligence agencies also communicate how these risks take form and intervene in our daily lives. If we compare the purpose of intelligence in relation to decision making described by Omand (2019) and the functions of risk communication (see Table 1) described by Renn and Levine (1991), we can find many similarities. Both descriptions seek to communicate an understanding and explain phenomena by making sense of the world as they see it—often in conjunction with a prediction of how it is expected to affect the future.

The second point of reflection is how successful the intelligence agencies are with their risk communication. Going back to the initial quote this thesis started with, it is clear that the agencies' communication to the public has fallen short of the normal standards of intelligence communication described by Kennedy: 'Assumptions must be made explicit. The quality and freshness of the information must be revealed. Limitations in collection and analysis must be outlined. Conclusions must be well supported and well reasoned' (2008, p. 124). This may not necessarily mean that they are unsuccessful, but it raises some concerns.

One of the key findings is the two separate approaches to communicating—or, rather, in the case of NIS, *not* communicating—probability. Here, we can raise the question of what the agencies aim to achieve. What do they really want the audience to be left with after their communication?

In this view, the results indicate that NIS had the most consistent answer. The results from NIS stated primarily 'raising awareness' as the key objective, as well as attempting to be open and transparent about their work. Implicitly, we can understand that their intention is not to communicate exact probability for events or threats but rather give the recipient information about how the world is viewed from their perspective. Although this falls short of a strict risk science perspective on risk communication, it can be argued that NIS has achieved their goal. Their position strongly correlates to the 'enlightenment function', seen in Table 1 (Renn & Levine, 1991). This must also be seen in conjunction with their role in society because they are an intelligence agency whose job is to look outside Norwegian borders. As one of the informants noted, in this context, NIS describe the backdrop. Consequently, other organisations such as PST address how this backdrop affects Norwegian citizens. Utilising this logic, it becomes evident that PST is the agency mainly addressing the risks Norwegian citizens face, at least in the most practical sense.

If we go back to the same question of what aim the message of PST has, we can see a more ambivalent answer. PST also sees raising awareness as their main objective, with the underlying notion that this should prompt the public to report suspicious activity and implement measures to counteract the presented threats. Unlike NIS, PST has chosen to communicate probability in the form of linguistic expressions, sometimes accompanied by numeric values and/or a table showing the explained relation between numeric and linguistic values. There may be a discrepancy between wanting the public to use the threat assessment to evaluate the need for implementing measures and the agency's withholding of vital information, such as underlying knowledge and uncertainties. From a reader/receiver's perspective, it might seem hard to implement suitable measures when the information is given at such a superficial level. A case that illustrates this is a recent news article criticising PST for being too general by only stating the most obvious in a recent released threat assessment:[40] 'All the obviousness in the last openly accessible PST-document devaluate the respect of that the Norwegian Police Security Service has something important to say'[41] (Stanghelle, 2023, p. 3). The present thesis argues that PST is achieving their main goal to raise awareness in the public. However, communicating probability seems to be less of a success. The latter view was also taken from the PST informants themselves. Going back to the risk communication functions by Renn and Levine (1991), PST is overreaching in terms of how many functions they want their communication to fill compared with how much information they reveal, at least if we look at this from an ordinary citizen's point of view, where the communication is reduced to internet access and an occasional news programme. This may certainly not be the case in their day-to-day communication with public interest groups and collaborating parties because this communication is customised and adjusted accordingly.

A complete success can be hard to promote from a strict risk science perspective. However, from a broader societal perspective, one could promote a different view. As society steadily shifts towards post-trust society (Löfstedt, 2005), organisations such as PST and NIS also need to communicate to promote public trust. The current thesis recognises that reaching the public with a message that strongly needs restrictions is a hard task to succeed in. Utilising risk science, the present thesis presents multiple suggestions for partially remedying some of these challenging circumstances (please see section 5.4).

[40] This threat assessment is not one of the analysed documents in this thesis.

[41] Translated original: 'Alle selvfølgelighetene i det siste åpne PST-dokumentet devaluerer respekten for at Politiets sikkerhetstjeneste har noe viktig å si'.

5.4 Recommendations

Leaning on existing theory in risk science and the analysis of the present study, the current thesis proposes four practical recommendations for further practice. These suggestions, based on risk science, are put forth to remedy the negative effect of the intelligence agencies' need for protecting background information, sources, capabilities and so forth. More research is needed, but these risk science suggestions can contribute to the further elevation in quality and accuracy of intelligence-based public threat communication.

1. **Give more weight to uncertainties.**
   The results clearly indicate the need for intelligence agencies to protect certain information regarding supportive evidence and uncertainties. However, some information on uncertainty was found to be given at times and can be seen as useful. An example is as follows: 'PST's threat assessment is based on the information PST possess at any given time and will always be encumbered with a certain degree of uncertainty'[42] (PST-06, p. 1). Such information tells the recipient that there could be conflicting information that is unknown to the agency. Additionally, one could inform the recipient about the general (uncertain) circumstances in which intelligence agencies conduct their work. Uncertainty information is implicitly communicated several places today, for example, document PST-07 addresses the challenges PST face with the increased use of encrypted platforms (p.28). However, such information is not systematically addressed. In a practical sense this could mean using a portion of the communication to educate the public about some of the challenges they face. The intention would not be to be excusatory or reject critique, but rather to inform the public about the uncertainties that are linked to the issue at hand (e.g. the unpredictable nature of other people's intentions, radicalisation process and so forth). The audience would be informed that situations might be dynamic and that there could be (conflicting) information hidden in *'intelligence blind spots'*. As one of the informants noted, 'There is a lot we don't know as a security service, and we constantly try to uncover what we don't know—and that's known as intelligence blind spots' (Informant #5, PST). Such uncertainty communication, followed by information on what the agency is doing to reduce the intelligence blind spots, can be more

[42] Translated original: 'PST's vurdering er basert på den informasjonen PST til enhver tid besitter, og vil alltid være beheftet med en viss grad av usikkerhet'.

effective as opposed to simply stating a short overview of the situation followed by a linguistic probability expression.

2. **Look at alternative ways to portray probability.**

   PST and NIS had a dissented practice on whether probability should be communicated to the public. From a risk science perspective, the level of detail should harmonise with the audiences' needs and level of understanding (Bouder, 2009). One should therefore reflect on what function the communication intends to serve (see e.g. Table 1). Probability should generally be given with a numerical value, followed by a linguistic expression. However, the present thesis also supports the view of Mandel and Irwin (2021) that intelligence-given probability could be given in a numerical value followed by a short explanatory text/statement, especially in *public* risk communication. The reason for this suggestion is mainly because of the shortcomings related to revealing evidence and uncertainty, combined with the fact that the communication is directed to laypeople without prior knowledge of the field. Providing a rationale to the numerical probability would be a more informative approach, promoting a more accurate interpretation and situational awareness.

3. **Test for trust.**

   The results have indicated that there is the need for a more thorough testing of public trust. This could be done by survey and/or interviews. Over time, consistent studies can provide insights into the changes in the level of trust and rationale behind those who report low trust. Knowledge of public trust can help form strategies for trust building and identify possible groups with particularly low trust.

4. **Test how the message resonates with different audiences.**

   To understand how the message is received, there needs to be an evaluation of how the message resonates with the audience. This would include testing the level of understanding after communications, how people view these risks, bias, question framing and so forth. This could be done by survey and/or interviews. Such information could provide relevant information for designing public risk communication on specific issues or topics.

5.5 Limitations

It must be acknowledged that the methods utilised have limitations. The qualitative interviews provide representation from agencies and the media but were limited to two people from each category. This has implications for how we can interpret the results. The results have shown what these people said in the interviews, and this means that other people might have seen the questions in a different light, producing different answers. The method of observation was also restricted to one event, which was the main release of their threat assessments. This would naturally imply a more 'one-size-fits-all' communication because this is a formal event with politicians and news media. Hence, if we had observed another event with a more 'targeted' audience, we would probably be able to also evaluate more dialogue-based communication, thereby producing a slightly different analysis. Finally, the collected material represents a small portion of the totality of information available. One cannot exclude the notion that there is information from other sources, such as social media, news articles and so forth, that could further enlighten the problem statement.

The analysis cannot be used to generalise about current practice. However, the intelligence informants in the present study were all very experienced and held key positions in their field. With the added triangulation of the data, the results are a unique insight into an otherwise secluded sector. Few people have gained access to the reasoning behind their public communications. The results can induce further research and fuel discussions on both the success of current approaches, as well as bridging between intelligence and risk science.

6 CONCLUSION

Because the Norwegian intelligence agencies seem to be more communicative about how they view national security risks, the present thesis set out to compare contemporary practices with the existing developments on public risk communication derived from risk science. This was done by a triangulation of research methods: interviews, collection and examination and observation. Thematic analysis was utilised to categorise and interpret the results.

6.1 Comparing the intelligence approach with risk science

Further research is needed, but the results indicate that there are distinctive characteristics in the intelligence sector, particularly the need for confidentiality, which consequently takes the intelligence sector in a deviating path from risk science. This is especially evident in the principles of *assembling the evidence* and *analysis of options* from the public risk communication framework because a credible justification for the underlying evidence and uncertainties is nonexistent. This leaves the audience without a holistic understanding of the risks. The results further indicate deviations from risk science on matters where the need for confidentiality is less relevant. This is directly linked to *acknowledgement of public perspectives* and *authority in charge* from the public risk communication framework. An approach more in line with risk science would seek knowledge about how the public perceives risks such as terrorism, foreign intelligence activity, espionage and so forth to further strive for a successful communication. Furthermore, a periodical testing of public trust and the underlying dimensions of trust could help understand and form strategies to maintain or increase the level of trust. Knowledge of public perceptions and trust can have implications for how the intelligence agencies should frame their descriptions and communicate with the public and vulnerable groups of society.

The results have also shown several accounts of where the intelligence approach conformed with risk science. This was the most evident in *interacting with the audience* and partially in *authority in charge* from the public risk communication framework. The agencies have kept a constant and clear message but also customise the message according to the audience and communication platform. They are clear on outlining their jurisdictions, and for the public this often means that issues where other agencies are more fit to speak are pointed out.

6.2 Applications

How intelligence agencies plan and preform public communications has large implications for the public because such agencies address security risks that affect all areas of society. Some of the main findings are obvious, in that the intelligence agencies need to protect certain information. However, the present study contributes to filling the research gap on contemporary intelligence practice by providing valuable insights into this otherwise secluded aspect of national security. The need for confidentiality prohibits the intelligence agencies' adaptation of the risk science approach as a whole. However, the current thesis has argued that several risk science principles can be implemented to further elevate the quality of their public risk/threat communication. The present thesis suggests that the risk science approach where more weight is given to uncertainty and vital elements such as *trust* and *message evaluation* is tested and understood, can pave the way for a more successful communication. More research is needed, but as several intelligence agencies are critiqued for their public communication, a look at the 40 years of research and development in risk science can be a starting point for developing a contemporary intelligence approach.

6.3 Recommendations for further research

For further research, a larger study could be done with a broader selection of interview participants, combined with observation or survey. Such research could promote the development of a holistic framework or guiding principles for intelligence-based risk communication. This approach would be beneficial for both society and the intelligence sector because it can affect public trust when such communication is perceived to have failed (e.g., the case of the Al Noor terrorist attack in Oslo 2019).

REFERENCES

25. juni-utvalget. (2023). *Evaluering av PST og politiet*. Oslo

Aven, T. (2018). An emerging new risk analysis science: Foundations and Implications. *Risk Analysis*, *38*(5), 876-888. https://doi.org/10.1111/risa.12899

Aven, T. (2020). *The science of risk analysis: Foundation and practice*. Routledge.

Aven, T., & Thekdi, S. (2021). *Risk science: An introduction*. Taylor & Francis Group.

Aven, T., & Ylönen, M. (2018). The enigma of knowledge in the risk field. In T. Aven & E. Zio (Eds.), *Knowledge in Risk Assessment and Management* (pp. 27-47). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119317906.ch2

Balog-Way, D., McComas, K., & Besley, J. (2020). The evolving field of risk communication. *Risk Analysis*, *40*(S1), 2240-2262. https://doi.org/10.1111/risa.13615

Bouder, F. (2009). *A practical guide to public risk communication, the five essensials of good practice*.

Bouder, F. (2010). Risk communication: Can practitioners do better at risk communication? Using evidence to develop best practice. *European journal of risk regulation*(3), 280-285.

Bouder, F. (2015). Risk communication of vaccines: Challenges in the post-trust environment. *Current Drug Safety*, *10*(1), 9-15. https://doi.org/10.2174/157488631001150407103916

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Bråten, O. A. (2011). *Håndbok i konflikthåndtering: Forebygging av trakassering, trusler og vold*. Høyskoleforlaget.

Buckley, J. (2013). *Managing intelligence: A guide for law enforcement professionals*. CRC Press.

Budescu, D. V., Broomell, S., & Por, H.-H. (2009). Improving communication of uncertainty in the reports of the intergovernmental panel on climate change. *Psychological Science*, *20*(3), 299-308. https://doi.org/10.1111/j.1467-9280.2009.02284.x

Budescu, D. V., Por, H.-H., & Broomell, S. B. (2012). Effective communication of uncertainty in the IPCC reports. *Climatic change*, *113*(2), 181-200. https://doi.org/10.1007/s10584-011-0330-3

Budescu, D. V., & Wallsten, T. S. (1985). Consistency in interpretation of probabilistic phrases. *Organizational behavior and human decision processes*, *36*(3), 391-405. https://doi.org/10.1016/0749-5978(85)90007-X

Coglianese, C. (2009). The Transparency President? The Obama Administration and Open Government. *Governance (Oxford)*, *22*(4), 529-544. https://doi.org/10.1111/j.1468-0491.2009.01451.x

Covello, V. T. (2009). Strategies for Overcoming Challenges to Effective Risk Communication. In R. L. Heath & H. D. O'Hair (Eds.), *Handbook of risk and crisis communication* (pp. 143-168). Routledge. https://doi.org/10.4324/9780203891629-14

Covello, V. T., Winterfeldt, D. v., & Slovic, P. (1986). Risk communication: A Review of the Literature. *Risk Abstracts*, *3*, 171-182.

Curtin, D., & Meijer, A. J. (2006). Does transparency strengthen legitimacy? *Information polity*, *11*(2), 109-122. https://doi.org/10.3233/ip-2006-0091

Davies, P. H. J., Gustafson, K., & Rigden, I. (2013). The Intelligence Cycle is dead, long live the Intelligence Cycle. In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 56-76). Routledge.

Dieckmann, N. F., Peters, E., Gregory, R., & Tusler, M. (2012). Making sense of uncertainty: advantages and disadvantages of providing an evaluative structure. *Journal of risk research*, *15*(7), 717-735. https://doi.org/10.1080/13669877.2012.666760

Dohmen, T., Quercia, S., & Willrodt, J. (2019). *Willingness to Take Risk: The Role of Risk Conception and Optimism*. Berlin: SOEPpapers on Multidisciplinary Panel Data Research

Evalueringsutvalget. (2020). *Evaluering av politiets og PSTs håndtering av terror- hendelsen i Bærum 10. august 2019*. Oslo

Fischhoff, B. (1995). Risk perception and communication unplugged: Twenty years of process. *Risk Analysis*, *15*(2), 137-145. https://doi.org/10.1111/j.1539-6924.1995.tb00308.x

Fischhoff, B. (2013). The sciences of science communication. *Proceedings of the National Academy of Sciences of the United States of America*, *110*(Supplement 3), 14033-14039. https://doi.org/10.1073/pnas.1213273110

Flage, R., & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA). *Reliability & Risk Analysis: Theory and Application*, *2*(13), 109-115.

Frewer, L. J., Miles, S., Brennan, M., Kuznesof, S., Ness, M., & Ritson, C. (2002). Public preferences for informed choice under conditions of risk uncertainty. *Public understanding of science (Bristol, England)*, *11*(4), 363-372. https://doi.org/10.1088/0963-6625/11/4/304

Gill, P., & Phythian, M. (2018). *Intelligence in an Insecure World* (3rd ed.). Polity Press.

Guo, B. H. W., Yiu, T. W., & González, V. A. (2016). Predicting safety behavior in the construction industry: Development and test of an integrative model. *Safety science*, *84*, 1-11. https://doi.org/10.1016/j.ssci.2015.11.020

Hallgreen, C. E., Mt-Isa, S., Lieftucht, A., Phillips, L. D., Hughes, D., Talbot, S., Asiimwe, A., Downey, G., Genov, G., Hermann, R., Noel, R., Peters, R., Micaleff, A., Tzoulaki, I., & Ashby, D. (2016). Literature review of visual representation of the results of benefit-risk assessments of medicinal products. *Pharmacoepidemiology and drug safety*, *25*(3), 238-250. https://doi.org/10.1002/pds.3880

Halpern-Felsher, B. L., Millstein, S. G., Ellen, J. M., Adler, N. E., Tschann, J. M., & Biehl, M. (2001). The role of behavioral experience in judging risks. *Health Psychology*, *20*(2), 120-126. https://doi.org/10.1037/0278-6133.20.2.120

Hatlebrekke, K. A. (2021). *The problem of secret intelligence*. Edinburgh University Press.

Herman, M. (2009). *Intelligence Power in Peace and War*. Cambridge University Press.

Ho, E. H., Budescu, D. V., Dhami, M. K., & Mandel, D. R. (2015). Improving the communication of uncertainty in climate science and intelligence analysis. *Behavioral science & policy*, *1*(2), 43-55. https://doi.org/10.1353/bsp.2015.0015

Hrudey, S. E., Conant, B., Douglas, I. P., Fawell, J., Gillespie, T., Hill, D., Leiss, W., Rose, J. B., & Sinclair, M. (2011). Managing uncertainty in the provision of safe drinking water. *Water Science & Technology Water Supply*, *11*(6), 675-681. https://doi.org/10.2166/ws.2011.075

Jenkins, S. C., Harris, A. J. L., & Lark, R. M. (2018). Understanding 'Unlikely (20% Likelihood)' or '20% Likelihood (Unlikely)' Outcomes: The Robustness of the Extremity Effect. *Journal of behavioral decision making*, *31*(4), 572-586. https://doi.org/10.1002/bdm.2072

Jensen, K. K. (2004). BSE in the UK: Why the risk communication strategy failed. *Journal of agricultural & environmental ethics*, *17*(4-5), 405-423. https://doi.org/10.1007/s10806-004-5186-3

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2010). *Introduksjon til samfunnsvitenskapelig metode* (4th ed.). Abstrakt forlag.

Johnson, B. B., & Slovic, P. (1998). Lay views on uncertainty in environmental health risk assessment. *Journal of risk research*, *1*(4), 261-279. https://doi.org/10.1080/136698798377042

Jore, S. H. (2017). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European journal for security research*, *4*(1), 157-174. https://doi.org/10.1007/s41125-017-0021-9

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2), 263-291. https://doi.org/10.2307/1914185

Kasperson, R. E., Renn, O., Slovic, P., Brown, H., Emel, J., Goble, R., Kasperson, J., & Ratick, S. (1988). The Social Amplification of Risk: A Conceptual Framework. *Risk Analysis*, *8*(2), 177-187. https://doi.org/https://doi.org/10.1111/j.1539-6924.1988.tb01168.x

Kaufmann, G., & Kaufmann, A. (2015). *Psykologi i organisasjon og ledelse* (5th ed.). Fagbokforlaget.

Kennedy, R. (2008). *Of knowledge and power: The complexities of national intelligence*. Praeger Security International.

Kvale, S., & Brinkmann, S. (2015). *Det kvalitative forskningsintervju* (T. M. Anderssen & J. Rygge, Trans.; 3rd ed.). Gyldendal akademisk.

Larsson, P. (2010). Tillit til politiet : Fra nærhet til forhandlet legitimitet. In S. R. Runhovde (Ed.), *Tillit til politiet* (Vol. 2010:4, pp. 7-19). Politihøgskolen.

Leiss, W. (1996). Three Phases in the Evolution of Risk Communication Practice. *The Annals of the American Academy of Political and Social Science*, *545*(1), 85-94. https://doi.org/10.1177/0002716296545001009

Linden, S. v. d., & Löfstedt, R. (2019). *Risk and uncertainty in a post-truth society*. Routledge.

Löfstedt, R. (2005). *Risk Management in Post-Trust Societies*. Palgrave Macmillan

Man, S. S., Chan, A. H. S., Alabdulkarim, S., & Zhang, T. (2021). The effect of personal and organizational factors on the risk-taking behavior of Hong Kong construction workers. *Safety science*, *136*. https://doi.org/10.1016/j.ssci.2020.105155

Mandel, D. R., & Irwin, D. (2021). Uncertainty, Intelligence, and National Security Decisionmaking. *International journal of intelligence and counterintelligence*, *34*(3), 558-582. https://doi.org/10.1080/08850607.2020.1809056

March, J. G., & Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management science*, *33*(11), 1404-1418. https://doi.org/10.1287/mnsc.33.11.1404

Meloy, J. R., & Hoffmann, J. (2014). *International handbook of threat assessment*. Oxford University Press.

Miles, S., & Frewer, L. J. (2003). Public perception of scientific uncertainty in relation to food hazards. *Journal of risk research*, *6*(3), 267-283. https://doi.org/10.1080/1366987032000088883

NS 5832:2014. (2014). *Samfunnssikkerhet Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse*.

O'Neill, O. (2002). *A question of trust*. Cambridge University Press.

OECD. (2002). *(Organization for Economic Cooperation and Development) Guidance Document on Risk Communication for Chemical Risk Management*. Environment, Health and Safety Publications

Omand, D. (2010). *Securing the state*. Oxford University Press.

Omand, D. (2019). Et historisk tilbakeblikk. In S. Stenslie, L. Haugom, & B. H. Vaage (Eds.), *Etterretningsanalyse i den digitale tid : en innføring* (pp. 33-50). Fagbokforlaget.

Phythian, M. (2013). Introduction: Beyond the intelligence cycle? In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 1-9). Routledge.

Phythian, M., & Gill, P. (2013). From Intelligence Cycle to web of intelligence: Complexity and the conceptualisation of intelligence. In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp. 21-43). Routledge.

Piètre-Cambacédès, L., & Bouissou, M. (2013). Cross-fertilization between safety and security engineering. *Reliability engineering & system safety*, *110*, 110-126. https://doi.org/10.1016/j.ress.2012.09.011

PST. (2023). National threat assessment 2023. *The Norwegian Security Police Service*.

Reniers, G. L. L., Cremer, K., & Buytaert, J. (2011). Continuously and simultaneously optimizing an organization’s safety and security culture and climate: The Improvement Diamond for Excellence Achievement and Leadership in Safety & Security (IDEAL S&S) model. *Journal of cleaner production*, *19*(11), 1239-1249. https://doi.org/10.1016/j.jclepro.2011.03.002

Renn, O. (1991). Risk communication and the social amplification of risk. In R. E. Kasperson & P. J. M. Stallen (Eds.), *Communicating risks to the public: International perspectives* (Vol. 4, pp. 287-327). Springer Netherlands.

Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Earthscan. https://doi.org/10.4324/9781849772440

Renn, O. (2010). Risk Communication: Insights and Requirements for Designing Successful Communication Programs on Health and Environmental Hazards. In L. H. Robert & H. D. O'Hair (Eds.), *Handbook of Risk and Crisis Communication* (pp. 80-99). Taylor and Francis. https://doi.org/10.4324/9780203891629

Renn, O., & Levine, D. (1991). Credibility and trust in risk communication. In R. E. Kasperson & P. J. M. Stallen (Eds.), *Communicating Risks to the Public* (pp. 175-217). Springer Netherlands. https://doi.org/10.1007/978-94-009-1952-5_10

Ringdal, K. (2013). *Enhet og mangfold: Samfunnsvitenskapelig forskning og kvantitativ metode* (3rd ed.). Fagbokforlaget.

Schein, E. H., & Schein, P. (2017). *Organizational culture and leadership* (5th ed.). John Wiley & Sons, Inc.

Sherman, K. (1964). Words of estimative probability. *Studies in Intelligence*, *8*(4), 49-65.

Singer, J. D. (1958). Threat-perception and the armament-tension dilemma. *The Journal of conflict resolution*, *2*(1), 90-105.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the Determinants of Risk Behavior. *The Academy of Management review*, *17*(1), 9-38. https://doi.org/10.2307/258646

Skagerlund, K., Forsblad, M., Slovic, P., & Vastfjall, D. (2020). The affect heuristic and risk perception - stability across elicitation methods and individual cognitive abilities. *Frontiers in psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.00970

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285. https://doi.org/10.1126/science.3563507

Slovic, P. (2000a). Do adolescent smokers know the risks? In *The perception of risk* (pp. 364-372). Taylor & Francis.

Slovic, P. (2000b). Perception of risk. In *The Perception of Risk* (pp. 220-231). Taylor & Francis.

SRA. (2018a). Risk analysis: Fundamental principles. https://www.sra.org/wp-content/uploads/2020/04/SRA-Fundamental-Principles-R2.pdf

SRA. (2018b). Society for risk analysis glossary. https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Stanghelle, H. (2023, 14.06). Verdiløs trusselvurdering. *Aftenposten*, 1.

Starr, C. (1969). Social Benefit versus Technological Risk. *Science*, *165*(3899), 1232-1238. https://doi.org/10.1126/science.165.3899.1232

Stenslie, S., Haugom, L., & Vaage, B. H. (2019). *Etterretningsanalyse i den digitale tid : en innføring*. Fagbokforlaget.

Teigen, K. H., Juanchich, M., & Riege, A. H. (2013). Improbable outcomes: Infrequent or extraordinary? *Cognition*, *127*(1), 119-139. https://doi.org/10.1016/j.cognition.2012.12.005

Thagaard, T. (2018). *Systematikk og innlevelse: En innføring i kvalitative metoder* (5th ed.). Fagbokforlaget.

The Language Council of Norway. (n.d). *Klarspråk - Sjekkliste for skribenter*. Retrieved 06.04 from https://www.sprakradet.no/klarsprak/om-skriving/generelle-skriverad-bokmal/

The Norwegian Armed Forces. (2021). *Intelligence doctrine for the Norwegian Armed Forces (Forsvarets etterretningsdoktrine)*.

Thekdi, S. A., & Aven, T. (2021). Risk Science in Higher Education: The Current and Future Role of Risk Science in the University Curriculum. *Risk Analysis*, *41*(12), 2322-2335. https://doi.org/10.1111/risa.13748

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124

Vandepeer, C. (2011). *Rethinking threat: Intelligence analysis, intentions, capabilities, and the threat of non-state actors* [Doctoral dissertation, The University of Adelaide]. https://digital.library.adelaide.edu.au/dspace/bitstream/2440/70732/8/02whole.pdf

Viola, L. A., Laidler, P., & Viola, L. A. (2022). *Trust and Transparency in an Age of Surveillance*. Taylor & Francis group.

Wiedemann, P., Schütz, H., Spangenberg, A., & Krug, H. F. (2011). Evidence maps: Communicating risk assessments in societal controversies: The case of engineered nanoparticles. *Risk Analysis*, *31*(11), 1770-1783. https://doi.org/10.1111/j.1539-6924.2011.01725.x

Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). Guilford Press.

Zhang, D. C., Highhouse, S., & Nye, C. D. (2019). Development and validation of the General Risk Propensity Scale (GRiPS). *Journal of behavioral decision making*, *32*(2), 152-167. https://doi.org/10.1002/bdm.2102

APPENDIX

Appendix A – Interview guide

Intelligence personnel

1. Your organisation communicates risks to the public, one example being the annual threat assessment. What is the purpose/goal of such communication to the public?
2. When you communicate about risks to the public, how do you demonstrate that you have a credible basis for your position? For instance, that there is collected sufficient data, the quality of the data, uncertainties etc.
3. In the design of public risk communication, how do you acknowledge how lay people understand the presented risks?
4. When you communicate risks to the public, what is your approach to discussing different risk management options and the associated pros and cons?
5. When you communicate risks to the public, what is your approach to defining your organisations responsibilities, and where other organisations are better capable to step in?
6. When you communicate risks to the public, how important are factors such as *trust* and *transparency*?
7. Describe the interaction with your audience in public risk communication.
8. Looking at today´s practice of public risk communication in your organisation. How would you describe the level of success - and why?
9. What are your thoughts on improvements one could make to the organisation's public risk communication?

Personnel from national media

1. *The National Police Security Service and The Intelligence Service* communicate risks to the public, one example being the annual threat assessment. What do you perceive to be the purpose/goal of such communication to the public?
2. How do they demonstrate a credible basis for their position? For instance, that there is collected sufficient data, the quality of the data, uncertainties etc.
3. To what degree are the risks presented in a way that is easy to understand? Are there certain aspects of the risks you feel is not addressed or properly explained?
4. When dealing with a certain risk, there will be different options on how to handle that risk. How would you say the different risk management options, with their pros and cons, are reflected in their risk communication?
5. To what degree has the organisations made clear their own responsibilities, and where other organisations are better capable to step in?
6. How important would you say factors such as *trust* and *transparency* are for the organisations public risk communication?
7. Describe the interaction between the organisations and the audience (you) in public risk communication.
8. Looking at today´s practice of public risk communication for these two organisations. How would you describe the level of success - and why?
9. What are your thoughts on improvements one could make to the organisations public risk communication?