UNIVERSITY
OF OSLO

Master thesis

Listening to the Same Words and Hearing Different Things:

A study of the Norwegian Police Security Service´s challenges when communicating threats to the private sector

Magnus Brandt Lågøyr

Peace and Conflict Studies
45 ECTS Credits

Department of Political Science
Faculty of Social Sciences
Spring 2024

Word count: 32 272

Abstract:

This thesis attempts to answer the question “what are the main challenges in the PST´s threat communication to the private sector?”. To answer this question, I have conducted a discourse analysis building on data from interviews with security experts in the private sector, at the Private Sector Security Council (the NSR), and at the Police Security Service (the PST). Given that an intelligence product is “essentially the consumer’s understanding of the information presented, rather than the substance of the information itself” (Hatlebrekke, 2019, p. 73), I have decided to focus on how intelligence is interpreted when attempting to answer my research question. The focus on interpretation is built on the notion that “[i]t is perfectly possible for two people to listen to the same words and hear entirely different things” (Macintyre, 2019, p. 219). Misinterpreting the threat posed to one´s company will result in said company implementing measures which are not correctly scaled to the “true” threat said company is faced with. Given the private sector´s importance for the Norwegian total defence and national security, especially in the current geopolitical security situation, the result will therefore be a weakened total defence.

A significant argument made in this thesis is that the main challenge in the PST´s threat communication is a lack of dialogue between the PST and the private sector. This lack of dialogue results in a lack of a shared understanding of reality which negatively impacts the broader relationship between the PST and the private sector, and in a large potential for discourse failure: a situation in which the intelligence consumer (the private sector) interprets intelligence in a different way than what the intelligence producer (the PST) expects, due to individual factors relating to human cognition, and external factors like the amount of dialogue between the producer and the consumer (Neumann and Smith, 2005; Hatlebrekke, 2019).

Acknowledgements:

To teachers and academics, from Rolf Dyhre to the lecturers at the University of Sheffield and at the University of Oslo, who taught me the skills and gave me the *confidence* needed to complete this thesis.

To my supervisor Øivind Bratberg, for embarking on the process of researching this rather unusual thesis topic with me, and for all the help and support along the way.

To my interviewees, who´s willingness to participate and give honest and direct answers provided the backbone to this study. I hope that you will find this thesis interesting and useful for the important work you do.

To my soon-to-be colleagues at Advansia, especially Jack, Arne Christian, Miriam, Stig, and Christina, for providing me with the inspiration for this thesis, and the background knowledge upon which it is built.

To Thom and Kamil, for introducing me to Yorkshire Tea.

To my friends and my family, for the love and support along the way.
A special thanks to mom and grandad for proofreading the thesis.

To my fellow PECOS students, for laughs, long lunches, and lifelong friendships.
We are finally here. We made it. And we did it together.

Finally, to my girlfriend Mari, who´s unconditional love and support is more important to me than I can express.

What follows is the product of everyone´s love, support, and guidance.
It represents what I have learned, and the stepping stone to what comes next.

Oslo, May 2024

Abbreviations:

CIA: Central Intelligence Agency

EOS-services: Intelligence, Surveillance, and Security Services

E-tjenesten: The Defence Intelligence Service

FBI: Federal Bureau of Investigation

MI5: Military Intelligence section 5

NOU: Norwegian Official Report

NSM: The National Security Authority

NSR: The Private Sector Security Council

NTV: National Threat Assessment

PST: The Police Security Service

WEPs: Words of estimative probability

Table of Contents

Chapter 1: Introduction

As has been written in a plethora of political speeches, opinion pieces and academic papers over the course of the last two years or so, Russia´s invasion of Ukraine on the 24th of February 2022 drastically changed international relations and security politics (Lawless, 2023). Many governments across Europe, which might have taken their nation´s security for granted since the end of the Cold War, suddenly realised they weren't as secure as they once thought. One consequence of the War in Ukraine has been an increased willingness among politicians to surge money into the armed forces and weapons manufacturing. Norway, which is the country of focus in this study, is no exception to this. Since the start of the war, the Norwegian Government has announced a number of proposals for increased investments in the Norwegian Armed Forces (see for example, Norwegian Ministry of Defence, 2023), and in the arms industry (Indrebø-Langlo and Jacobsen, 2023). However, a nation´s security is not only a product of the relative strength of their military compared to unfriendly actors such as Russia.

Since World War 2, Norwegian defence policy has been organised around a concept called "total defence" (FFI, 2022). Traditionally, total defence (or "totalforsvar" in Norwegian) was "based on the idea of utilising society's limited resources as effectively as possible, primarily at the upper level of the crisis spectrum (armed conflict)" in order to "safeguard Norway's territory, independence and national values, and to protect the civilian population“ (Norwegian Ministry of Defence and Norwegian Ministry of Justice and Public Security, 2018, p. 9). "Society´s limited resources" refer to both military and civilian resources, which is what differentiates total defence from a more traditional military-centred definition of defence. In the early 2000s, the total defence concept was subject to a modernisation process. The main change emanating from this process was the expansion of the concept to include:

> "mutual support and cooperation between the Norwegian Armed Forces and civil society in connection with contingency planning, crisis management and consequence management across the entire crisis spectrum - from peace via security policy crisis to armed conflict" (Norwegian Ministry of Defence and Norwegian Ministry of Justice and Public Security, 2018, p. 10).

Given that Norway´s security and defence policy is built on this total defence concept, non-military actors, like private sector companies, play a key role regardless of the geopolitical context of the day. However, increasing geopolitical tensions, partly driven by the aforementioned War in Ukraine, have further enhanced the importance of the private sector (NSM, 2023). The fact that we have seen reports stating that "Chinese spies have targeted the Dutch semiconductor, aerospace and maritime industries to try to strengthen China's armed forces" (Reuters, 2024) further underlines this point. This is something I will expand on in the context chapter.

This thesis focuses on a key, yet understudied, part of the Norwegian total defence. Namely, how the Norwegian Police Security Service (PST) communicates about threats to the private sector, which enables the private sector to protect themselves against said threats. Specifically, it assesses challenges related to how the intelligence products shared by the PST is understood by private sector actors. The PST is the Norwegian domestic security service, and one of the three Norwegian intelligence and security services (PST, 2023a). In chapter 2.3.1, I expand on what the PST does, why I have chosen to study its external threat communication, and the relationship between the PST and the two other services.

For the purpose of this study, I have focused on what one interviewee referred to as the "A-team", or the best-in-class of the private sector security actors. According to the Private Sector Security Council (the NSR), there is a strong correlation between who actively engages with the threat intelligence shared by the PST, and the size of the companies these people work at (NSR, 2021, p. 15). Hence, I will focus on larger companies, whose security officials are part of the "A-team".

Furthermore, in order to further specify which organisations I wanted to interview, I have decided to focus on the NSR and its owners as they, according to the Total Preparedness Commission (2023, p. 195), represent the breadth of the private sector in a security context. As I will return to in the methods chapter, I asked the NSR to help me identify which specific companies I should contact. Given that this part of the private sector is more exposed to intelligence activity and threats from state actors than it is to terrorism, this thesis focuses on intelligence activity and threats from state actors.

Looking at other parts of the private sector which less frequently engage with threat intelligence is absolutely a worthwhile topic of study. However, if I were to focus on this group, a more relevant question to ask would be why they don’t engage with the threat intelligence they receive from the PST, and not how they interpret it. In the interest of maintaining a narrow focus suitable to the scope of a master´s thesis, I have decided not to investigate this issue or group of companies.

The reason for looking at interpretation is that an intelligence product is “essentially the consumer’s understanding of the information presented, rather than the substance of the information itself” (Hatlebrekke, 2019, p. 73). Furthermore, studying how the intelligence products shared by the PST are interpreted is highlighted as a key area of further study in the only research project which has assessed the PST´s external communication. Namely, Bergersen´s recent PhD thesis which looks at the dilemmas of communicating about terror threats in Norway (Bergersen, 2023). In her thesis she writes that:

> “Another apparent expansion would therefore be to take the concept of public threat perception more explicitly into consideration. From the interviews with the PST, it became apparent that how the public understands and relates to the external communication from the PST, such as the periodic threat assessment reports, was something they did not know much about. […] How the communication is received and understood by the public, and whether this matches the motivation, rationale, and justification behind the communication […] therefore seems like a study worthwhile (Bergersen, 2023, p. 278).

Given that Bergersen´s PhD thesis has a different focus than this thesis has, for example that she focuses on terror threat communication to the general public and not on interpretation of intelligence, I have based my study on the work of other scholars. Primarily, the late Norwegian intelligence studies scholar and intelligence officer, Kjetil Anders Hatlebrekke (see for example, Hatlebrekke, 2019) and David R. Mandel at York University in Canada (see for example, Mandel and Irwin, 2021; Mandel, 2022; Irwin and Mandel, 2023).

1.1 Research question

The research question this thesis seeks to answer is:

What are the main challenges in the PST´s threat communication to the private sector?

In order to answer this question, I have conducted relational, semi-structured interviews with the PST, the NSR, and private sector security officials. My thesis project, hereunder the data construction (interviews), received approval from SIKT on November 9th, 2023. I used the data from these interviews as the basis for an interpretivist discourse analysis which unpacks how the interviewees understand several key issues like how much uncertainty the PST´s assessments are imbued with. This is because, as mentioned, I am interested in how the PST´s threat communication is interpreted, and not just *what* the PST communicates. The decision to focus on challenges related to interpretation was a result of studying the literature on intelligence communication and finding interpretation to be a key challenge (see for example, Irwin and Mandel, 2023).

To structure my analysis and work with this study more broadly, I have devised three sub-questions which are answered in the three sub-chapters in my analysis chapter:

Sub-question 1: How is confidence and the consequences of sharing it understood?

The first sub-question focuses on how the interviewees interpret confidence, and whether they think confidence should be shared (which it currently isn't). Simply put, a confidence assessment is a way of expressing how much uncertainty a given threat assessment is imbued with. The discussion around confidence is used as a form of "proxy" to explore the degree to which the private sector and the PST have a shared understanding of reality, and how much dialogue the two parties have. It also gives a window into how the PST thinks about intelligence sharing.

Sub-question 2: How do the PST and the private sector view each other and their relationship?

The second sub-question helps further unpack why, and to what extent, there is a lack of dialogue between the PST and the private sector through looking at how they understand their relationship. Given that the amount of dialogue between intelligence producer (the

PST) and intelligence consumer (the private sector), and the relationship between the two, have a direct impact on how the consumer understands intelligence (see for example, Hatlebrekke, 2019, p. 227, 2019, p. 73), assessing this helps answer the main research question.

Sub-question 3: Is there a potential for discourse failure?

The third and final sub-question draws on the answers to the first two sub-questions to assess whether the discursive relationship between the PST and private sector companies indicates a potential for misconceptions on the receiving end. Discourse failure is a situation in which the intelligence consumer interprets intelligence in a different way than what the intelligence producer expects, due to individual factors relating to human cognition, and external factors like the amount of dialogue between the producer and the consumer (Hatlebrekke, 2019).

1.2 Main argument

A significant argument made in this thesis is that the main challenge in the PST´s threat communication is a lack of dialogue between the PST and the private sector. This lack of dialogue results in a large potential for discourse failure, and in a lack of a shared understanding of reality which negatively impacts the broader relationship between the PST and the private sector. This argument is based on several examples from my interviews where the PST and the private sector have differing understandings of reality, which in turn demonstrate the lack of dialogue. These examples include how much confidence the PST´s assessments have, who has agency to improve the relationship between the PST and the private sector, and whether its ability or willingness which impacts the degree to which the PST engages in dialogue and shares intelligence with the private sector.

1.3 Thesis outline

The rest of this thesis is structured as follows. In chapter 2, I provide a more detailed description of the context within which my study is situated. This includes explaining how the private sector deals with threats, and how threats are currently communicated to the private sector. In chapter 3, I lay the theoretical and conceptual foundation for the rest of the thesis through discussing the existing literature on intelligence sharing, what confidence and probability is, and how intelligence is (mis)interpreted. Chapter 4 contains an explanation of how I have gone about conducting this study, including my methodological approach, choices made along the way, and their implications. In chapter 5, I answer my three sub-questions by analysing the interview data I have constructed. Finally, chapter 6 concludes this thesis by summarizing the other chapters and providing a clear answer to my research question. I round off the chapter by discussing limitations to my study, policy suggestions, and ideas for further studies.

This study is highly interdisciplinary, just like the field of peace and conflict studies. In this thesis, I draw on insights from fields like psychology, intelligence studies, political science, security studies, and communication. Together, insights from these and other fields enable me to provide a comprehensive answer to my research question.

Chapter 2: Why the private sector needs information

If the following chapters and their contributions to knowledge are to be understood by someone not already intimately familiar with the topic at hand, as well as the Norwegian national security structure, this chapter needs to provide a thorough introduction to the empirical context surrounding this thesis. The fact that the topic is not commonly discussed within the realm of political science and peace and conflict studies further necessitates this effort. Hence, the overarching aim of this chapter is to give the reader the contextual understanding needed to be ready to delve into the forthcoming more academically and theoretically complex chapters, while also providing the contextual foundation for the discourse analysis. Furthermore, in this chapter I will also lay out the case for this thesis´ empirical relevance for current affairs and for the field of peace and conflict studies.

2.1 The role of the private sector in the total defence

The importance of the role the private sector plays in Norway´s total defence is highlighted in a number of recent major reports. I will now draw on three such reports in order to demonstrate the importance of the private sector, namely the Norwegian National Security Authority´s (the NSM) "Advice on National security" (NSM, 2023), and the two Norwegian Official Reports (NOUs) resulting from the work of The Defence Commission (2023) and The Total Preparedness Commission (2023). After demonstrating the ever-present importance of the private sector, I will move on to show why the private sector has become increasingly important in light of the current geopolitical situation. In addition to serving the purpose of providing the necessary background information for the reader ahead of the chapters to come, this part of the text is also key to the thesis´ relevance claim. That being said, before I explain why the private sector is important, I want to briefly highlight two ways of understanding the private sector´s role in the total defence concept, and in emergency preparedness more broadly.

2.1.1 How to understand the role of the private sector

The Total Preparedness Commission report presents two perspectives on how we can understand the role of the private sector in emergency preparedness and total defence (The Total Preparedness Commission, 2023, p. 182). The first one, titled "the society perspective", views the private sector as being an integrated part of a larger security ecosystem consisting of state authorities, as well as private and voluntary actors. A central part of this perspective is that the private sector actively contributes to the nation´s total defence and to their own security by their own volition. Simply put, the society perspective assumes that the private sector´s participation in the total defence is a result of them viewing themselves as part of a larger collective (the society) (The Total Preparedness Commission, 2023, p. 182).

The second way of viewing the private sector´s role in the total defence and national emergency preparedness is called “the authority perspective”. According to this view, the private sector´s contribution to the total defence is a result of national authorities having a need for, or directly requiring that the private sector contributes (The Total Preparedness Commission, 2023, p. 182). This means that the private sector is viewed as more of an external contributor than an integrated part of an ecosystem, like it is in the society perspective.

While the Total Preparedness Commission (2023, p. 183) states explicitly that it primarily builds on the authority perspective, I will not make any determinations when it comes to which perspective I prefer. Therefore, the reason for presenting these two perspectives in this chapter is that they will be incorporated into the questions in the interviews in order to unpack how the actors see themselves and their relationship to the other party. Furthermore, it is also useful to be aware of these perspectives for this study and the topic writ large.

2.1.2 Why the private sector is (always) important

One of the first things which is emphasised in the NSM´s “Advise on National Security” report is the concept of mutual dependency between different levels of security (NSM, 2023, p. 8). The report states that due to things like digitalisation, technological developments, and increasingly overlapping value and supply chains, the boundaries between the different levels of security are becoming less and less clear (NSM, 2023, p. 8). As a result, the four levels, namely, the individual, companies/organisations, society, and the state are becoming increasingly interdependent (The Total Preparedness Commission, 2023, p. 155). While the state still has the overarching responsibility for national security, the state simply can´t effectively carry out that responsibility without cooperating with the three other levels in light of the increased interdependence and changing threat landscape (NSM, 2023, p. 9). The latter part of this, namely the changing threat landscape, is something I will return to in the next sub-section on why the private sector is currently extra important for national security.

This idea of mutual dependency, or interdependency if you like, is something which is interlinked with the total defence concept, especially the modernised version of it. Building on the aforementioned NOUs and the NSM´s report, I will now concretise the mutual dependency and take it from theoretical concept to tangible parts and mechanisms. Concretising the mutual dependency between the state and the private sector first and foremost rests on an assessment of the values inherent in private sector companies, and the importance of these values for national security. I will not cover all of the values or assets in the private sector in-depth as that would take up far too much space. However, I will provide a brief overview of some illustrative examples which help concretise the mutual dependency.

Traditionally, the state relied on the private sector for a limited number of assets like food, transportation, and fuel (The Total Preparedness Commission, 2023). These are key assets, without which defending a nation or responding to a crisis is simply not possible. Today, the state, hereunder the armed forces, still relies on the private sector for these three things. However, as society has developed, and as what is required for crisis management and war has developed with it, the state security apparatus has become increasingly reliant on the values and assets inherent in the private sector. For example, NATO relies on the private sector for about 90 percent of their transport needs during large military operations (The Total Preparedness Commission, 2023, p. 157). Furthermore, more traditional assets needed for the defence of a nation like weapons are now also produced by private sector companies, a fact which further underpins just how dependent the state is on the private sector in Norway (The Defence Commission, 2023).

Another example of this is communication networks/IT systems, both physical cables and servers, as well as websites and cloud storage systems. In today´s hyperconnected digital world, the way we store information and communicate with each other is heavily dependent on IT systems. In a crisis situation and in day-to-day protection of a state and its interests, IT systems are also crucial. Previously, the state owned and operated a lot of these functions and pieces of infrastructure. However, today, about 90 percent of transatlantic internet traffic, including military communication, goes through subsea fibreoptic cables which are owned and operated by private actors (The Total Preparedness Commission, 2023, p. 157).

Yet another example is knowledge about and production of things like weapons, AI powered technology, and energy. As I will return to in the next section on why the private sector is currently extra important, energy production infrastructure, as well as knowledge about cutting edge energy production and storage technology, is becoming increasingly interlinked with national security. This means that the state is increasingly dependent on private companies like Equinor and research institutions like the Institute for Energy Technology (IFE, no date) as they control knowledge about such topics and the physical infrastructure needed to extract resources like oil and gas. However, as these companies can´t protect these assets by themselves, they are also dependent on the state for protection, as we saw in the aftermath of the Nord Stream 2 pipeline explosion (The Defence Commission, 2023, p. 236).

Lastly, so-called "dual use" technology is another asset the private sector holds which creates a mutual dependency between them and the state. Simply put, dual use technology is technology which has both civilian and military applications (PST, 2023a, p. 20). Examples include advanced sensor technology, autonomous systems, quantum computers, and various pieces of hardware used in the oil and gas sector. This kind of technology is highly sought after by foreign nations as it can play a key part in the development of military systems which they would not be able to acquire directly. States like Russia and China therefore attempt to acquire this kind of "dual use" technology indirectly, often through shell corporations, as that is easier than trying to acquire the final military system itself (this is referred to as covert acquisitions) (E-tjenesten, 2023, p. 24).

The fact that foreign nations are actively trying to acquire dual use technology from Norwegian companies (see for example, E-tjenesten, 2023) means that the private sector needs assistance from the security services (for example in the form of information) in order to guard against covert acquisitions. Furthermore, in addition to the fact that it is in the state´s interest to prevent such covert acquisitions, the security services and the military are also themselves dependent on the dual use technology developed and produced by private sector companies. Therefore, this is another example of the mutual dependency between the public and the private sector.

Having demonstrated why the private sector is key to national security, and mutually dependent on the state, I will now show why the current geopolitical situation has further enhanced the private sector´s importance, and the aforementioned mutual dependency.

2.1.3 Why the private sector is (currently extra) important

While the Norwegian state is always mutually dependent on the private sector, it is increasingly so in light of the War in Ukraine. I now want to highlight two reasons why the private sector is both increasingly important, and thereby also more exposed to attacks. Namely, the increased importance of energy for Norway and Europe´s security, and the deterioration of the separation between civilian and military targets (The Defence Commission, 2023).

In September 2022, in the wake of the attack on the Nord Stream gas pipelines, the Norwegian government decided to make Equinor and Gassco subject to the requirements of the Security Act (Hovland and Holmes, 2022). This means that they must comply with stricter rules for security, and that they can be allowed to receive some classified information. Equinor and Gassco are two of the largest companies in the oil and gas industry, and the decision to make them subject to the Security Act was a result of the government deciding to classify the extraction of petroleum, as well as the transport of gas in pipes to Europe, as foundational national functions in light of the increased importance of energy (Hovland and Holmes, 2022). This decision reflects a larger trend in Norwegian and European politics where energy production, transport, and storage are increasingly being seen as tied to national security due to Russia´s use of energy as a weapon in the War in

Ukraine (LaBelle, 2023). Given that production, transport, and storage of energy in Norway is dominated by private sector actors (The Total Preparedness Commission, 2023), it follows logically that the private sector´s importance is increased in tandem with the increased importance of energy.

In addition to seeing energy being turned into a key security asset as a result of the War in Ukraine, the war has also contributed significantly to the deterioration of the separation between civilian and military targets (The Defence Commission, 2023, p. 96). This is by no means a new trend. However, the war has certainly contributed to it, while also making it more visible and concrete for Norway and for Europe writ large.

According to The Defence Commission (2023, p. 96), the deteriorating respect for international law and for the separation between civilian and military targets means that authoritarian states (like Russia) will be more likely to attack civilian infrastructure like that which is operated by the private sector. Hence, the War in Ukraine will not only increase the value of the assets held by the private sector, but also the likelihood that they will be subject to attacks and threats like intelligence activities, something we have already seen a number of examples of (see for example PST, 2023a). This means that the private sector needs to be prepared for these kinds of threats and reduce risk when possible. Given that how the private sector deals with threats is one of the central themes in this thesis, I will now give a brief overview of the main analytical tools the private sector use for dealing with threats and risk. This section will also form the basis for the subsequent section which covers how threats are communicated, since information about threats is at the heart of how the private sector deals with threats and risk.

2.2 How the private sector deals with threats and risk

While the state doesn’t mandate a specific type of risk assessment method, most if not all public and private organisations base their assessments on one of two “Norwegian standard” (NS) risk assessment methods. Namely, either NS 5814, which is most commonly used for “unintentional unwanted events” with quantifiable risks such as the risk of an oil platform collapsing or the risk associated with flooding, or NS 5832 which is most commonly used for “intentional unwanted events” such as espionage or terrorist attacks (Busmundrud *et al.*, 2015). While both methods help one to calculate risk, they differ in the way they go about it. If one utilises NS 5814, one calculates risk as a product of the *probability* of an unwanted event occurring, times the *consequence* of that event. That results in a number, which signifies the level of risk associated with that specific scenario or event (Busmundrud *et al.*, 2015).

On the other hand, NS 5832, which for reference is the method highlighted in the PST´s national threat assessment which I will return to in the next section, calculates risk as a product of a *threat actor* attempting to exploit a *vulnerability* in order to get access to a *value* (Busmundrud *et al.*, 2015; PST, 2023a, p. 2). This model is commonly referred to as the three factor or triangle model as it is often visualised as a triangle with the three factors on each corner of the triangle, and risk being the size of the triangle. In order to reduce risk according to this model, one has to shrink one of the corners (preferably the vulnerability), which would then reduce the overall size of the triangle (or the amount of risk). The key takeaway here is that in order to know how much risk one is left with, one has to have an accurate assessment of one´s values and vulnerabilities, as well as of the potential threat actors (Busmundrud *et al.*, 2015).

The last part is what this thesis focuses on. More specifically, this thesis dives into how information about threat actors is communicated from the PST to the private sector. Information which the private sector uses to protect their assets/values, which in turn is also the state´s values due to the mutual dependence between the private sector and the state under the total defence concept. Rounding off this context chapter, I will now explain how the PST currently communicates threats to the private sector. This section will also include a brief explanation of the PST´s responsibilities and their relation to the two other Norwegian security and intelligence agencies. I will then round off this chapter by making some concluding points on the empirical "real life" context within which this thesis is situated.

2.3 How threats (and uncertainty) are currently communicated

Fundamentally, intelligence services´ main responsibility is to "provide decision-making support to decision-makers" (Hatlebrekke, 2019, p. 23). Traditionally, this support has been primarily provided to state actors such as the government and the police. However, as this chapter has laid out in detail, the private sector also needs information. And due to the mutual dependency between the state and the private sector, it’s also in the state´s (or the intelligence services´) interest to provide them with that information.

In this final part of the context chapter, I give an overview of the Norwegian security and intelligence services. Then, I explain how the PST currently communicates threats, specifically focusing on the National Threat Assessment (NTV). Finally, I explain the “puzzle” which sits at the heart of my research question. Like the rest of the context chapter, this section does not dive into the academic literature/research on this topic. However, this sub-chapter does serve as the steppingstone to the theoretical framework chapter which goes in-depth on the academic literature on threat communication.

2.3.1 Norwegian security and intelligence services

Before looking at how the PST currently communicates threats to the private sector, I need to explain the relationship between the different Norwegian security and intelligence services in order to justify why I have chosen to focus on the PST in this thesis. Norway has three intelligence and security services, often referred to as the three EOS-services. EOS is short for intelligence, surveillance, and security in Norwegian (The EOS committee, no date). The three EOS-services are the PST (the Police Security Service), the NSM (the National Security Authority) and E-tjenesten (the Defence Intelligence Service). While they all contribute to Norwegian national security and all publish annual unclassified threat/risk assessments, they all slightly differ in terms of their responsibilities. There is also a fourth EOS-service, namely the FSA (Defence Security Department) (The EOS committee, no date). However, the FSA only works within the confines of the military, and is most often not included when one refers to the EOS-services.

Being the domestic security service, similar to the FBI (Federal Bureau of Investigation) in the US, the PST´s main task is to “prevent and investigate serious crimes that threaten national security” (PST, 2023a, p. 0). In practice, this means that they are responsible for protecting against terrorism/extremism, espionage, threats to dignitaries, sabotage, and proliferation of weapons of mass destruction. E-tjenesten, which is formally part of the

Norwegian military, has some of the same kinds of thematic responsibilities like terrorism and espionage. However, as they are the foreign intelligence service, similar to the CIA (Central Intelligence Agency) in the US, they operate abroad where they aim to gather intelligence which can form the basis for decision making by the Norwegian state, and for the Norwegian military during missions abroad (E-tjenesten, 2023). Finally, the NSM is Norway's directorate for preventive security. As opposed to E-tjenesten and the PST, which both *collect* intelligence on threat actors, the NSM is mainly focused on assessing vulnerabilities and recommending risk-reduction measures based on the threat assessments offered by the PST and E-tjenesten (PST, 2023a, p. 0). The NSM also bears responsibility for preventing and responding to serious cyber security incidents.

The reason why I have chosen to focus on the PST and how they communicate to the private sector is closely linked to how and what the three EOS-services communicate. Given that I want to focus on how information about threats is communicated, looking at the NSM would not be suitable as while they do communicate directly with the private sector, they mainly communicate about risks and vulnerabilities. E-tjenesten, on the other hand, does share some information about threat actors openly, for instance in their annual public threat assessment called "FOCUS" (E-tjenesten, 2023). However, they almost exclusively communicate to the state, the PST, the NSM, and to the military. Furthermore, they are also famously difficult to get access to, which makes them ill-suited for this kind of research project.

The PST, on the other hand, not only communicates about threats, but they also do so directly to the private sector. According to the PST themselves, they have a responsibility for communicating with the private sector, and every day PST officials meet with private sector companies to provide them with advice (PST, no date). This is not to say that studying the PST is without its challenges. However, I will return to those challenges in the methods chapter. Now, I will introduce what the PST refers to as the cornerstone of their external threat communication (PST, no date), namely the National Threat Assessment.

2.3.2 The National Threat Assessment (NTV)

The National Threat Assessment, or NTV for short, is an annual threat assessment report published by the PST. In the 2023 edition of the NTV, three categories of threats are assessed: state intelligence activities, extremism/terrorism, and threats to dignitaries (PST, 2023a). The PST presents two different, but closely related kinds of assessments in the NTV, namely a verbal statement of the probability of a certain threat occurring and a description of those threats. For example, when presenting their assessment of the threat from right-wing extremists in the 2023 edition of the NTV, they say that there is an "*even chance* that right-wing extremists will attempt to carry out terrorist acts in Norway in 2023" (PST, 2023a, p. 31). Accompanying this statement about the probability is a broader description of right-wing extremist ideology, means of attack, as well as changes and trends.

It's important to note that neither the NTV, nor other pieces of non-classified information shared by the PST for that matter, contains information about what's called *confidence*. Or simply put how certain the PST is about the probability they assign to the different threats. This means that confidence is a measure of the uncertainty associated with an assessment. In the theoretical framework chapter, I go more in-depth on what confidence is, what influences confidence/uncertainty, and the relationship between probability assessments and confidence. For now, I want to round off this chapter by highlighting the "puzzle" my thesis seeks to unpack. Then, I conclude this chapter with a short summary of the chapter´s main points, and how they relate to the theoretical framework and the rest of the thesis.

2.3.3 Puzzle

Sharing what are often bits and pieces of information about threats with the private sector, due in part to information being classified, presents a number of challenges. For example, in the wake of the aforementioned Nord Stream explosion, the PST admitted in conversations with the NSR that it struggled to communicate to the private sector (Hovtun, 2023). Furthermore, the Total Preparedness Commission (2023, p. 117) writes that in addition to there being challenges when the PST or the other intelligence and security services want to communicate to the private sector, there is normally also a lack of willingness and ability to share information. That being said, the PST recently announced that they are establishing a new group for external activities within the counterintelligence division which will focus on communicating threat assessments to among others the private sector (PST, 2023b), so there is clearly some appetite to improve their external threat communication. When assessing the literature on this topic in the theoretical framework, I dive deeper into the concrete challenges associated with threat communication. However, I will highlight one challenge and the accompanying consequences related to that challenge here; namely the dilemma associated with sharing intelligence publicly.

It is perhaps easy to say that the "solution" to the PST´s communication challenges is to just share all the information that the private sector asks for. And while that will seemingly solve the issues resulting from the private sector having an incomplete information picture upon which they base their risk assessments, sharing all that information also has a clear downside. According to Chinese war philosophy,

> "[i]ntelligence needs to be kept secret, simply because the power of intelligence knowledge will be diminished or, at worst, vanish if the adversary knows what the opponent knows or does not know" (Hatlebrekke, 2019, p. 21).

In this case, this means that if the PST shares all that it knows publicly (or in an unclassified/unsecure manner), that effectively reduces the value of said information. Hence, the PST needs to strike a balance between sharing enough so that the private sector and other actors who do not have access to classified information can develop adequate risk-reduction measure, but not so much that the value of what they know is reduced too much. Furthermore, as I will discuss in-depth in the theoretical framework chapter, even if the private sector has access to information, there is no guarantee that they will interpret that information "correctly" which could also result in them basing their risk assessments on a faulty knowledge foundation.

That leads me to the puzzle this thesis will shed light on, namely what challenges the PST is faced with when communicating about threats to the private sector. In a situation where having a private sector which is prepared to deal with the current threat landscape is key to national security as part of the total defence concept, trying to solve this puzzle is highly relevant and important for contemporary policymaking.

2.4 Summary

In this chapter I have provided an overview of the larger context surrounding my thesis, and how my specific research question is connected to the field of peace and conflict studies. I have done so by showing that how the PST communicates threats to the private sector relates to the broader field of security and defence studies through the total defence concept and mutual dependence. I have also explained why my research question is relevant in today´s geopolitical situation by showing how the importance of the private sector in the Norwegian total defence has been enhanced following the outbreak of the War in Ukraine. In the next chapter I go into depth on the academic literature in the field of threat communication. This does, together with the context provided in this chapter, provide the foundation for the questions I pose in the interviews, as well as the framework for the discourse analysis.

Chapter 3: Theoretical framework

“Intelligence can never be truths, only uncertain theories about the future” writes Hatlebrekke (2019, p. 35). Building on an understanding of intelligence as something fundamentally uncertain, this chapter assesses the academic literature on intelligence and uncertainty/confidence, including what intelligence is, why it is (not) shared, and how it is interpreted. Due to the rather limited number of studies which look at my case in particular, both in terms of my country of choice and the issues related to sharing confidence, I will draw on studies which go slightly beyond the specific focus of this study. For example, this means drawing on a study of how individuals interpret probability words, which has been conducted in Canada (Irwin and Mandel, 2023), in addition to pieces which look at confidence in particular (see for example, Dieckmann, Mauro and Slovic, 2010).

The goal of this chapter is to lay out the current state of the literature on intelligence communication, thereby establishing the research gap this thesis aims to contribute to filling. In doing so, this chapter introduces the theories and studies which form the theoretical foundation for the data construction and subsequent discourse analysis.

3.1 What is intelligence?

The foundation for a study, regardless of topic, must be a clear definition of what it is one is studying. The reason for this is that without a clear definition of the core concepts, such as intelligence in this case, the reader would struggle to both understand and interrogate the findings of said study (Goertz and Mahoney, 2012). This is particularly the case when one is dealing with so-called “essentially contested concepts” like terrorism or freedom, which are concepts surrounded by so much disagreement about their meaning that arriving upon a mutually agreed definition is nigh on impossible (Gallie, 1955). However, it is also important when studying a concept like intelligence, as how one defines it has major implications for how one goes about studying it. For the purpose of this study, I view intelligence as being “secretly generated wisdom beyond the limits of formal reasoning that makes uncertain estimates less uncertain, and that consequently generates political, strategic and operational advantages over adversaries” (Hatlebrekke, 2019, p. 265).

Examples of pieces of intelligence which would be communicated from the PST to the private sector would be which kinds of industries, what knowledge, and which people Russian intelligence officials would be interested in. Furthermore, it could also be information about how foreign intelligence officials would go about getting access to those things. These are all things which are discussed in the National Threat Assessment (NTV), which was introduced in the context chapter (PST, 2023a).

Furthermore, and arguably even more importantly, this study builds on Hatlebrekke´s understanding of an intelligence product, which is what is communicated to an intelligence consumer (for example a private sector actor):

> "The intelligence product is therefore essentially the consumer's understanding of the information presented, rather than the substance of the information itself – a perspective that highlights the importance of a good relationship between the intelligence producer and the intelligence consumer" (Hatlebrekke, 2019, p. 73).

The reason why this definition is key to my thesis is that it emphasises the importance of interpretation of information and the importance of the relationship between the intelligence producer and the intelligence consumer. In a way, this definition of intelligence also legitimises and underscores the importance of studying the interpretation of intelligence and the relationship between consumer and producer, which is exactly what this thesis does.

What "the relationship between consumer and producer" is, or what it should be, is something which warrants further attention. It is also something which has received some scholarly attention over the years. One view, often referred to as Sherman Kent´s view, is that there should be a sufficient amount of distance between the consumer and the producer, so that independence and objectivity could be maintained (Brown, 2020). This view became the dominant one following the so-called "Intelligence Debate of 1949", also known as the "Kent-Kendal debate" (Brown, 2020).

However, as more recent studies have shown (Marrin, 2008), simply presenting objective facts to policymakers won't end up changing their minds as "even when policymakers do make use of intelligence, it is often only insofar as it supports their preordained conclusions"

(Brown, 2020). Hence, it is argued that one has to move from Kent´s emphasis on independence and objectivity to a system were "independence is desirable and objectivity is necessary, but relevance is mandatory" (Brown, 2020, para. 31). In practice, this means cultivating a relationship between intelligence consumer and intelligence producer in which the producer knows what intelligence is relevant for policymakers, while still being independent and objective enough to present intelligence which might break with the views of policymakers (Hatlebrekke, 2019). In fairness, Kent did say that intelligence "cannot serve if it does not know the doers' minds; it cannot serve if it has not their confidence" (Brown, 2020). However, what Brown (2020) argues, which I tend to agree with, is that Kent´s view of the relationship tended to overemphasise the importance of independence and distance between consumer and producer. In his work, Hatlebrekke (2019) also highlights that a good dialogue between producer and consumer is key in order to avoid discourse failure. Hence his focus on the "importance of a good relationship between the intelligence producer and the intelligence consumer" (Hatlebrekke, 2019, p. 73). What discourse failure is, and its link to the relationship between consumer and producer, is something I return to in chapter 3.5.2.

3.2 Analytical certainty

In addition to clearly defining intelligence, analytical certainty also needs to be defined and discussed. Not least owing to the fact that intelligence professionals and regular people alike consistently fail to clearly define and separate the two parts of analytical certainty, namely likelihood and confidence (Irwin and Mandel, 2023, p. 943). Simply put, analytical certainty is a collective term for the two measures used to describe the quality and contents of an intelligence assessment (Mandel, 2020, chap. 19, p. 6). In chapter 2.3.2, which introduced the National Threat Assessment (NTV), I briefly explained that confidence is a measure of the uncertainty associated with an intelligence assessment, and that likelihood is a measure of how likely it is that a certain event will take place. This distinction mirrors what is found in statistical analysis where the value of a coefficient associated with a particular variable rises and falls independently from the associated confidence interval/p-value. In this sub-chapter, I will go more in-depth and discuss both what the two parts of analytical certainty are, how they relate to each other, and which factors influence confidence.

3.2.1 Likelihood

As I explained in the context chapter, intelligence organisations like the PST use likelihood expressions like “even chance” or “highly likely” when communicating about threats (PST, 2023a). The use of these so-called “words of estimative probability”, or “WEPs”, in intelligence communication was originally proposed in a piece by Sherman Kent (1964), who is known as the father of intelligence analysis (Brown, 2020). Kent´s proposal was a result of him, during the course of his work within the US intelligence community, experiencing that there was a great deal of confusion and misinterpretation associated with the way intelligence was communicated (Kent, 1964). Specifically, in the piece where he proposes the use of WEPs, he cites having experienced that policymakers and intelligence producers alike had vastly different interpretations of the words used to describe probability, in addition to the fact that they also used a wide variety of different words for describing the same level of probability (Kent, 1964). He therefore proposed using a standardised set of probability words tied to numerical ranges. Today, most if not all intelligence organisations and military organisations use such standardised WEPs and accompanying numerical tables to explain what the different words mean (see for example PST, 2023a, p. 3; Mandel, 2020).

The other main way of communicating likelihood is solely using numerical expressions of probability. This means that instead of writing that there is an even chance of an event occurring, one would say that there is a 50 percent chance of an event occurring. However, this way of communicating is way less frequently used by intelligence producers due to their preference for sharing linguistic likelihood assessments as opposed to numerical ones (Irwin and Mandel, 2023, p. 944). Both linguistic and numerical ways of communicating likelihood by using one simple expression like “even chance” or “50 percent chance” are known as point assessments (Dieckmann, Mauro and Slovic, 2010).

While intelligence producers prefer to *share* linguistic likelihood assessments, they simultaneously prefer to *receive* numerical likelihood assessments, something which is known as the “communication mode preference paradox” (Irwin and Mandel, 2023, p. 944). This indicates that while the intelligence services think that numbers are more useful, there are some dilemmas associated with sharing numbers which leads them to share words even when they think that numbers are more useful. I will return to this when discussing why intelligence is (not) shared in chapter 3.3. Before doing so, I want to cover what confidence is, how it is communicated, and what influences it.

3.2.2 Confidence

As opposed to likelihood expressions, which explain how likely it is that a certain event occurs, confidence assessments are a way of expressing the level of uncertainty associated with a particular intelligence assessment. The level of confidence associated with an assessment is often communicated by saying that an assessment has high, medium, or low confidence (Mandel, 2020, chap. 19, p. 6). High confidence would for example indicate that the assessment is based on well-corroborated information, undisputed reasoning, and so on. As with likelihood assessments, there are also issues associated with how individuals interpret such verbal confidence assessments. For example, how uncertain is an assessment which has "medium" confidence? This is an issue I will return to in chapter 3.5 which covers how intelligence is interpreted.

Another way of communicating confidence is so-called likelihood ranges. These express confidence by providing a kind of "outer boundary" to point assessments, which in practice looks something like this: there is a 5 % chance of an attack occurring, but the probability could be as low as 1 % or as high as 10 % (Dieckmann, Mauro and Slovic, 2010, p. 990). Linking back to the comparison I made between analytical certainty and statistical analysis, sharing a likelihood range is comparable to sharing the values of the outer bounds of where the coefficient for a variable might be "in reality".

Unlike likelihood, which is regularly shared in open intelligence products, confidence is not shared as often. At least not in Norway, which is the country of focus for my study. However, in the US, confidence has been shared more regularly over the last two decades, largely because of tensions related to the Iraq invasion in 2003. The failure to communicate uncertainty associated with the Iraq weapons of mass destruction (WMD) assessments was pointed to as one of the reasons for why the intelligence was misunderstood, something which ultimately became the pre-text for the Iraq War (Mandel and Irwin, 2021, p. 559). In the aftermath of this, lawmakers mandated the sharing of confidence assessments in intelligence products (*Intelligence Reform And Terrorism Prevention Act Of 2004*, 2004, sec. 1019). Furthermore, the US intelligence community (including, but not limited to, the FBI and the CIA) also saw fit to begin to share confidence information publicly in an attempt to avoid being blamed for making incorrect assessments. The reason being that sharing confidence assessments would allow them to rightly point out that the assessments they were making were uncertain, which helps them move away from the impression that the intelligence community is omniscient (Mandel, 2020, chap. 19, p. 1).

The Norwegian intelligence services are yet to be drawn into an intelligence scandal as serious as that which resulted in the Iraq War. However, during an episode of the Norwegian debate programme “Dagsnytt 18”, during which the 2022 Oslo terror attack was discussed, the then Deputy Head of the PST was questioned about the PST´s decision to lower the terror threat level and issue an assessment which said that the likelihood of an Islamic terrorist attack was decreased prior of the attack taking place (*Dagsnytt 18 - 13. januar 2023*, 2023). Given that information about confidence is classified, she could not reveal the confidence associated with those assessments. However, her answers clearly indicated that there is a level of uncertainty associated with said assessments. This fits into a broader debate in Norway about threat assessments in which the PST has been criticised for not accurately assessing or communicating the threat level (Stanghelle, 2023). And while the issues surrounding the 2022 Oslo terror attack are not as major of a scandal as that surrounding the Iraq War, it has still led to criticisms of the PST and questions about its ability to assess threats and protect Norway against those threats (Torres, 2023).

While confidence is normally used to measure the uncertainty of a likelihood assessment relating to the future, it can also relate to intelligence assessments about past events. An example of this is when the US intelligence community put out a statement saying that they believed with high confidence that the attack on the Al-Ahli hospital in Gaza was conducted by Palestinian militants (Seligman, 2023). Another example would be US intelligence community assessments about the origin of the coronavirus (Office of the Director of National Intelligence and National Intelligence Council, 2021). This stands in contrast to assessments about future events (which is the focus of this study) where both likelihood and confidence are involved. I will now discuss the factors which impact said confidence assessments, focusing on factors which impact confidence related to assessments of future events.

3.2.3 Factors influencing confidence

Currently, there is no internationally agreed standard for how to communicate confidence, let alone a standard definition of what confidence is. This fact is highlighted in a NATO report on the topic (Mandel, 2020). In the aptly named chapter "*How intelligence organisations communicate confidence (unclearly)*", the report states that:

> "Ultimately, we argue that current confidence standards are poorly conceived, ambiguous, vague, and unclear, and may effectively augment the potential for miscommunication" (Mandel, 2020, chap. 19, p. 2).

Hence, I am not able to state definitively which factors are considered to influence confidence. However, what I will do is to highlight some factors pointed to in the NATO report. This will help explain the concept of confidence to the reader of this thesis. Furthermore, it will also be a key part of the theoretical foundation for the part of the thesis which seeks to get at the PST´s and the private sector´s understanding of confidence and uncertainty in intelligence.

Confidence, or uncertainty assessments, needs to be understood in light of the simple fact that intelligence assessments are fundamentally uncertain (Hatlebrekke, 2019). This is due to the inherent uncertainty associated with trying to predict the future. We can´t know for certain what happens in the future since what has yet to happen is simply unknowable. Predictions can never be 100 % certain, and hence there will always be some degree of uncertainty associated with any intelligence assessment. However, some predictions about the future are less uncertain than others. The NATO report (Mandel, 2020, chap. 19, p. 11) lays out five factors which impact confidence: Source reliability, information credibility, evidence consistency/convergence, strength of logic/reasoning, and quantity and significance of assumptions and information gaps. These can again be separated into two different categories: factors related to incoming information (the first three factors), and factors related to how said information is analysed (the final two factors).

An example of how incoming information might contribute to uncertainty would be that the source who provided the information often or sometimes provides information which turns out to be untrue or inaccurate. This can be due to them not having a complete understanding of a situation, because they are subject to deception tactics from those whom the source is trying to acquire information about/from, or because the source itself is trying to deceive the receiver of the information that it provides (Mandel, 2020, chap. 19). An example of how analysis of information can contribute to uncertainty would be when analysts must make assumptions about a threat or situation due to the lack of information about said threat or situation. If these assumptions are based on weak reasoning and are being used to bridge significant knowledge gaps, the final intelligence product would be imbued with more uncertainty as it is based on educated guesses as opposed to pieces of intelligence (which themselves are imbued with uncertainty) (Mandel, 2020, chap. 19).

Having introduced likelihood and confidence as constitutive elements of analytical certainty, I will now move on to why analytical certainty and intelligence products more broadly are (not) shared. The chapter introduces what the literature tells us about why intelligence is or is not shared. As opposed to just looking at why confidence is not shared, I also look at the literature on why intelligence assessments are not shared, due to the lack of academic literature on the former. Following the chapter on intelligence sharing/communication, I move into the other part of intelligence communication, namely how intelligence is interpreted.

3.3 Why is intelligence (not) shared?

Broadly speaking, two main categories of reasons for (not) sharing intelligence are identified in the literature. The two categories are cultural reasons, or reasons related to the *willingness* to share intelligence, and structural reasons, or reasons related to the *ability* to share information. This distinction can be found in the Total Preparedness Commission´s Report (2023, p. 117), which states that the ability and willingness to share intelligence is lacking within the Norwegian EOS-services. It can also be found in a master´s thesis which looks at information sharing in the work to combat radicalization and violent extremism in Scandinavia (Bråthen, 2021).

I will now lay out some of the main cultural and structural factors which, according to the literature, might impact intelligence sharing from the PST to the private sector. The goal is to introduce the reader to some of the arguments which were used by interviewees when I questioned them about the reasons why the PST has decided against sharing confidence information. Introducing these arguments also helps me identify key narratives surrounding this decision, and interpret what those narratives in the broader discourse can tell us beyond just why the PST has made the decision it has.

3.3.1 Ability to share

The PST´s ability to share intelligence information with the private sector is largely shaped by the Security Act (2018, para. 5), and rules relating to the dissemination of classified information. The reason for this is that a lot of the intelligence information which the PST has is classified. This means that even if the PST wanted to share intelligence products with the private sector, that would not be possible if the information is not de-classified, or if the actor receiving the information was privy to classified information. As a sidenote, the Total Preparedness Commission (2023, p. 117) also highlights that there is a lack of infrastructure for sharing classified information. Furthermore, the Total Preparedness Commission (2023, p. 117) also states that too few people have been given the security clearance needed to be privy to said information.

Both the Total Preparedness Commission report (2023) and literature on this topic highlight laws and regulations as key determinants of whether security services share information or not. For example, the aforementioned thesis by Bråthen (2021) argues that laws, in addition to cultural factors relating to willingness to share, have a direct impact on the PST´s information sharing in the field of terrorism prevention. Furthermore, an opinion piece by Hovtun (2023) also highlights how laws, regulation, and missing infrastructure limits the PST´s ability to share intelligence assessments with relevant private sector actors. The piece therefore proposes the establishment of new systems for information sharing between the security services and the private sector, writing that all sensitive information doesn’t need to be classified and that all unclassified information doesn’t need to be public (Hovtun, 2023).

3.3.2 Willingness to share

The willingness to share is a far more complicated matter than the ability to share. This is because while the ability to share is shaped by (more or less) static laws, the PST´s willingness to share is a result of multiple dynamic dilemmas and cost-benefit assessments. In the context chapter I presented the total defence concept and why the private sector´s importance for the total defence means that it is in the security service´s interest to share intelligence with the private sector. Furthermore, I also presented the dilemma related to the diminishing value of open intelligence. The idea here is that the value of intelligence is predicated on the adversary not knowing that their opponent knows or does not know something (Hatlebrekke, 2019, p. 21). By making intelligence openly available, one is therefore inadvertently reducing its value.

There are many dynamics and dilemmas which can impact the PST´s willingness to share information aside from the two laid out in the context chapter. I now want to highlight one dynamic in particular. While it hasn't been assigned a name in the literature, I will refer to it as the "getting credit, avoiding blame" dilemma. The core of this dilemma is that, broadly speaking, security services want to communicate in a way which protects them from getting the blame if an unwanted event occurs, and gives them credit when they accurately predict or prevent an event from occurring (Dieckmann, Mauro and Slovic, 2010; Hood, 2011). This becomes a dilemma because broadly speaking, the way security and intelligence services go about this is to share verbal expressions of probability without information about confidence (Dieckmann, Mauro and Slovic, 2010). The reason for this is that studies indicate that security services assume that sharing isolated WEPs, as opposed to numerical expressions of probability and accompanying confidence assessments/ranges, reduces the amount of blame they will get when things go south. This is because they think that making so-called "point assessments" which are more open to interpretation, as opposed to including probability ranges, makes them seem more competent and knowledgeable (Dieckmann, Mauro and Slovic, 2010). Notably, it doesn't seem as this is the case in the US intelligence community as previously mentioned (Mandel, 2020, chap. 19, p. 1).

The issue with this way of trying to get credit and avoid blame, and the reason why I refer to this as a dilemma, is that this way of communicating intelligence is prone to misinterpretation (Irwin and Mandel, 2023). Therefore, by trying to get credit and avoid blame, security services are increasing the chance of the intelligence they are communicating being misunderstood. Hence, there is a dilemma between communicating in a way which gives them credit and avoids blame, and communicating is a way which impacts the risk of misunderstandings. The dilemma arguably mirrors key aspects of the "communication mode preference paradox" mentioned in chapter 3.2.1, where intelligence producers express a preference for sharing linguistic likelihood assessments, while they simultaneously prefer to receive numerical likelihood assessments (Irwin and Mandel, 2023, p. 944). This is because while they find numbers to be more useful as they are more precise and less open to (mis)interpretation, they simultaneously want to leave their assessments open to interpretation as that will enable them to present what is the "correct" interpretation once an event happens or doesn't happen (Hood, 2011; Mandel, 2022, p. 5). Thereby getting credit or avoiding blame regardless of whether they correctly or incorrectly assessed the threat.

A study from the US casts serious doubt on the validity of the underlying assumption inherent in the security services chosen way of trying to get credit and avoid blame. According to the study, it is not the case that withholding confidence assessments leads intelligence and security services to get more credit and less blame. In the study, the authors test how participants react to being presented with intelligence products which include a variety of ways of expressing probability and confidence (Dieckmann, Mauro and Slovic, 2010). By testing how participants react to being presented with intelligence with and without confidence information, the study gets at the validity of the core assumption underpinning security services´ approach to avoiding blame and getting credit.

Broadly speaking, the study finds that when looking at intelligence assessments in hindsight, people tend to assign less blame to assessments which communicate uncertainty/confidence through the inclusion of probability ranges (Dieckmann, Mauro and Slovic, 2010). The study also finds that people don't view security services as less competent or trustworthy as previously thought, assigning more credibility to assessments which are transparent about confidence. According to the authors of the study, one reason for these findings might be that when point assessments are shared without confidence information, the assessment gives a false impression of accuracy, and it is therefore viewed as more wrong if the prediction turns out to be incorrect. On the other hand, assessments which are explicit about the inherent uncertainty in the assessment are less prone to this fault as they are viewed as less absolute and precise (Dieckmann, Mauro and Slovic, 2010, p. 997). This is something which lends support to the decisions the US intelligence community made about sharing confidence assessments post-Iraq (Mandel, 2020, chap. 19, p. 1). The downside to sharing confidence is that decision makers can be more hesitant to act on such "imprecise" information, which again might influence a security service´s decision about whether or not to share confidence information (Dieckmann, Mauro and Slovic, 2010, p. 988). If one is working under the assumption that the PST is aware of the US study which challenges the conventional wisdom on how to avoid blame, this downside might be why they have decided against sharing confidence in their assessments. This is something which will be picked up on in the analysis chapter when analysing whether it´s ability or willingness which is shaping the PST´s intelligence sharing policies.

Another explanation is that the PST still thinks that not sharing confidence makes them seem more knowledgeable. If so, this would lend support to Mandel´s so-called ignorance hypothesis which states that there is a "widespread ignorance of scientific principles and values, within both intelligence and policy communities" (Mandel, 2022, p. 79) which leads intelligence communities to make decisions about for example uncertainty communication based on "untenable assumption[s]" (Mandel, 2022, p. 87) as opposed to scientific studies. Either way, getting to the bottom of what their decision to not share is based on, whether that is a well-informed weighing of pros and cons, or on assumptions about how the intelligence consumer would react, is a key goal of this study.

Having explained one of the main factors which might impact the PST´s willingness to share intelligence with the private sector, I will now look at theories and studies related to how intelligence is interpreted by the consumer. It´s worth noting that there is a degree of overlap between this sub-chapter on willingness to share, and the chapter on how intelligence is interpreted. The reason for this is that how intelligence is interpreted can play a role in the PST´s willingness to share. This is because how the PST assumes that the private sector understands the PST can play into their calculations about whether or not so share. If the PST for example thinks that the private sector has a good understanding of the degree of uncertainty in their threat assessments, they might not find it necessary to share their confidence assessments.

3.4 What impacts interpretation?

Before I delve into how intelligence is interpreted, I need to provide some background on what shapes how people interpret and perceive the world around them more broadly. I have chosen to look at two tightly connected sets of factors which impact interpretation. Namely those tied to individual perception and those tied to institutional norms and ways of thinking. While there are many theories and approaches to explaining and understanding how people interpret the world around them, I have decided to focus on a constructivist approach (Halperin and Heath, 2020), in addition to sociological institutionalism which itself builds on constructivism (Hall and Taylor, 1996). I have done so because these two are suitable theoretical foundations for my project as they are both compatible with the view that "[t]he intelligence product is […] the consumer's understanding of the information presented, rather than the substance of the information itself" (Hatlebrekke, 2019, p. 73).

Constructivism emphasises how knowledge is not simply received passively, but interpreted by the individual in light of their understanding of reality and the context within which they exist. Simply put, according to constructivist thought, "meanings are socially and discursively constructed" (Halperin and Heath, 2020, p. 365). For this thesis, the important takeaway from this is the belief that how meaning is constructed, or how individuals interpret the world around them, is shaped in part by that individual´s prior experiences and pre-existing understanding of the world around them (often referred to in psychology as schemas). A simple way to explain this idea is to look at how two individuals with different prior experiences and understandings of the world respond to a question like "how much snow is a lot of snow?". When prompted with this question, someone from Norway and someone from Egypt close to the Sahara Desert are likely to give vastly different answers, as what they consider "a lot of snow" will be based on their prior experiences which to some extent is shaped by where they are born and raised.

Based on my own experience of doing my bachelor's degree in the UK, more specifically in the city of Sheffield, when it occasionally snowed there, my fellow students and I would see the same amount of snow and have vastly different opinions on how "much" snow it really was. This was because what they considered to be "a lot of snow" there was completely different from what I was used to from back home in Norway. I experienced that British students´ frame of reference for what constituted a large amount of snow was vastly different from mine. That being said, where one is from is hardly the only thing which impacts interpretation from a constructivist´s viewpoint. For example, if a British student regularly goes on skiing holidays in the Alps or in Norway, their understanding of how much snow "a lot of snow" is, is likely to be shaped by those experiences. This example of how two people can look at the exact same thing and come to different conclusions about its size closely mirrors some of the issues related to interpretation of WEPs and confidence in intelligence communication which I cover in chapter 3.5. For example, when a person who has never worked for the PST is told that there is "a lot of intelligence activity" in Norway, that person will likely interpret that statement differently than a person working in the PST who is privy to detailed and concrete examples of current and past intelligence activity. Finally, it's also possible for one person to look at the same amount of snow in two different places and conclude that it constitutes "a lot of snow" in one place (for example the Sahara desert) and "not a lot of snow" in another place (like Norway). This highlights the importance of the context within which something is interpreted, which is also important to keep in mind when analysing intelligence communication.

Another thing which shapes interpretation is institutions. According to the sociological institutionalism theory, institutions shape the values, norms, behaviour and "the very terms through which meaning is assigned in social life" of the individuals which reside in them (Hall and Taylor, 1996, p. 948). Basically, according to this theory, institutions shape who we are and therefore also how we interpret the world around us if one believes, as constructivists do, that meaning is "socially and discursively constructed" (Halperin and Heath, 2020, p. 365) on the back of one´s prior experiences, and so on. In sociological institutionalism, the reason why institutions shape the individual´s interpretation is tied to something called "the logic of appropriateness". Simply put, the logic of appropriateness perspective states that individuals will act in accordance with the rules and norms of the institutions they take part in “because they are seen as natural, rightful, expected, and legitimate” (March and Olsen, 2004, p. 3). Because individuals are shaped by the institutions they are a part of, they are likely to mirror or at least be aware of the dominant views in those institutions (or organisations). Hence, interviewing individuals should provide a good window into the thinking within a given organisation.

When trying to incorporate the sociological institutionalism theory into this thesis, one key problem arises. Namely that the definition of what an institution is, is rather unclear because the term concept has been applied to so many different things (Alvesson and Spicer, 2019, p. 205). This is commonly referred to as conceptual stretching, and is something which happens when trying to fit an increasing amount of things into the same concept, thereby stretching or expanding the definition of what can be counted as being part of that concept until the concept loses its meaning (Sartori, 1970). Therefore, for the concept “institution” and the broader sociological institutionalism theory to be useful, there is a need to clearly state what I mean when I refer to institutions.

When referring to institutions in this thesis, I am primarily referring to concrete organisations, like the PST or a private sector company, or broader groups of organisations like the private sector. This does not mean that I am ignoring the impact of other things that are commonly referred to as institutions. However, as I am primarily interested in studying how organisations think, through interviewing individuals within those organisations, and not how the common person in the street thinks, trying to get at all the different institutions (broadly defined) which have an impact on interpretation is not the focus. That being said, it is useful to keep in mind that there are multiple things which might impact how someone interprets something, if and when I find differences in how people within the same institution interpret something.

3.5 How intelligence is interpreted

In addition to supplementing the chapter on intelligence sharing, this chapter will mainly serve as a foundation for trying to understand how the PST and the private sector understand intelligence, and perhaps even more importantly how they understand each other´s understanding, since that is key to being able to answer my research question. In this chapter I will therefore cover key studies and theories surrounding intelligence interpretation, including the theory of discourse failure which can help shed light on why intelligence is misinterpreted.

3.5.1 Misinterpretation of confidence and likelihood

As previously mentioned, confidence and likelihood are often conflated by intelligence professionals and regular people alike (Irwin and Mandel, 2023, p. 943). A study conducted in Norway has also found this to be the case (Halvorsen, 2020). Not only do people struggle to understand the two, as is evident from the fact that confidence has been used to express likelihood in several instances (Friedman and Zeckhauser, 2012). A study has also shown that when confidence and likelihood are communicated, people tend to see them as moving in tandem as opposed to being two independent indicators (Irwin and Mandel, 2023, p. 953). This point warrants further explanation. It is true that the two are linked in so far as confidence assessments are used to express the level of uncertainty associated with a likelihood assessment. However, in a study by Irwin and Mandel (2023), respondents tended to think that when an event has a high likelihood of occurring, that means that the assessment has higher confidence and vice versa. Again, just like in statistical analysis, it is simply not the case that a higher coefficient or likelihood assessment goes hand in hand with a lower p-value or a higher confidence assessment.

Another problem identified in the literature on this topic has to do with how people interpret WEPs. While the goal of using WEPs is to reduce the potential for misinterpretation, studies show that the one WEP is associated with a vast variety of numerical interpretations (Mandel and Irwin, 2021). Even when presented with tables which explain what the WEPs truly mean, like what is done in the PST´s NTV (PST, 2023a), people still assign a large range of different numerical interpretations to the same WEPs, though shared understanding is improved somewhat (Mandel and Irwin, 2021, p. 562). While this exact issue has not been tested for when it comes to confidence words, it stands to reason that one could find similar issues with confidence words given how much misinterpretation surrounds the use of confidence words.

Furthermore, it also seems to be the case that when presented with a confidence assessment for a likelihood assessment, the level of confidence impacts people´s interpretation of what “likely” or “unlikely” means. According to one study,

> “the term likely communicated with low confidence elicited a significantly lower midpoint interpretation (i.e., was judged less probable) than the term unlikely communicated with high confidence” (Irwin and Mandel, 2023, p. 952).

On its face, this doesn’t make a whole lot of sense. However, several other studies have emphasised how people struggle to separate and interpret confidence and likelihood (for list of studies, see Duke, 2023, p. 2). So, while the quote presented here seems to make little sense, when we are aware of the difference between confidence and likelihood, this is an example of just how much of a challenge intelligence and security services are faced with when trying to communicate using WEPs. What is unknown so far is if this challenge is as large in the private sector (in Norway) as it is for the intelligence professionals and “common people” surveyed in these studies. This is a gap in the literature which this thesis seeks to contribute to filling.

3.5.2 Discourse failure

So why is this happening? Why do intelligence professionals and regular people alike understand likelihood and confidence in so many different ways? One theory which might help explain this is called “discourse failure”. First introduced in a piece by Neumann and Smith (2005), discourse failure is a situation in which the intelligence consumer interprets intelligence in a different way than what the intelligence producer expects, due to individual factors relating to human cognition, and external factors like the amount of dialogue between the producer and the consumer (Hatlebrekke, 2019). Discourse failure is therefore a situation in which there is a disconnect between the intelligence consumer´s and the intelligence producer´s understanding of reality.

Given that “the intelligence product is […] essentially the consumer’s understanding of the information presented, rather than the substance of the information itself” (Hatlebrekke, 2019, p. 73), a discourse failure would basically entail that the intelligence consumer is receiving a different “product” than what the producer thinks that it has sent. This again would have a direct impact on how the consumer acts in relation to the threat being communicated about, as they might over- or underestimate the “true” level of said threat, leading them to over- or underdimension their risk reduction measures.

There are two interrelated causes of discourse failure. The first is related to human cognition, or the way we humans understand the world around us (Hatlebrekke, 2019, p. 40). Hatlebrekke (2019, p. 58) points to two specific cognitive phenomena which can result in discourse failure; cognitive closure and the problem of induction. The problem of induction is “the belief that history repeats itself” (Hatlebrekke, 2019, p. 1), and results in threats that occur in new variations being “challenging or, at worst, impossible to foresee” (Hatlebrekke, 2019, p. 4). The problem of induction causes cognitive closure, which is the human tendency to avoid complex and uncertain answers and information (Hatlebrekke, 2019, p. 82). This all manifests itself in intelligence consumers lacking the willingness to accept new threats which don’t conform to their pre-existing beliefs.

The second cause of discourse failure is lacking information sharing or dialogue between intelligence producer and intelligence consumer. Since cognitive closure and the problem of induction are both almost ingrained ways in which humans approach the world, overcoming these things depends on information sharing and dialogue which “challenges preconceived assumptions” (Hatlebrekke, 2019, p. 221). In the words of Hatlebrekke (2019, p. 227):

> “The dialogue must be based on understanding and respect, and more importantly, the intelligence producer must understand the consumer’s needs, as well as the consumer having to understand the essence of intelligence. ‘Thus intelligence is at the mercy of users’ unpredictable attitudes towards it; but it tries to make its own luck with them through persuasion, personal relations and marketing.’ This illustrates that a consumer’s comprehension of the intelligence product depends on the quality of the dialogue between the producer and the consumer.”

Given that it's very difficult to observe examples of the issues related to human cognition, not least because this is not a psychology thesis, I will focus on identifying lack of dialogue when assessing potential for discourse failure.

It is worth noting that in the Neumann and Smith (2005) piece, discourse failure is discussed in the context of intelligence communication *within* the state. Given that I am studying intelligence communication between a state actor and a non-state actor, whether the original conceptualisation and understanding of discourse failure fits with the findings of this study needs to be discussed. This will be done in chapter 5.3.3, in which I, in light of the data I have constructed, discuss whether discourse failure is inevitable when communicating intelligence from a state actor to a non-state actor.

3.5.3 Relationship between different ways of understanding interpretation

Finally, I want to briefly explain the relationship between the discourse failure theory and the broader discussion about what impacts interpretation which is based on constructivist thought and sociological institutionalism. The reason why these are complementary is that while they speak to two different but related issues, they are built on the same view that "meanings are socially and discursively constructed" (Halperin and Heath, 2020, p. 365).

Constructivism and the sociological institutionalism theory are used to explain how different organisations, and the individuals within them, construct meaning and why they (don't) belong to the same discourse as other organisations and individuals. This is a useful foundation for trying to unpick why a lack of belonging to the same discourse leads to the private sector and the PST have different understandings of for example what type of information the PST is supposed to share.

On the other hand, discourse failure is a more apt foundation for understanding the part of intelligence sharing which relates to why individuals struggle to comprehend new threats and information which doesn't fit with their existing understanding of the threat landscape. The same underlying dynamics are at play for both, like the fact that both factors relating to how individuals interpret the world around them, and external factors related to the impact of dialogue and belonging to institutions, impact interpretation. As mentioned, the main observable cause of both differing understandings of reality and discourse failure is a lack of dialogue, hence why this is what I have focused on in the analysis.

3.6 Summary

In this chapter I have laid out the key studies, theories, and concepts upon which my study is based. Building on the context established in the previous chapter, this chapter has provided the foundation for the questions I pose in the interviews, as well as a framework for the discourse analysis. The chapter has also highlighted key studies in this field, and what is missing from the current body of academic research. Specifically, what I deem to be missing in the literature is studies on intelligence communication between security/intelligence services and the private sector, studies on decision making surrounding intelligence sharing, hereunder the sharing of confidence, and studies in countries outside of the US and Canada. By looking at intelligence communication between the PST and the private sector in Norway, I hope to contribute to filling this gap. In the next chapter, I will lay out my methodological approach, including how I have gone about constructing (interview) data, my logic of inference, the challenges I have faced, and why I have made the choices I have made.

Chapter 4: Methods

Broadly speaking, this thesis is a qualitative, small N, abductive study, meaning that it aims to draw inferences and make "probable conclusions" about a case or puzzle (Merriam-Webster, no date) from a process of going back and forth between pre-existing theory and in-depth analysis of a small number of observations (Schwartz-Shea and Yanow, 2012, p. 28). In this study, the observations are interviews with security professionals working at, or associated with the PST, the NSR, and major private sector companies. This makes the unit of observation individuals at these institutions/organisations, while the unit of analysis is the PST on one side, and the private sector on the other.

Given that the topic and chosen case are very much in the early phase of the research cycle, seeking descriptive and interpretive inferences is suitable. This is because these kinds of inferences help provide an understanding of a case, which is important when attempting to unearth new dynamics and theories (Gerring, 2012), a key objective of early-phase research (Lieberman, 2020). This is not to say that seeking causal inferences in *an* early-phase study is inappropriate or impossible, but rather that *my* chosen research question and the nature of *my* study lends itself better to interpretive and descriptive inferences. For example, making methodologically sound causal claims about this topic would likely mean having to collect/construct data from a significantly larger number of individuals in the PST, given the lack of pre-existing openly available information. Given the difficulties I have experienced getting access to just two people in the PST, such an effort would be far beyond the scope of a master´s thesis.

Lastly, this study is built on an interpretivist logic of inference. This implies understanding knowledge and reality as socially constructed, meaning that how people understand the world around them is subjective and shaped by prior experiences and beliefs (Schwartz-Shea and Yanow, 2012), as I explained in chapter 3.4. I have chosen to build my study on an interpretivist logic of inference because I am interested in studying how interviewees understand or interpret key topics of interest. This stands in contrast to a positivist approach, which would be more appropriate if I was seeking an "objectively true" account of, for example, precisely why the PST has chosen not to share information about confidence (Fujii, 2017, p. 2). As a result of not focusing on finding “objective” testable and replicable conclusions as is common in positivist studies (Schwartz-Shea and Yanow, 2012, p. 92), reflexivity will be key in order to demonstrate the reliability and quality of this study (Schwartz-Shea and Yanow, 2012, p. 99).

I begin this chapter by introducing two interrelated challenges faced when conducting this study, namely confirmation bias and issues related to double hermeneutic. Then, I lay out how I have conducted this study, including how I have gone about trying to insulate the analysis, and data construction from said issues. I also discuss key decisions relating to things like interviewee selection, data analysis and ethical considerations.

4.1 Confirmation bias and double hermeneutic

> “In launching Operation RYAN, Andropov broke the first rule of intelligence: never ask for confirmation of something you already believe. […] Yuri Andropov, pedantic and autocratic, was utterly convinced that his KGB minions would find evidence of a looming nuclear assault. So that is what they did” (Macintyre, 2019, pp. 145–146).

The above quote illustrates a key issue in the intelligence and security world, which is the realm within which this study is situated. Furthermore, it just so happens to also be a core issue in academic studies like this one, where it is often referred to as confirmation bias. Originally coined by Wason (1960), “confirmation bias is the tendency to seek out information that supports a position while ignoring or minimizing inconsistent information” (Cook and Smallman, 2008, p. 745).

In all phases of this study, avoiding both confirmation bias and basing one´s work on pre-conceived conclusions has been crucial. It is especially important given the subjective nature of both discourse analysis as a method of analysis and relational interviews where the goal is to get at an individual´s subjective interpretation or understanding of an issue. When dealing with interpretation of interpretation, or “double hermeneutic” (Giddens, 1982), reflexivity or “the process of engaging in self-reflection about who we are as researchers, how our subjectivities and biases guide and inform the research process, and how our worldview is shaped by the research we do and vice versa” (Jamieson, Govaart and Pownall, 2023, p. 1) is key. And while this might help at the very least locate the source of any misinterpretation and inaccurate conclusions, my study will inevitably be open to something akin to discourse failure; a situation where I as the researcher might end up interpreting something said by an interviewee in a different way than what they thought I would. The reasons for which I discussed in chapter 3.4 on what impacts interpretation.

Given that I am not aiming to test a particular theory in this study, and that the study is exploratory in its nature, it is perhaps not immediately clear in what instances I needed to be mindful of confirmation bias. However, examples of such situations include seeking out evidence of the different issues identified in the literature, like for instance discourse failure, (mis)interpreting answers in a way which makes them fit a pre-conceived narrative, and hearing something in one of the first interviews and then subsequently actively seeking to find evidence which supports that finding in later interviews. This could for example happen by embedding premises based on pre-conceived conclusions in my questions, and actively "fishing" for a certain answer by asking follow-up questions which guide the interviewee towards giving specific answers which support initial findings.

4.2 Data construction

In this sub-chapter I will explain how I have gone about constructing the data for this study, building primarily on literature on elite and expert interviews (Petintseva, Faria and Eski, 2020), relational interviewing (Fujii, 2017), and on interviewing people in security and intelligence services (Davies, 2001). Note that in line with the interpretivist foundation this study is built on, I write *construction* of data as opposed to *collection* of data. This is to further underline the assumption that data, in this case interview data, is shaped (or constructed) in a context and by the actors involved in the data *construction*, as opposed to just *collected* by a researcher without that person having an impact on the data. I will start by covering how I went about accessing and selecting interviewees, before moving on to how the interviews were conducted. All the while focusing on factors which impacted the construction of the data. It's important to specify that while I am using what my interviewees said to analyse the organisation they are a part of, the interviewees are speaking based on their individual understanding and interpretation, and not as official representatives of their organisation.

4.2.1 Access and interviewee selection

There were primarily two things which impacted my interview selection. Firstly, building on my prior knowledge of people and organisations in the Norwegian national security structure, and the Total Preparedness Commission´s assessment that the NSR and its owners represent the breadth of the private sector in a security context (The Total Preparedness Commission, 2023, p. 195), I developed a set of criteria for whom I wanted to interview. On the PST side, I wanted to interview someone who had knowledge of the debate about confidence sharing/external threat communication, and the PST´s relationship with the private sector. Given that state actors and the intelligence threat is most relevant for the private sector and therefore also the primary focus of this thesis, I wanted to talk to someone working on that topic.

On the private sector side, I wanted to talk to people who didn't have access to classified information on a regular basis as this could mean that they had access to information about confidence. Secondly, I wanted to talk to "best in class" security people (elites/experts) at major companies as those would be more likely to have informed opinions about the topic of study, in addition to them representing key actors in Norway's total defence. This decision has the potential to introduce some selection bias, which is something I will return to. To see if the answers I got from the people I interviewed in the private sector reflected a larger sentiment in the private sector, and in order to be better placed to assess the answers I got from the PST officials, I also decided to interview the NSR themselves. This is described in the literature as triangulation, or the act of using different sources and angles to access a claim or issue to ensure the quality of the findings (Natow, 2020).

The other main factor which impacted interviewee selection, and one of the most profound challenges I was faced with when conducting this study, was getting access to interviewees. Broadly speaking, access is a well-documented challenge in so-called elite and expert interviews (Petintseva, Faria and Eski, 2020, p. 3). However, attempting to interview security service officials in particular further exacerbated these challenges, as security and intelligence organisations are particularly difficult to access (Davies, 2001). I therefore made use of my contact network and focused on identifying key gatekeepers who could grant me access. On the private sector side, I reached out to the NSR and asked if they could forward my request to people who fit the selection criteria. On the PST side, I established contact with the communications department at the PST through someone I worked with during my internship at a private security consultancy company, who recently finished a long career at the PST.

Furthermore, when reaching out to both the PST and the private sector I was open about my connection to this person, and the fact that I am due to start working at the company where I completed my internship after finishing my degree. I did this to build up the trust, rapport, and the “insider status” of me and my project. Thereby making it more likely that they would say yes to an interview than if I had just been a “random master student”, something which is supported by the literature on interviewing elites and experts (Petintseva, Faria and Eski, 2020, p. 71). Furthermore, I also framed the project in a way which emphasised both the importance of the individual interviewee’s participation for the study, and what they would get out the study, while also making sure to not present the study as an attempt to expose critique worthy practices (especially at the PST). Here, it was important to strike a balance between presenting the project in a way which “encourage[s] participation while not concealing the underlying focus of the study” (Petintseva, Faria and Eski, 2020, p. 77).

The decisions I have made also have their downsides. Firstly, this kind of convenience sampling/snowballing based on some selection criteria, and driven largely by who I got access to, has the potential to introduce bias. This is especially the case if the PST and the NSR recommended that I interview people who would give me answers which conformed with their “agenda”. Secondly, as I will return to when presenting findings and my analysis, the regional location of the companies/individuals I interviewed, and the size of the companies might also have an impact on the responses they gave. Thirdly, the limited number of participants means that it´s hard for me to know to what extent what I have found is representative of the organisations I am analysing. However, I did experience that by the time I got to the third, fourth and fifth interviews with the private sector/the NSR, I kept hearing pretty much the same things. This indicates that I might have achieved saturation in this group. Furthermore, given that I don’t aim to be able to generalise my findings, achieving a large, representative sample is not as important if I am open about what kind of people I have talked to (see overview of interviewees in appendix).

The use of gatekeepers and my personal contact network raises some ethical concerns relating to privacy and anonymity of the interviewees. One of the concrete measures I implemented to compensate, or at least mitigate the potential issues relating to this, was to be open with potential interviewees about where I got their contact information so that they knew the extent to which I was able to ensure their anonymity. As the overview of interviewees in the appendix will show, I have chosen to anonymise interviewees by assigning them a codename based on which group they are a part of. That being said, I have provided some background information on the interviewees, like which sector the private sector interviewees belong to (for example energy or finance) and which part of the PST my interviewees are part of (for example communications or counterintelligence). Doing so gives the reader a better insight into which kinds of people I have interviewed, which is important when trying to evaluate the credibility of my analysis and conclusion.

The main goal of granting anonymity was to enable the interviewees to be honest and willing to share their (as times critical) individual interpretations, especially as it related to the relationship between the PST and the private sector.

4.2.2 Conducting interviews

In keeping with the interpretivist approach to this study, I conducted relational interviews. This meant focusing on trying to get at the interviewee's understanding and interpretation of the topic through a two-way dialogue, as opposed to asking them to give a more objective, factual account of events and discussions (Fujii, 2017). I did so by opting for semi-structured interviews, in which I came prepared with some broader questions and topics I wanted to cover. Then, during the interview I focused on asking follow-up questions. To minimise the risk of incorrectly interpreting what the interviewees said, I asked questions in the form of "do I understand you correctly if I say that…?". These kinds of questions were well suited to my chosen Socratic interviewer style (Petintseva, Faria and Eski, 2020, p. 32), which is signified by for example challenging assumptions and asking interviewees to consider consequences, implications, and other sides of an argument.

The interview guide developed over time for two reasons. Firstly, as a result of going back and forth between interviewing and looking at studies and theories, and secondly so that I could ask questions aimed at checking if subsequent interviewees understood issues in the same way as the initial ones. One issue with the latter of these two was finding a balance between this strategy and veering towards "leading the witness" by asking questions which were too leading, which could bias the answers given. Then again, given that the interviews were relational, the answers would never be completely objective since data in such interviews are constructed in an interaction between interviewee and interviewer, and not collected with the goal of achieving positivist-style objectivity.

That being said, ensuring that the interviewees had a shared understanding of key concepts was important for the validity of the findings. At the same time, I was also interested in uncovering examples of differing interpretations and understanding of key topics, like the relationship between the PST and the private sector. Hence, I for example asked interviewees early in the interview about how they understood the term "confidence", and then proceeded to provide a definition when they had explained how they understood it. Doing so allowed me to see if confidence was understood in roughly the same way by the interviewees, while also ensuring that the subsequent answers given in each interview was based on a shared understanding of confidence. This enhanced the validity of the findings and analysis. The definition of confidence I presented during the interviews was based on how confidence has been defined in this thesis.

My ability to ask follow-ups was helped by using the "University of Oslo Nettskjema Dictaphone app" to record the interviews, as this allowed me to focus on what was being said and taking some limited notes, as opposed to focusing on writing down everything which was said. Furthermore, I also used the built-in University of Oslo AI "Autotekst" transcription tool which is based on the "Whisper" program from Open AI to transcribe my interviews verbatim. However, as the programme is not 100% accurate, I did have to go through the transcription and make some manual edits.

To make the interviewees feel comfortable, I chose to conduct the interviews in their native language Norwegian. Furthermore, I steered away from questions which touched on classified information, and granted interviewees anonymity. I also told my interviewees that I would send them the quotes I wanted to include in the thesis so that they could approve or object to them, something I did in early May. My experience was that this led to interviews where the interviewees seemed open to providing clear, direct, and honest answers and reflections. Furthermore, the amount of jargon and acronyms which was used, and the amount of knowledge the interviewees seemed to assume on my part, leads me to conclude that they viewed me as an insider, which could have impacted their responses. For example, they skipped providing more "obvious" information and went straight to more advanced, in-depth reflections, something which gave me more time to engage with and probe their underlying assumptions and interpretation.

4.3 Data analysis

At their core, discourses are "systems of meaning-production that fix meaning, however temporarily, and enable actors to make sense of the world and to act within it" (Dunn and Neumann, 2016, p. 21). Discourse analysis can then be defined as a method which enables the researcher to analyse how meaning is produced and expressed through language. Or in other words, utilising discourse analysis enables the researcher to study an individual, group, or organisation´s understanding and construction of reality (Dunn and Neumann, 2016, p. 24). In my study, the goal of using discourse analysis is to see what my interview data can reveal about how the interviewees understand confidence, the debate around sharing it, and the broader relationship between the private sector and the PST. Thereby enabling me to assess challenges faced by the PST in their threat communication to the private sector. One key requirement for conducting this type of research is having an in-depth understanding of the context and field which one is studying (Dunn and Neumann, 2016). Therefore, in addition to my insider status and insider knowledge being useful for getting access to interviewees, it was also useful when analysing the interview data. It is, however, also something which could have impacted the way I analysed the data, as how I subjectively analysed the data was shaped by prior experiences and biases. For example, the fact that I am entering the field I am studying once I graduate might have made me more hesitant to present findings which are overly critical of the PST or other actors.

Being able to analyse organisations based on interviews with individuals at said organisations rests on the assumption that individuals are shaped by, and therefore also reflect key parts of, the institutions they are a part of. This is because, as previously mentioned, institutions shape the values, norms, behaviour and “the very terms through which meaning is assigned in social life” of the individuals which reside in them (Hall and Taylor, 1996, p. 948). However, given that individuals are shaped by multiple institutions and their own unique personal experiences, I also decided to look at some reports, newspaper articles, and studies in order to triangulate my findings, as is advisable when studying intelligence and security services (Davies, 2001). These sources primarily provided context surrounding the interview data, as opposed to being part of the data being analysed like the interview data was. Hence, I don’t explicitly discuss the selection strategy of said documents in the data construction chapter. That being said, what kinds of reports and documents I looked at could have impacted my findings, hence why this is something I discuss when conducting the analysis.

4.3.1 Practical application of discourse analysis

My approach to discourse analysis is based on the work on Dunn and Neumann (2016). I have chosen to focus on the first three parts of their proposed way of conducting a discourse analysis, namely identifying, inventorying, and mapping discourses. This means leaving out the part which Dunn and Neumann (2016, p. 121) refer to as layering, as this approach is primarily useful when looking at the development of discourse(s) over time, something which this thesis does not do. Simply put, identifying discourses means getting an overview of the different discourses relevant for one´s research, inventorying discourses means laying out the discourses one has identified in a way which shows how they are located next to/within each other, while mapping discourses entails looking more closely at the relationship between the discourses, for example how multiple discourses “compete” to be the dominant one in relation to a particular issue or domain (Dunn and Neumann, 2016, pp. 103–121).

In practice, this meant subjecting my interview data to a so-called close reading, where I carefully read the data, attempting to identify discourses which could help me answer my research question. For example, I would look for words and phrases used to describe the relationship between the PST and the private sector. Then, I used those findings as the foundation for interpreting how the interviewees understood the other party and their relationship, and how this impacts/is reflected in the debate about intelligence sharing. This was done in part by looking at how the different discourses related to each other through the process of inventorying, and subsequently mapping.

In order to contextualise the findings, I drew on reports (see for example, The Total Preparedness Commission, 2023) and other publicly available data like the PST´s own podcast (see for example, PST, no date) and previous academic studies discussed in the theoretical framework chapter. The goal here was to demonstrate how my findings fit with pre-existing knowledge and seeing if external context and information could aid in making probable conclusions about what I had found. For example, I would look at how the interviewees in the private sector´s interpretation of why the PST didn't share confidence fit with prior reports and studies which investigated these kinds of issues.

In line with the choice to build by study on abductive reasoning, throughout the process of conducting the analysis, I went back and forth between analysing the interview material and looking at studies and theories which would help me draw inferences and make probable conclusions. This abductive approach was also mirrored when coding the interview transcripts in NVivo. When coding, I started with some overarching codes based on my overarching research question, with a particular focus on the sub questions, and created new codes as I found interesting things in the data, all the while looking for data which could help answer my research question. The resulting codebook can be found in the appendix.

Chapter 5: Analysis

So far, I have laid out how I have gone about conducting this study, and the context, both empirical and academic, within which this study is situated. Building on that work, in this chapter I analyse my data in light of the three sub-questions posed at the beginning of the thesis. The analysis draws on data from the seven interviews I have conducted: Two with people at or associated with the NSR, three with people in the private sector (in the industry, energy, and finance sectors), and two at the PST (one working in the counterintelligence department and one in the communications department). In addition to this, the analysis draws on previously introduced context, concepts, theories, studies, and reports. Furthermore, I also draw on some additional reports which help provide further context and aid in analysing the answers given by the interviewees.

When referring to interview data during the analysis, I either refer to which group of interviewees presented a view (for example "the interviewees from the PST") or to specific individuals using their assigned codenames (for example Industry 1 or NSR 2). Furthermore, given that the interviews were conducted in Norwegian, when directly quoting interviewees, I provide their original quotes in Norwegian in the form of a footnote. In some instances, I also do this when paraphrasing answers given by the interviewees.

As I wrote in the methods chapter, I understand the term discourse to mean "systems of meaning-production that fix meaning, however temporarily, and enable actors to make sense of the world and to act within it" (Dunn and Neumann, 2016, p. 21). When using the term discourse within the confines of this chapter and in the conclusion, discourse refers to things said or written about a specific topic. For example, the term discourse is used to describe the collection of different views expressed by interviewees about whether confidence should be shared. Related to this, the term narrative is used to describe a more uniform group of statements, a specific idea, or interpretation (for example the misunderstanding narrative) found within a discourse. Both narratives and discourses are therefore collections of data about a topic which I analyse to unpack my interviewees understanding of reality.

The analysis presented to the first two sub-chapters in this chapter forms the basis for the third sub-chapter in which I discuss the potential for discourse failure. An answer to my main research question follows in the conclusion chapter and builds on the analysis presented in this chapter.

5.1 Confidence and the sharing debate

In this sub-chapter, I tackle the first of three sub-questions, namely "*How is confidence and the consequences of sharing it understood?*". To do so, I focus on three main things, which are reflected in the three sub-headings in this sub-chapter. Firstly, I look at how the interviewees understand confidence and uncertainty in intelligence. This includes looking at both how interviewees understand confidence itself from a more definitional perspective, and how they understand confidence as it relates to the PST´s assessments specifically. Then, I present the dominant narrative in the debate surrounding sharing of confidence, which I have named "the misunderstanding narrative". Finally, I look at other arguments and views on the sharing debate. Throughout, this sub-chapter sheds light on the main research question by virtue of answering the first sub-question. It also presents key analytical findings which are picked up on and developed further in the two subsequent sub-chapters in this analysis chapter.

5.1.1 Confidence and uncertainty in intelligence

When asked to define confidence, the interviewees were able to provide a definition of confidence as something to the effect of confidence being an assessment of a probability assessment, which says something about how much uncertainty said probability assessment is imbued with. While the interviewees gave answers to the question about what they thought confidence was, every interviewee apart from Industry 1 seemed to display some hesitancy towards providing said definition. To me, this indicated that confidence as a concept is not something which is well established and understood. This was something which several of the interviewees confirmed when I later directly asked them about this. For example, PST 2 said "to exaggerate a little, how is the PST supposed to be able to convey something they don't really have a 100% understanding of themselves?".[1] It's important to

[1] «Det tror jeg er litt satt på spissen da. Hvordan skal PST klare å formidle noe de egentlig ikke har 100% forståelse for selv? Sikkert noen analytikere som blir irriterte nå, men nå tenker jeg på hele organisasjonen.»

note here that PST 2 clarified that they didn’t necessarily refer to the analysts at the PST, who PST 2 said might get annoyed by this quote, but to the organization writ large.

On the private sector side, Energy 1 referred to confidence as a theoretical component which was a bit too complicated to deal with on a day-to-day basis.[2] While Industry 1 and Finance 1 said that they dealt with confidence more regularly, all interviewees were very clear about the fact that they didn’t use the term confidence when talking to people who were not part of the so-called “professional security environment” (a group of “best in class” security people, often working at major companies or at consultancy companies). The reason for this was, in their view, that the use of confidence was likely to confuse the intelligence consumer. This view was backed up by claims that people outside of the professional security environment already struggle to understand the probability words. It also folds into the misunderstanding narrative I will return to in chapter 5.1.2.

Barring one quantitative study by Halvorsen (2020), which found that the officials surveyed had a low, or a very low degree of shared understanding of the probability words, no studies on how security professionals and the broad public in Norway (mis)understand probability and confidence words have been conducted. That being said, as I discussed at length in the theoretical framework chapter, studies like one by Irwin and Mandel (2023, p. 943) have found that security professionals and the broader public alike tended to provide vastly different understandings of confidence and probability.

While I found evidence of some hesitancy and insecurity among the interviewees when I asked them about confidence as a concept, the most interesting finding about how confidence is understood relates to the PST´s external threat communication. I found that there was no collective understanding in the private sector of what level of confidence is embedded in the information shared by the PST. While some, like NSR 1, said that they thought the information had high confidence, others like Industry 1 said that they thought it had medium confidence. The interviewees in the private sector/the NSR also gave different answers when I asked if they thought parts of the NTV had higher confidence than others

[2] «Jeg tror det er en sånn teoretisk komponent som er akkurat for stor til å ta med seg inn i hverdagen.»

(for example the assessments about intelligence activities vs those about terrorism). Some said it was pretty much universal across threat categories, some said that the intelligence activity assessments had higher confidence, while others thought that the terrorism assessments had higher confidence. These answers lend further support to the claim that the private sector doesn’t have a shared understanding of confidence as it relates to the PST´s threat communication.

The discourse in the private sector about confidence in the PST´s assessments highlight an obvious puzzle: why did I get so many different answers to these two questions? One explanation is that different private sector actors and the NSR all have different perceptions of how certain the PST is about their assessments. This is supported by the fact that the interviewees gave quite detailed explanations for the answers given, which clearly showed differing understandings of how (un)certain the PST´s assessments are. This is a key finding for the purposes of answering my research question as if there is no universal understanding of how much confidence the PST´s assessments are imbued with, that speaks to a lack of shared understanding of reality within the private sector, and between the PST and the private sector.

That being said, given that the terms confidence and probability tend to be interpreted vastly differently by different actors (for list of studies proving this, see Duke, 2023, p. 2), one cannot rule out that this could have led to interviewees having a similar understanding of the PST´s information, while also using different words to describe how much confidence a given assessment has. For example, when describing the level of confidence, did an interviewee say that the PST´s assessments have medium and not high confidence because predicting the future is inherently uncertain, which in their mind makes it impossible to have high confidence? Or did they do so because they didn’t think that the PST had good enough intelligence to be able to make predictions which have high confidence? The way the interviewees elaborated about their assessments of how high or low confidence the PST has indicates that it’s probably a bit of both.

5.1.2 The misunderstanding narrative

Both the discussion about confidence in the PST´s threat communication, and the preceding analysis of how confidence is understood more broadly is intrinsically linked to the dominant narrative in the discourse about whether or not the PST should share information about confidence in their external threat communication. While there are other arguments and narratives in the discourse about the PST´s threat communication, which I will return to in chapter 5.1.3, "the misunderstanding narrative" was the dominant narrative in the discourse.

During the interviews, my experience was that the misunderstanding narrative was presented as a so-called "natural fact". By this, I mean to say that the view that sharing confidence would cause misunderstanding and confusion was presented as a definitive fact and "not called into question" (Dunn and Neumann, 2016, p. 111) by any interviewees. All the interviewees therefore said that they didn't think that confidence should be shared in public threat communication, like in the NTV. Note here that I write *public* threat communication specifically. This is because there also seemed to be broad agreement that confidence could, and perhaps should, be shared with the professional security environment. Which, according to NSR 1, is probably able to deal with and understand more information than it is currently given. In NSR 1´s opinion, this could even include information which is "exempt from public disclosure", if sharing is done within soon to be established closed arenas for information sharing, as opposed to in the NTV.[3]

As a result of its dominant position in the discourse surrounding the debate about sharing confidence, the misunderstanding narrative works to legitimise and support the PST´s current policy by presenting the sharing of information as contradictory to the interests of the rest of society. The fact that the private sector doesn't think that information about confidence should be shared in the NTV, despite thinking that they themselves could make use of that information, suggests that the private sector views the NTV as a product which is

[3] «De klarer det, og så kommer «kickeren»: De hadde sannsynligvis klart å forholde seg til mye mer, fordi dette er det profesjonelle sikkerhetsmiljøet. Min påstand er at du faktisk kunne delt og ting som hadde vært unntatt offentlighet til den gjengen. Altså at du kunne gått enda lengre til det profesjonelle sikkerhetsmiljøet, fordi at du kunne laget arenaer for informasjonsutveksling.»

primarily designed to communicate threats to the broad public, and not to the professional security environment in the private sector.

The combination of the misunderstanding narrative, and the lack of a shared understanding in the private sector of how much uncertainty the PST´s information is imbued with (as shown in chapter 5.1.1), raise questions about the use of the narrative to justify the current policy towards sharing confidence. If the reason for not sharing is that sharing will cause misunderstandings and confusion, and there is already confusion and misunderstandings, why is the misunderstanding narrative being used by the PST to justify the policy? One explanation could be that the PST thinks that the private sector has the same understanding of how much confidence the PST´s information has as they do, making sharing unnecessary for this group. However, while PST 2 thought that the private sector generally assumed that the PST´s information had high confidence,[4] PST 1 thought that the private sector had a vast variety of different understandings of the level of confidence (which is what I found in chapter 5.1.1).[5]

So, either PST 1 is not in line with the understanding of reality at the PST, or there is no broad understanding of this issue at the PST, and there are other arguments in the discourse which are impacting the PST´s policy. It is also possible that the PST is aware of the misunderstanding, which is seemingly present in the professional security environment, but that they are electing not to share confidence which could clear up this confusion, as the NTV is also read by the broader public - a group which is less likely to understand and make use of said confidence information.

Another explanation is that the PST is concerned about how sharing confidence could contribute to *increased* confusion in the interpretation of probability words, especially among the broader public, as opposed to them being concerned that sharing of confidence could contributing to *causing* confusion. This explanation is supported by PST 1 saying that

[4] «Jeg tenker at overordnet så håper jeg og tror at de tror at det er ganske sikkert.»
[5] «Jeg tipper at du får veldig mange forskjellige svar. Noen sier nok at vi fremstår sikre, andre sier sikkert at vi fremstår uryddige, eller at det er diffus kommunikasjon. At det er vanskelig å skjønne hva vi mener.»

using confidence in threat communication would just be *even more* confusing.[6] Furthermore, this reasoning for not sharing confidence also tracks with the study by Irwin and Mandel (2023, p. 952), which showed how sharing confidence together with probability words has a significant impact on interpretation of the probability assessment. Specifically, that study showed that sharing confidence could lead people to say that the term likely indicated a lower probability of something occurring than the term unlikely.

Having laid out the misunderstanding narrative and some possible explanations for why it might impact the decision to not share confidence, I will now move onto the next part of this sub-chapter in which I will look at other arguments within the "to share or not to share" discourse.

5.1.3 To share or not to share?

The final thing I want to do in this sub-chapter is to highlight three alternative narratives in the discourse on sharing of confidence. In addition to the misunderstanding narrative, these three narratives help paint a picture of how the consequences of sharing confidence is understood by my interviewees. The three narratives I look at are (1) how sharing impacts the credibility and status of the PST and their public threat communication, (2) the previously discussed sharing dilemma (or the balance between openness and exposing sources and methods), and finally (3) how sharing confidence could impact which measures the private sector chooses to implement to mitigate the threats described by the PST. In doing so, I also map these narratives to show how they relate to each other and how they work to construct and convey the interviewees understanding of reality.

In general, these three narratives are complimentary to the misunderstanding narrative as they don't seem to challenge the way reality it is portrayed in the misunderstanding narrative, nor its dominant position. That being said, some variants of the three narratives do challenge the decision to not share confidence. They do so by highlighting other consequences of sharing, apart from those tied to misunderstanding. Simultaneously, some present consequences which work to further legitimise the PST´s decision. I now provide

[6] «Tror som sagt, det å dra inn konfidens tror jeg bare vil være enda mer forvirrende, så da tenker jeg heller at man bør tilstrebe å være så tydelig og konkret som mulig, da»

concrete examples of how these narratives interact, what they “look” like, and their role in the discourse.

Credibility/status of the PST and their assessments

One thing I asked about, and which was brought up independently by the interviewees, was how sharing confidence would impact the credibility and status of the PST and their assessments. And by extension if such potential impacts could influence the decision to share. As opposed to the understanding of the misunderstanding narrative, which was close to universal across all the interviewees, the discourse surrounding how sharing confidence would impact the credibility/status of the PST saw the interviewees at the PST and in the private sector present quite different understandings of reality. When asked about what they thought the impact of sharing would be on the PST´s status and credibility, PST 1[7] and PST 2[8] both said that they thought that it would make the PST seem more honest and credible. This is a view which is supported by a previously discussed study which showed that people tend to assign more credibility to assessments which are transparent about confidence (Dieckmann, Mauro and Slovic, 2010).

However, while PST 1 and PST 2´s view is in line with this study, it is notably not in line with what the private sector thought would happen to the PST´s status and credibility if confidence was shared. All the five non-PST interviewees gave variations of the same answer when talking about how sharing confidence would impact the PST´s status and credibility. Simply put, they said that sharing confidence would make the PST seem less certain of their assessments and expose them to criticism to the tone of “how can you be so uncertain when you have all these resources?”. Several of these interviewees also said that they thought one of the reasons for the PST not wanting to share information about confidence was that the PST was afraid of seeming to not be in control, which would “not be a good look for a security service”.[9]

[7] «Man hadde jo på en måte fremstått kanskje mer ærlig, da.»

[8] «Det [troverdigheten] tror jeg hadde blitt bedre. Åpenbart ja, man må være flink til å si at dette ikke er en fasit på hva som kommer til å skje i 2024, men trendene er nok der. Men det mener jeg helt klart.»

[9] «Det er ikke bra at sikkerhetsmyndigheten fremstår som for usikker»

Given that the private sector generally didn’t think that the PST had very high confidence in their assessments, it makes sense that they would think that sharing information about confidence which showed that the PST had low confidence would make the PST seem less certain. Or in other words, it seems as though the private sector thinks that the PST is less in control than what the PST is perceived to be by the public, and that the PST is afraid of “exposing” this lack of control. On the other hand, as the PST indicated that their assessments in the NTV have a high level of confidence, it follows logically that they would not be as concerned about such negative consequences. On the contrary, the PST saw sharing as having a positive impact on their reputation and how transparent people think the PST is.

While the literature on intelligence sharing pointed to “avoiding blame and getting credit” as key factors which impact policy on sharing (Dieckmann, Mauro and Slovic, 2010; Hood, 2011), none of my interviewees said that they thought that sharing confidence would have much, if any, impact on the amount of blame assigned in the wake of something like a terrorist attack. I did not get any answers which has been able to help me shed light on why people thought this, hence why I am not able to explain why my findings deviate from existing literature on this question.

Sharing dilemma

Another omnipresent narrative in the discourse on sharing confidence was the sharing dilemma, which I have discussed in both the context chapter and the theoretical framework chapter. On the private sector side, all the interviewees explicitly stated, regardless of their broader opinion on the PST´s policies on intelligence sharing, that there must always be a balance between sharing information, and protecting sources and methods of intelligence collection. While several interviewees said that the PST could share more information than they currently do, while still not exposing too much of their sources and methods, the sharing dilemma was presented as an absolute fact and as a key argument in the discourse surrounding sharing of confidence.

On the PST´s side, and especially when talking to PST 2, the sharing dilemma was presented as the key determinant of intelligence sharing policy. Protecting sources, especially when information comes from other countries´ intelligence services, is key for the PST as "being known in security service´s circles as having wide open doors to the public will be negative in the long run".[10] The reason for this is, according to PST 2, that if one is known to share "too much", other nations´ security services, as well as other non-state actors in Norway, will be less willing to share information with the PST, fearing that the PST will end up exposing them, their sources, and their methods. Therefore, if the "owner" of a piece of intelligence says that they don't want the PST to share it, the PST will not share that information.[11]

The sharing dilemma narrative works to legitimise and support the current PST policy of not sharing confidence by providing a reason for not sharing which is viewed as legitimate in the discourse. However, NSR 1 did point out that this argument is mainly valid if there is a lack of a non-classified but still confidential way in which the PST can share information with the private sector. Having such systems would make it possible to share some more information with a select group of people without exposing the PST´s sources and methods to threat actors such as Russia. Establishing such systems would not completely undercut the sharing dilemma as an argument in favour of not sharing, as some things would still need to be kept strictly classified within the confines of the PST and the EOS-services. However, the eyes of NSR 1, it would in reduce the argument´s validity when discussing the potential for sharing confidence information with the private sector.

Impact on measures

The final part of the discourse about sharing of confidence I want to highlight surrounds what impact sharing would have on which measures the private sector chooses to implement to mitigate the threats described by the PST. While the arguments and discourse about sharing´s impact on measures don't directly challenge the misunderstanding narrative´s core claim that sharing would cause confusion in the broader public, the arguments about impact on measures does to a certain extent challenge the current PST

[10] «Jeg tror jo at hvis vi deler ukontrollert for mye, det tror jeg på sikt vil være negativt for oss som sikkerhetstjeneste. For Norge kan i det internasjonale samarbeidet ikke være kjent for å ha vid åpne dører for offentligheten.»

[11] «Hvis de som eier informasjonen ikke ønsker at vi skal gå videre med det, så gjør vi ikke det.»

policy. They do so by highlighting how not sharing has a potentially detrimental impact on the private sector´s ability to put in place measures which deal with threats. Conversely, sharing has the potential to result in a better knowledge foundation for decision-making in the private sector.

Specifically, PST 2 said that they thought that if the PST shared information about confidence, and the confidence was high, private sector actors would probably not dare to ignore that threat assessment when considering which measures to implement.[12] This was based on the idea that when confidence is not shared, a private sector decision maker could choose to ignore the threat assessment on the grounds that said assessment was so uncertain that the threat described might never materialise. However, this argument is a bit of a double-edge sword, because if confidence was shared and the confidence was low, a decision maker might use that to justify not implementing measures. This analysis is not hypothetical or just speculation, as Energy 1 said that they would be more likely to implement measures if an assessment had high confidence than if it had low confidence.[13] It is also supported by Dieckmann, Mauro and Slovic (2010, p. 988), who write that decision-makers are more hesitant to act on information which is perceived as imprecise or uncertain.

The private sector interviewees also presented two arguments which show how sharing confidence might be beneficial. Firstly, Industry 1 pointed to the issue of circular intelligence. Or:

> “information that is reported as an unconfirmed fact or assessment that is subsequently repeated in another agency or analyst’s assessment as a true report. The first agency or analyst sees it in someone else’s report and seizes on it as independent proof that his or her own information has been confirmed by another source” (Vickers, 2001, p. 8).

[12] «ja, hvis det hadde blitt sikrere, så hadde de vel ikke turt å ta sjansen på å ikke iverksette tiltak.»

[13] «Nei, jeg tror hvis de hadde sagt at det er lav konfidens knyttet til Kina som er en etterretningsaktør med onde hensikter overfor energisektoren i Norge, og de har lav konfidens til det, så er det klart at da må man kanskje vurdere hvor vanskelig skal vi gjøre det for selskapet å gjøre handel med Kina, kjøpe produkter fra Kina, er verdikjedene så sårbare som vi har trodd?»

This is particularly an issue when confidence is not shared, as an analyst could see a piece of information (for example in the NTV) and (incorrectly) assume that it has high confidence. The analyst would then base their own assessment on that piece of information, and perhaps even discuss the threat in question with analysts at other companies who have also made the same assessment based on the same piece of information. Hence, what was initially one piece of information with low confidence suddenly becomes an assessment with high confidence as it is apparently "confirmed" by other sources. This is already a problem in the private sector, hence why Industry 1 said that they and their colleagues in other companies use confidence and discuss which sources they have built their assessments on when discussing threats to avoid issues related to circular intelligence.

The second issue highlighted by the private sector interviewees is related to the first one and has to do with why the PST assign the probability value they do to a threat. When assessing whether or not to prioritise spending money and time protecting against a threat, it is, according to NSR 2, important to know if the probability of a threat occurring is said to be "low" due to there not being any information which indicates a pending threat, or if there is a lot of good information which shows that the actor in question is unlikely to pose a threat.[14] In the former case, it might be the case that the threat is not going to materialise, but it might also be the case that the security service has not found indications of a pending threat. In the latter case, the security service "knows" that the threat is unlikely to materialise as they have a good overview of the relevant actors and so on. If confidence was shared, one could take that into account during the decision-making process. Something which might lead one to implement some precautionary measures in the former case, but not in the latter, despite the probability of the threat being "low".

5.2 The PST, the Private Sector, and their relationship

In this sub-chapter, I tackle the second of three sub-questions, namely "*How do the PST and the private sector view each other and their relationship?*". To answer this question, I draw on both my interview data and some additional reports, newspaper articles, and the like.

[14] «Hvis PST sier trusselnivået er lavt, så er det en veldig stor forskjell på hvorvidt de mener det er lavt på grunn av at de har masse informasjon, full kontroll på alle trussel aktørene som sitter der, eller om det er bare fordi de har ikke noen informasjon som skal tilsi…»

The goal of using these additional sources is to contextualize and enhance the credibility of my findings through the process of triangulation. Throughout this sub-chapter, I highlight how the data I have used has the potential to introduce bias. This is particularly important in this sub-chapter, as the data I have constructed indicates that views on the relationship between the PST and the private sector is influenced by factors such as where in the country a company is based, which sector on is a part of, and how reliant one is on information from the PST.

While my interviewees described the PST as professional, independent, knowledgeable, and trustworthy, a reoccurring theme across my interviews and the additional sources I have looked at is that there is room for improvement in the relationship between the PST and the private sector. That being said, while the data clearly shows that the idea of unrealised potential is dominant in the discourse, it just as clearly shows that people have vastly different understandings of how major the issues are, and where the issues are "located". Or more specifically, why the relationship between the PST and the private sector doesn't work as well as it perhaps should do. I will highlight three categories of the issues in the relationship which were expressed during the interviews. Firstly, I look at whether the interviewees thought that it is ability or willingness which causes the PST´s (lack of) external threat communication. Secondly, I look at a narrative which provides a holistic explanation or reason for why the PST acts the way it does. Thirdly, I discuss different perceptions of who has agency, or the capacity/power to act (Brown, McLean and McMillan, 2018, p. 7), to improve the relationship.

5.2.1 Ability and/or willingness to share

The Total Preparedness Commission (2023, p. 117) writes that the willingness and ability to share information in the EOS-services, hereunder in the PST, is lacking. When I asked my interviewees about what they thought of this assessment, I found that the PST, the NSR, and the private sector all have different interpretations of whether its willingness, ability, or a mix of the two which is "lacking" at the PST. I will now highlight the different understandings of this issue and what the competing narratives can tell us about how the PST is viewed. I will also look at what this can tell us about the relationship between the PST and the private sector.

Broadly speaking, the interviewees in the private sector, as well as NSR 2, all thought that the Total Preparedness Commission´s assessment was correct in that there is a lack of willingness and ability to share information. Furthermore, there was also broad agreement that things have improved over the years. Especially if one compares the last few years, where the PST has been more present in the media and published more substantial NTV reports, to the situation five or ten years ago when the PST was far more closed off from the public. Where these interviewees differ in their understanding of reality is when it comes to whether it´s ability and/or willingness which is lacking. Industry 1 and Energy 1 both said that quite firmly that they believed that the main issue was a lack of willingness, which they viewed as a result of the culture at the PST. Industry 1 even went as far as to say that the willingness to share information with the private sector at the PST was not only lacking, but absent.[15] NSR 2 echoed the view that willingness was the primary driver, whilst Finance 1 said that it was a mix of the two. Finance 1 did, however, go on to expand on their answer in a way which leads me to conclude that they thought that willingness was somewhat more of a driver than ability.

How the culture at the PST impacts sharing is something I will pick up on in chapter 5.2.2. However, I will note now that in Hatlebrekke´s assessment of why the different parts of the US intelligence community failed to share information prior to 9/11, he points to "serious problems related to information sharing because there existed a deep-rooted cultural resistance to it" (Hatlebrekke, 2019, p. 122). Hence, if culture is a driver of lack of willingness to share, that would mirror issues found in the US.

Returning to the issue of willingness vs ability, NSR 1 is somewhat of an outlier on the private sector side as they were less critical of the PST, while also saying that the practicalities of sharing information, or the ability to share, was the main issue. They further emphasised this by saying that "one must not underestimate the practicalities of sharing

[15] «Jeg er fullstendig enig. Tjenestene, men da er jo spesifisert til PST, og ikke nødvendigvis de andre. Mangelfull, ville adda kanskje et ord og for å gjøre det mer, og fraværende.»

information”[16], and that “willingness to share is a result of the ability to share”[17] and not the other way around as the other interviewees thought.

Based on my data, it seems as though one of reasons for this difference of understanding of reality between NSR 1 and the rest of the private sector interviewees is the amount of contact the interviewees have with the PST. NSR 1 said that they are in regular contact with the PST, whilst the other interviewees all said that they feel as though the distance between them, and the PST, is very large. In the words of Energy 1, having regular contact with the PST is only possible if you “know someone in Nydalen” (which is where the PST´s headquarters are located).[18] This does not mean that NSR 1´s understanding of reality is incompatible with, or contradictory to, the other interviewees understanding of reality. In fact, given that several reports in recent years have pointed to issues related to the PST not being good enough at sharing information (see for example, The Traavik Committee, 2012, pp. 38–39; The Extremism Commission, 2024, p. 270), it is likely that the difference of interpretation is a direct result of NSR 1 getting more information and being in close contact with the PST than the private sector at large. I will not make any determination about whether its willingness or ability which is dictating the PST´s (lack of) intelligence sharing. However, I will note that the person who is in closest contact with the PST, namely NSR 1, who should have the best window into the PST´s thinking, thinks that it´s ability which is the most impactful impediment to intelligence sharing.

While on the topic of how different people/groups interpret the PST and their information sharing, it’s worth noting that the way the interviewees in the private sector understand reality is influenced by them all being in the Oslo area. According to NSR 1, “there is no doubt that it is easier to contact a regional office of the PST” than it is to contact the headquarters in Oslo.[19] Given that the PST no longer has a regional office in the Oslo area, the people I have interviewed are likely to have less contact with the PST than individuals and companies in other parts of the country. Both PST 1 and PST 2 recognised that the

[16] «Man må ikke undervurdere den praktiske delen av å dele informasjon»
[17] «Jeg vil si at evnen er mangelfull. Og viljen følger av …»
[18] «Og næringslivet har et kontaktpunkt de faktisk kan ringe til, som ikke er avhengig av at du kjenner en som jobber i Nydalen.»
[19] «Det er ingen tvil om at det er lettere å kontakte et regionkontor»

companies in the Oslo area may feel as though the distance between them and the PST is larger than in other parts of the country in which there are regional PST offices. This is especially the case as those offices are the backbone of the PST´s interaction with the private sector according to my interviewees at the PST.

Finally, I want to cover what the PST themselves thought about the willingness vs ability discussion. Both PST 1 and PST 2 highlighted issues related to the practicalities of sharing classified information and the resources they have at their disposal as things which limit their ability to communicate to the private sector. Specifically, PST 1 talked about the need to prioritise who they talk to in the private sector given the limited amount of time they and their colleagues have at their disposal. They also said that this might lead some actors who do not get prioritised to develop a negative outlook on the PST. Furthermore, PST 2 talked about how the PST is a small security service compared to other nations´ security services.[20]

While what these interviewees said clearly point to ability as the main factor impacting sharing of information, it is worth noting that the PST would probably be unlikely to admit to having a lack of willingness to share information as that would be a bad look for the organisation. That being said, PST 1 was clear about the fact that the PST is by no means perfect in the way they communicate to the private sector. However, PST 1 also seemed surprised at both the assessment from the Total Preparedness Commission (2023) and by the fact that the private sector agreed with said assessment.[21] To me, this indicates a lack of dialogue between the PST and the private sector, which results in the two having different understandings of reality. This is something which I will pick up on when discussing the potential for discourse failure. Finally, it’s worth noting that the finding that NSR 1 is the person closest to having the same understanding of reality as the PST, supports the claim that increased dialogue is key to ensuring a more shared understanding of reality, given that NSR 1 is the person in closest dialogue with the PST.

[20] «Men det er klart at i internasjonale sammenhenger så er jo PST en forholdsvis liten tjeneste.»

[21] «Ja, det er litt overraskende, jeg hadde jo trodd at vi var mer tilgjengelige. Men det var min persepsjon da.»

5.2.2 ***Police*** security service

During my interview with NSR 2, the interviewee said the following while talking about the willingness vs ability question:

> "Let me tell you what one of the issues are: it is that it's the ***police*** security service, and not just the ***national*** security service".[22]

When I asked what NSR 2 meant by this they said that the issue is that the PST is a police organization, as opposed to a civilian organisation like MI5 (Military Intelligence section 5) in the UK, and other similar domestic national security/intelligence services in other countries. Furthermore, NSR 2 went on to say that "they [the PST] suffer a bit from having a police culture, as opposed to having a national security service culture".[23]

I will now highlight some of the things having a police culture entail, according to NSR 2. Then, I show how some of the things raised by other interviewees fit into this narrative, even though the other interviewees didn't tie these things to this narrative as explicitly as NSR 2 did. It's worth reiterating that what I am presenting here is not my personal view of the PST, but rather what my interviewees think about the PST and what the discourse can tell us. It is also worth noting that the findings relating to the ***police*** security service narrative might not be transferable to other countries. The reason for this is that according to NSR 2, Norway is one of few countries, in addition to some of its Nordic neighbours, in which the domestic security/intelligence service is a police organisation. The transferability of these findings to countries with civilian security/intelligence services is therefore likely to be limited.

NSR 2 points to two main consequences or implications of the PST having a police culture. Firstly, they point to how the PST´s main priority is traditional police matters such as apprehending and prosecuting terrorists, intelligence officers, and the like. This results in a "closed off, internal and different type of competence" than what one finds on civilian security services like MI5.[24] The fact that the PST prioritises traditional police matters over

[22] «Jeg skal si deg hva som er et av problemene, det er at det er politiets sikkerhetstjeneste, og ikke bare nasjonalsikkerhetstjeneste.»
[23] «De lider litt under av å ha en politikultur, i stedet for en nasjonal sikkerhetstjenestekultur»
[24] «Ja, det er en politikultur som er der, som går på mye mer, etterforskning og påtale og hele den politi-biten. Og det er noe som medfører også et mer sånn lukka, indre, og annen type kompetanse.»

contact and engagement with the private sector was confirmed in a newspaper article in which the Head of the PST is quoted saying that uncovering radicalisation, terror plans, and intelligence activity is the part of the PST´s work which has the highest priority, and not contact with external actors (Kibar, 2024). I am not aware of any studies which compare the PST with an organisation like MI5. However, the Traavik Committee (2012) and other more recent public reports assessing the PST (see for example, The Extremism Commission, 2024), point to the organisation being too closed off and not engaging enough with other actors.

Secondly, NSR 2 points to how the PST, as a result of having a police culture, is old-fashioned and not very willing to embrace new methods and external knowledge. This is again supported by the Traavik Committee (2012, p. 3, own translation), which NSR 2 referred to during the interview, which writes that:

> "The PST is still characterised by a static organisational culture bound by traditions which does not adequately emphasise and appreciate development, creativity, and new ways of thinking. According to the committee, this is at present perhaps the PST´s largest challenge."

It is very much possible that this has changed since this report was written in 2012, as my interviewees say that they have seen improvements in the PST´s external threat communication in the last couple of years. However, even if some improvement has occurred since 2012, it is still the case that several of my interviewees, including NSR 2, Industry 1, and Energy 1, expressed views of the PST which mirror those of the Traavik Committee (2012).

The view that the PST is old-fashioned and not very willing to embrace new methods and external knowledge also fits with something said by Energy 1. According to Energy 1, the police in general, and to some extent also the PST, suffer from a culture where it's "the boots on the ground" who know best, and that their knowledge is viewed as better than that of external research.[25] This finding mirrors Mandel´s (2022, p. 79) previously introduced

[25] «Uansett om man får forskningsrapporter som sier det ene eller andre, så er det liksom gutter med støvler på som vet best. De har sett verden som ingen andre har sett den. Jeg tror jo at PST er en mer lærende organisasjon enn politi forøvrig. Men jeg tror de lider under [det] samme.»

ignorance hypothesis which states that there is a “widespread ignorance of scientific principles and values, within both intelligence and policy communities”.

5.2.3 Who has agency?

The final thing I want to do in this sub-chapter is to discuss how the actors view the question of who has agency to improve their relationship. In the broader context of answering the question of how the PST and the private sector view each other and their relationship, the discourse surrounding this question is a key datapoint which further underpins the finding that there is a major disconnect between how the PST and the private sector view each other, and their relationship.

On the private sector side, the clear impression is that the interviewees think that it´s mainly the PST which has agency when it comes to improving the relationship. When discussing what they view as a lack of engagement and dialogue, Industry 1 in particular gave the impression that the PST is the only one which has agency to change the relationship. At times, Industry 1 seemed to express a sense of resignation and even frustration when talking about attempts to reach out to the PST with proposals to improve their relationship. To exemplify why they felt as though the private sector lacks agency, Industry 1 highlighted a newspaper article in which a senior PST official was interviewed about threat of foreign intelligence collection. In the piece, the PST official says the following about academia and Norwegian companies working on technology development:

> “Someone gets it and are professional in the way they work with their own research. Others are completely gullible and very, very naive” (Kibar and Engen, 2020, own translation).

When Industry 1 referred to this piece, they described it as a “long, detailed piece about the Norwegian private sector´s uselessness and naivety”.[26] Furthermore, they went on to say that when they and their colleagues at other major Norwegian companies saw this piece, they didn’t share the PST official´s portrayal of reality at all. Industry 1 went on to say that considering the private sector´s “repeated unsuccessful attempts to improve two-way

[26] «Det var en sånn lang, utførlig artikkel om norsk næringsliv sin udugelighet, egentlig, og naivitet»

dialogue and cooperation between the PST and the private sector",[27] this article "created a larger distance in any future form of dialogue", and that it was an expression of "a form of arrogance", even though this was "perhaps not the original intent". [28] Considering this, it's not surprising that the impression I was left with was that the individuals in the private sector in general don't think that they have agency when it comes to improving the relationship.

On their side, the PST interviewees did not dismiss the idea that there are parts of the relationship which they have agency to improve. For example, PST 2 said that the cooperation could be better, and that the most concrete thing they could do was to provide briefings to the private sector which are not classified, but still secret.[29] That being said, the general takeaway from the interviews with PST 1 and PST 2 was that they placed agency more firmly in the hands of the private sector. For example, PST 1 said that if there is a company which sits wanting to talk to the PST, they have to reach out themselves because the PST is not always capable of initialising contact.[30] As mentioned at the start of this section on who has agency, this dissonance between how the PST and the private sector understands who has agency reflects a broader disconnect between how the PST and the private sector understand the reality of their relationship.

5.3 Potential for discourse failure

Rounding off this analysis chapter, I want to answer the final of the three sub-questions, namely *"Is there a potential for discourse failure?"*. This sub-chapter builds on the analysis from two previous sub-chapters. It shows both why, and in what concrete ways, the discourse surrounding the PST´s decision not to share confidence indicates a strong potential for discourse failure: a situation in which the intelligence consumer interprets

[27] «Og vel vitende om at vi på det tidspunktet har vi gjort x antall fremstøt overfor PST for å bedre dialogen, både enkeltvis, altså direkte på sjef PST, samlet utvalgsmessig, alle de store norske internasjonale er samlet i et utvalg, vi har gjort det sammen som utvalg. Vi har gjort det via NSR, og direktør i NSR, og for sjef PST […]»

[28] «[…] og det kan godt hende at hensikten var en annen, men det du da skaper er en enda større avstand i en eller annen form for fremtidig dialog med den tilnærmingen. Og for oss er det jo en form for arroganse i det.»

[29] «Ja, jeg tror at det er et uforløst, at samarbeidet kan bli bedre. Da tror jeg at det mest konkrete der ville kunne være å gi de brifer som ikke er offentlige, men som heller ikke er graderte.»

[30] « […] budskapet til næringslivet er, at, «der man ønsker kontakt, så ta kontakt». Og det er ikke alltid vi klarer å initiere ting, fordi vi vet ikke, eller ser ikke, eller aner ikke, eller har ikke kunnskap, eller har ikke tenkt tankene. Så hvis det er firma som på en måte sitter og ønsker gjerne å snakke med PST, så må de ta kontakt.»

intelligence in a different way than what the intelligence producer expects, due to individual factors relating to human cognition, and external factors like the amount of dialogue between the producer and the consumer (Hatlebrekke, 2019).

Before delving into the reasons why I conclude that there is a large potential for discourse failure, I want to highlight one fact which could reduce the potential for discourse failure. Namely that the PST seem to be aware of the issues related to how individuals interpret threat communication. This was best illustrated during the interview with PST 1, who described how they go about asking follow-up questions aimed at checking that people understand what PST 1 said when holding presentations for private sector actors.[31] While I am not privy to exactly which questions PST 1 asks, this approach can help increase the degree to which the actors belong in the same discursive realm by engaging the intelligence consumer in a two-way dialogue. Thereby reducing the potential for discourse failure between the PST and those present at these presentations.

The rest of this sub-chapter is structured as follows. Firstly, I look at a dynamic which could cause discourse failure. Secondly, I show examples of this dynamic in the discourse. Thirdly, I discuss whether, on a more theoretical and conceptual level, discourse failure is inevitable in my chosen case.

5.3.1 Dynamic which could cause discourse failure

When identifying dynamics which could cause discourse failure, one needs to look for things which impact the degree to which the actors belong to the same discursive realm. By discursive realm I mean that they have some shared points of reference, and a common understanding of meaning and the context within which said meaning is produced and communicated (Kristoffersen and Hatlebrekke, 2023, p. 213). According to Hatlebrekke (2019, p. 227), "a consumer's comprehension of the intelligence product depends on the quality of the dialogue between the producer and the consumer". It is the quality of, and at

[31] «Og så tror jeg at mottakere er forskjellige også. Så misforståelser bør man jo unngå i stor grad. Men da tenker jeg at det er viktigere at man i alle fall har, hvis man har mulighet da, til å få lest tilbake da, fra forsamlingen: «hva jeg har sagt nå?». Jo, du har sagt følgende. Ok. Da har du i alle fall skjønt det jeg har kommunisert. Det er sånn sjekk her. Men jeg tror alltid du vil få. Folk er forskjellige da. Og folk oppfatter ting ulikt.»

times absence of such dialogue which is the main dynamic contributing to increased potential for discourse failure in the case I am analysing.

When talking about how difficult it is to communicate about threats to the public, PST 2 said "that is the reason why we all the time have a continuous dialogue with ourselves about how we can solve this".[32] The admission that threat communication is difficult, and that the PST is still trying to improve is not really noteworthy. That being said, it is noteworthy that when trying to solve issues related to *external* threat communication, the PST has an *internal* dialogue. When one is struggling to find out how one can communicate to a group, surely engaging in dialogue with said group would increase one´s chance of success? The fact that the PST has decided to have this dialogue internally is, based on the interviews I have done, indicative of the PST´s overarching approach to threat communication.

5.3.2 Examples of lack of dialogue

I now want to show some concrete examples of how lack of dialogue between the PST and the private sector is leading to different understandings of reality. The goal of this is to demonstrate the lack of dialogue, as this is a core thing which can cause discourse failure. To do so, I highlight examples of where the PST and the private sector have different understandings of key aspects of their relationship. I cover examples which are related to the following things: the PST´s mandate, what constitutes sharing, what to share, and sharing vs dialogue. As with other parts of this analysis chapter, factors like regional location, prior experiences, which sector they belong to and more might impact the different interviewees´ understanding of reality. When this seems to have a strong impact on an interviewee´s understanding of reality, I highlight that. However, it is still worth noting that this is something which might bias this analysis, something I discuss more in the in the conclusion chapter.

While one might say that the different understandings of reality might be a result of different opinions and not a result of lacking dialogue, the way the interviewees talked about these issues makes it clear to me that not just disagreements, but different

[32] «Det er jo derfor vi hele tiden, det er en sånn kontinuerlig dialog med oss selv om hvordan vi skal løse dette.»

understandings of reality brought on by a lack of understanding/awareness of the other side´s understanding of reality, resulting from a lack of dialogue.

The PST´s mandate

In Norwegian law, the PST´s mandate is found in the Police Act paragraph 17a and 17b (*The Police Act*, 1995). While the interviewees who brought up the PST´s mandate all acknowledged that this is the legal mandate for the PST, there were some different interpretations of what this mandate entails in practice. One example of this is whether it's appropriate that the PST can/should have so-called "private sector contacts". Currently, the police, the National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM), and The National Criminal Investigation Service (KRIPOS), all have private sector contacts which are individuals tasked with engaging with private sector actors on a daily basis with the aim of preventing crime targeted at private sector companies (NSR, no date).

Every single interviewee on the private sector side all praised the work done by the current private sector contacts, and said that they could not understand why the PST would not establish a similar structure. Industry 1, who said that they could not in their wildest fantasies understand why the PST does not establish private sector contacts, as doing so would make both the PST´s life and the private sector´s life much easier,[33] went on to say that they thought that the PST didn't think that having regular contact with the private sector was part of their mandate. Industry 1 was very clear on the fact that they did not interpret the PST´s mandate in this way, but this was merely how they guessed that the PST interpreted their own mandate.

When I asked the PST about their lack of private sector contacts, PST 1 said that "if one looks at the Police Act 17a and 17b, it´s prevention of among other things illegal intelligence operations which is our job. So, it´s perhaps not natural for the PST to have formalised roles

[33] «Jeg kan ikke i min villeste fantasi skjønne hvorfor de ikke har det, for det ville gjort deres hverdag enklere, og det ville gjort vår hverdag enklere.»

as private sector contacts”.[34] PST 2 said that while they did not know exactly what the police´s private sector contacts did, they thought that the PST officials who work on engagement with external actors fills roughly the same role as private sector contacts would. Furthermore, they also said that the police´s private sector contacts provide the PST with relevant information, and that having their own contacts was probably not necessary.

The PST interviewees´ view on this matter stands in stark contrast to how the private sector sees this matter, thereby demonstrating a lack of shared understanding of reality. Given that the private sector does not see how the PST´s mandate is a reason for the PST not having private sector contacts, this is also an example of why the private sector might see the PST´s lack of engagement with the private sector as being a result of a lack of willingness, and not a result of their ability being restricted by existing laws.

What constitutes sharing?

Another example of differing understandings of reality is related to what constitutes sharing of intelligence. Again, this is an example of where the PST´s and the private sector´s understanding differ from each other. NSR 1 was the interviewee which most clearly articulated this issue. They said that the officials at the PST who work on external communication think that they are sharing a lot as they are increasingly present in the media, they publish the NTV, they have a podcast, and so on. However, according to NSR 1, for those in the professional security environment, this might not be considered sharing. Even though the PST does publish a lot of information, this information is not considered as “sharing” because it is open to anyone who wants to read it.[35]

In addition to being an example of the two sides not having a shared understanding of what constitutes sharing, this finding can help explain why the PST thinks that they are pretty

[34] «Hvis man leser liksom politiloven 17a, 17b da, så er det det som går på forebygging av blant annet ulovlig etterretningsaktivitet, som er jobben vår. Så i det er det kanskje ikke naturlig å ha formalisert roller som næringslivskontakter for PST.»

[35] «Men det er akkurat som at du føler at hvis du jobber i profesjonelle sikkerhetsmiljøet, så føler du også litt at de offentlige produktene er liksom ikke deling. Det er offentlig. Det kan jo hvem som helst lese. Og så skapes det en følelse av at du ikke får informasjon fordi det som kommer er offentlig. Men det kommer jo masse informasjon»

good at sharing information, whilst my private sector interviewees tend to have a different and far less positive interpretation of the amount of information which is "shared".

What to share?

While on the topic of intelligence sharing, there is also a question about what kind of information the private sector expects the PST to share, and what information the PST themselves sees as their job to share. During the interviews, a recurring criticism of the PST was that the information they share is too general, not well enough targeted at the interviewees´ sector, and more broadly that the PST doesn't seem to understand the different sectors. Energy 1 said that the PST must have a broad, "jack of all trades, master of none" approach owing to them being a state organisation. However, they were still critical of what they perceived as the PST´s lack of understanding of sector/company specific issues. This is also something which was highlighted by other interviewees who wanted more concrete threat assessments and not what they describe as the broad/general type of information which is currently published in the NTV.

Both PST 1 and PST 2 recognised that some actors may feel as though the NTV for instance is not as applicable to them as it is to other companies or sectors. However, when talking about an actor who had requested advice from the PST about whether they should purchase a specific piece of equipment used for oil drilling, PST 2 said the following:

> "So, if someone is disappointed based on them not getting that information, they will continue to be disappointed. It is up to the individual company to figure that out".[36]

This quote stands in quite stark contrast to the expectations the private sector has to the PST´s intelligence sharing. It therefore shows how the private sector expecting something of the PST which the PST does not see as their job, something which lends further support to the claim that there is a lack of dialogue, resulting in different understandings of reality.

[36] «Så hvis noen er skuffet på den bakgrunnen, så vil de jo fortsette å være skuffet. Det er opp til bedriften å finne ut av det.»

Sharing vs dialogue

The final example of lack of dialogue and differing understandings of reality I want to highlight is related to what the actors expect their relationship to look like. Specifically, this relates to whether the actors expect that the relationship to be based on sharing, primarily from the PST to the private sector, or on a two-way dialogue. PST 1 and PST 2 very clearly expressed that they want the private sector to reach out when they have something to report. Simultaneously, PST 1 said that the reason for why the private sector might not be happy with the current state of the relationship was that some might not get the PST to come to them to give a presentation about threats. To me, this shows that the PST thinks that what the private sector expects from the relationship is sharing, primarily from the PST to the private sector.

When taking to the private sector, they had a very different view on what they expected the relationship to look like. Firstly, both Industry 1 and Finance 1 said that they have information that they thought the PST could find useful, but that they didn’t get the impression that the PST wanted it. Given the sheer amount of appeals the PST make for information I found this very surprising. I have been unable to find any explanation for this, either in my interview data or in other sources. However, it is seemingly an example of where the PST´s stated desire for the private sector to share information has not been communicated in a way which has shaped how the private sector understand the PST and the relationship.

Secondly, in addition to some of them not feeling as though the PST wanted their information, all the three private sector interviewees expressed a desire for more regular dialogue with the PST, as opposed to what they experience today which they described as top-down, one-way communication from the PST. Specifically, they wanted to have a regular dialogue which could lower the threshold to ask questions and discuss things like confidence. The takeaway here is that while the PST thinks that what the private sector is expecting more sharing, the private sector in fact expects a continuous dialogue. This chasm between the private sector´s view and the PST´s understanding yet again illustrates a lack of dialogue and two very different understandings of reality, hereunder the other sides´ understanding of reality.

From a theoretical perspective, regular dialogue has two distinct benefits. Firstly, according to Kristoffersen and Hatlebrekke (2023, p. 79), regular dialogue will lead to a more shared understanding of reality, thereby contributing to reducing tension in the relationship between the PST and the private sector, which has resulted from differing understandings of reality. Secondly, dialogue is key to reducing the potential for discourse failure, as when quality dialogue accompanies intelligence sharing, it helps overcome issues related to cognitive closure and the problem of induction (Hatlebrekke, 2019, p. 227).

5.3.3 The inevitability of discourse failure

During the abductive process of going back and forth between the data I have analysed, and the theories and context which is the foundation for said analysis, I found a potential shortcoming with the discourse failure theory when it's applied to intelligence communication from a state actor to a non-state actor. The issue, which has led me to name this section "the inevitability of discourse failure", is a result of a tension between the way the Norwegian total defence is structured, hereunder which type of information the private sector has access to, and the way discourse failure is understood in the existing academic literature.

While I have discussed what discourse failure is, I have so far not properly discussed the origin of the theory, barring *who* coined the term. In the piece which is cited as the source of the term, discourse failure is presented as an explanation for why the US was unable to prevent the 9/11 terror attacks (Neumann and Smith, 2005). Discourse failure is viewed as one "failure", like collection failure or analytical failure, which can contribute to an intelligence failure. Intelligence failure is "when an actor does not collect and analyse information adequately, formulate sound policy based on intelligence (and other considerations), or respond effectively" (Clark, 2023). The key takeaway from the origin of the term discourse failure, is that it was created to describe a failure *within* the state apparatus. This is notable because intelligence consumers within the state have access to classified information, as opposed to intelligence consumers in the private sector in Norway who, barring a select few companies, don't have access to this kind of information. Given that an intelligence consumer´s understanding of the intelligence, and by extension the potential for discourse failure, is largely dependent on a "the quality of the dialogue between the producer and the consumer” (Hatlebrekke, 2019, p. 227), the fact that the intelligence producer is not allowed to share classified information is a significant barrier to achieving this kind of quality dialogue. Going back to the willingness vs ability discussion from earlier in this chapter, this means that even if the PST is *willing* to engage in quality dialogue with the private sector with the aim of reducing the potential for discourse failure, they are not *able* to share classified information which could help create a shared understanding of reality. The reason being that sharing more detailed pieces of information, whether the information is classified or not, would diminish the value of said intelligence and expose sources and methods of collection as was described by my interviewees.

This leads onto the aforementioned shortcoming in the way discourse failure is understood in the existing academic literature. In the literature, whether that be in the article which introduced the term discourse failure (Neumann and Smith, 2005) or Hatlebrekke´s (2019) book “The Problem of Secret Intelligence”, discourse failure is presented as something which is avoidable. Hatlebrekke (2019, p. 33) acknowledges that even when there is a good quality dialogue between intelligence producer and consumer, and the consumer has access to classified information, discourse failure can occur due to cognitive closure on the part of the consumer. However, he still describes discourse failure in a way which leads me to conclude that he views it as avoidable.

For the reasons described above, this thesis challenges the view that discourse failure is avoidable, specifically in a situation where the intelligence consumer is an actor without access to classified information. Furthermore, in addition to seeing discourse failure as being to some extent unavoidable in this situation, it is increasingly difficult to avoid it when the piece of intelligence being communicated is a probability and/or confidence assessment. As shown by the studies discussed in the theory chapter (see for example, Dieckmann, Mauro and Slovic, 2010; Mandel, 2020; Duke, 2023; Irwin and Mandel, 2023), confidence and probability words are prone to misunderstanding. While threat assessments like the PST´s NTV contain descriptions of threat actors in addition to the probability point assessments, this type of publicly available product cannot contain the same level of detail about threat actors as classified assessments communicated to decision-makers in government. Hence, even if the PST has the willingness to engage in quality dialogue to iron out misinterpretations and discourse failure related to the communication of threats using probability and confidence assessments, they are not allowed to do so to the same extent as they can do when dealing with actors with security clearances within the state.

Viewing discourse failure as something which is to some extent unavoidable (at least in my case) means that the starting point for assessing whether there is a potential for discourse failure is not whether there is potential discourse failure or not, but whether there is a potential for *more* discourse failure. This view is based on one not seeing discourse failure as a binary issue; meaning that one doesn’t see discourse failure as either occurring or not occurring. The two key pieces looking at discourse failure (Neumann and Smith, 2005; Hatlebrekke, 2019), don’t directly address this question. That being said, in several places throughout his book, Hatlebrekke (2019) mentions how different factors has the potential to *increase* discourse failure which leads me to conclude that he doesn’t see the degree to which discourse failure is present as a binary matter. Reason being that it would be strange to talk about an increase of anything if one treats said thing as only having two outcomes or states (a binary).

Finally, it’s worth noting that I am not saying that eliminating discourse failure between the PST and the private sector is impossible. My argument is that within the confines of the *current system* of information sharing, discourse failure is unavoidable. Still, with increased de-classification of intelligence combined with a system for “unclassified but still secret” information sharing, as highlighted by NSR 1, and better dialogue between the PST and the private sector, the potential for *increased* discourse failure can be reduced. However, as long as the PST and the private sector doesn’t have access to the same information, it will be difficult for the actors to have the same understanding of reality. Furthermore, even if they had access to the same information, it is likely that other factors impacting people´s interpretation, like cognitive closure, would prevent a complete elimination of discourse failure.

Chapter 6: Conclusion

It has been almost 20 years since Neumann and Smith (2005) introduced the term "discourse failure". And while discourse failure has received some scholarly attention over the years, perhaps most notably in the work of the late Kjetil Hatlebrekke (2019), it is still mainly confined to academia as well as to intelligence and security services. As I expand on in this chapter, this thesis shows that discourse failure is not merely an abstract academic concept. Rather, it seems to be a term which describes a concrete situation caused by the current state of the relationship between the PST and the private sector in Norway.

The process of conducting this study has consisted of several key steps, culminating in the different chapters in this thesis. In chapter 1, I introduced my research topic and my research question, including my three sub-questions. I also provided an overview of how the thesis would proceed, and a short introduction to my main argument. In chapter 2, I situated my study in a broader empirical context and laid out the case for this thesis´ empirical relevance for current affairs, and for the field of peace and conflict studies. Furthermore, this chapter also provided the reader with the contextual understanding needed prior to engaging with the subsequent chapters. In chapter 3, I introduced the reader to the theories and studies upon which my study is built. In doing so, I introduced the reader to key concepts and debates in the literature which formed the basis for my data construction and my subsequent analysis. In chapter 4, I laid out how I have gone about conducting my study, why I have made the choices I have made, and the implications of those choices. Finally, in chapter 5 I analysed the data I have constructed, in light of the theories and context provided in earlier chapters. Here, I showed (1) how and why the private sector and the PST have different understandings of confidence, (2) how the relationship between the PST and the private sector is marked by different understandings of the reality of their relationship, and finally (3) why the data indicates a large potential for discourse failure.

I will now provide an overarching conclusion, building on the analysis in chapter 5, and the contents from the other chapters. Finally, I round of this thesis by discussing limitations of my study, policy suggestions, and suggestions for further studies.

6.1 Main conclusion

So: ***what are the main challenges in the PST´s threat communication to the private sector?*** The discourse I have analysed shows that the main challenge in the PST´s threat communication is a lack of dialogue between the PST and the private sector. This lack of dialogue results in a large potential for discourse failure, and in a lack of a shared understanding of reality which negatively impacts the broader relationship between the PST and the private sector.

In the analysis chapter, I presented several examples of both a lack of dialogue, and concrete instances of the resulting lack of shared understanding of reality. These include different understandings of how much confidence the PST´s assessments have, who has agency to improve the relationship between the PST and the private sector, and whether its ability or willingness which is impacting the degree to which the PST engages in dialogue, and shares intelligence with the private sector. A quote from my interview with Energy 1 is illustrative of my interpretation of the discourse surrounding intelligence sharing and the relationship between the PST and the private sector:

> "My experience is that they present information. They give us a product, the offer us something we can choose to read and relate to. I don't experience that there is a great expectation from the PST that we will do anything [with the information], really. We just don't hear anything else from them".[37]

As I discussed when answering the third sub-question which focuses on whether there is a potential for discourse failure, and when presenting the discourse failure theory, there is a clear link between lack of dialogue and discourse failure. Simply put, dialogue is needed to counteract the induction problem and cognitive closure, which can result in the intelligence consumer not interpreting the intelligence shared by the intelligence produced in the way the producer expects (Hatlebrekke, 2019). Therefore, when intelligence is shared in a situation where dialogue is not occurring, the value of sharing said intelligence is reduced because the intelligence will have a high chance of being misinterpreted.

[37] «Jeg opplever at de presenterer informasjon. De gir oss et produkt, de tilbyr oss noe som vi kan velge å lese og forholde oss til. Jeg opplever jo ikke at det er noen stor forventning fra de om at vi skal gjøre noe, egentlig. Vi hører jo ikke noe fra de ellers.»

Stepping back, it’s worth reflecting on the consequences of my findings and analysis for the Norwegian total defence. If, as I have found in my study, there is a lack of dialogue between the PST and the private sector, and there is a large potential for discourse failure, this will have a direct impact on the Norwegian total defence. This is because if the private sector is misinterpreting the information shared by the PST, this will result in the private sector having a faulty knowledge foundation when they are assessing the threat in the NS 5832 triangle risk assessment method (Busmundrud *et al.*, 2015). Incorrectly assessing the threat, and therefore the risk posed to one´s company, will result in said company implementing measures which are not correctly scaled to the “true” risk they face. Given the private sector´s importance for the Norwegian total defence and national security, especially in the current geopolitical security situation, the result will therefore be a weakened total defence.

This finding sits at the core of this study´s contribution to knowledge within the field of peace and conflict studies. By studying the relationship between key actors in the Norwegian total defence through analysing the PST´s threat communication to the private sector, this thesis has contributed to knowledge about how to “understand the multifaceted challenges associated with war and conflict” (University of Oslo, no date). Furthermore, the interdisciplinary nature of peace and conflict studies as a sub-field has also been well suited to this study as it has enabled me to draw on theories and knowledge from several academic fields. Including, but not limited to, psychology, communication studies, security studies, and the broader field of political science.

6.2 Limitations

There are three main limitations to this study. The first has to do with the number of people I have interviewed. While conducting seven interviews for a master´s thesis is by no means a small amount, the potential for selection bias is still something worth considering. This is something I expanded on in the methods chapter, but it’s worth reiterating that I have tried to mitigate the impact of the amount of interview data by looking at other sources, and by interviewing the NSR. The aim of doing this was to enhance the credibility of the findings through the process of triangulation, or the act of using different sources and angles to access a claim or issue to ensure the quality of the findings (Natow, 2020).

The second limitation has to do with the degree to which the individuals I have interviewed are representative of the views, and interpretation of reality, within their organisation or institution. While my study builds on the sociological institutionalism theory, which tells us that individuals´ understanding of reality is impacted by the institutions they are part of (Hall and Taylor, 1996), how individuals interpret things are also impacted by individual factors, such as prior experiences. For example, Industry 1 might have been more critical of the PST than other interviewees because they remember when the PST had a local office in Sandvika, which Industry 1 used to have a more continuous dialogue with. Therefore, a limitation of this study is that there is no guarantee that I have gotten an accurate overview of the way the PST and the private sector understand key issues through interviewing individuals in these institutions. That being said, as with the first limitation, I have tried to compensate for this by triangulating my findings by incorporating additional sources like reports assessing the PST (see for example, The Traavik Committee, 2012), in my analysis.

The third limitation, which I also expanded on in the methods chapter, has to do with the fact that the analysis in this study is based on so-called double hermeneutic, or interpretation of interpretation (Giddens, 1982). This means that there is a risk that my prior experiences, including my quasi-insider status within the security field, could lead me to interpret the data in a way which doesn't reflect the understanding of reality my interviewees tried to convey. However, given that issues related to subjective interpretation in interpretivist studies like this one is not something one can avoid, I have merely been reflexive about my own position and background to highlight what has led me to interpret the data in the way I did.

6.3 Policy suggestions

One question I have left unanswered so far is whether confidence should be shared. Based on the data I have analysed and the studies I have presented in the theoretical framework chapter, my suggestion is that confidence should be shared with the professional security environment in the private sector. There are two closely related reasons for this. Firstly, there is no clear understanding in the private sector of how much confidence the PST´s threat assessments are imbued with. Secondly, how much confidence the private sector thinks that the PST´s assessments are imbued with seemingly has a direct impact on which measures they implement. Therefore, sharing confidence would create a shared understanding of the level of confidence in the PST´s assessments, which would improve the private sector´s understanding of the threats they face. It is important to note that if confidence was to be shared, it should be accompanied by increased dialogue between the PST and the private sector about things like how to understand the relationship between confidence and probability. The reason for this is that studies have shown that sharing confidence in addition to probability can lead to increased misinterpretation of the probability assessment (Irwin and Mandel, 2023, p. 952).

While I suggest that confidence should be shared with the professional security environment, I don’t think that it should be shared with the broader public. This is because, as was described by NSR 1, the broader public doesn’t have the same foundation for understanding confidence and its relationship with probability as the professional security environment has. Furthermore, the broader public is not in charge of specific mitigating measure in the same way as the private sector is. Hence, sharing confidence with the public would not have the same potential positive effect as sharing confidence with the private sector, while also having a higher change of causing confusion. Finally, sharing confidence with the broader public would have a far greater risk of exposing what the PST knows to unfriendly actors than just sharing it in a secret, but not classified way to the professional security environment in the private sector.

Another policy suggestion based on my study is that the PST, and the broader state apparatus, should conduct a thorough assessment of how information about threats is communicated to private sector actors, with specific emphasis on issues related to dialogue, and how information is interpreted. Furthermore, the PST should engage in dialogue with the private sector, perhaps facilitated by the NSR, with the aim of trying to create (and maintain) a shared understanding of each other´s views, and what they want their relationship to look like. Doing so could reduce some of the tension and frustration I picked up on during my interviews. Furthermore, this could improve the cooperation between the PST and the private sector, something which would be in the best interest of all parties, and of the Norwegian total defence more broadly.

6.4 Further studies

I have two suggestions for further studies. The first is to interview a broader group of people, both in different sectors, in different parts of Norway, and at companies of different sizes, to see if my findings are representative of the private sector at large, or just of a couple of large companies in the Oslo-region. The second suggestion is to conduct a similar study in both the other Scandinavian countries, who all have police security services akin to the Norwegian Police Security Service, and in countries with civilian/non-police security services. The goal of doing so would be to see if my findings are unique to countries with police security services, or a broader phenomenon impacting the relationship between security services and the private sector.

Bibliography:

Alvesson, M. and Spicer, A. (2019) ‘Neo-Institutional Theory and Organization Studies: A Mid-Life Crisis?’, *Organization Studies*, 40(2), pp. 199–218. Available at: https://doi.org/10.1177/0170840618772610.

Bergersen, S. (2023) *Conveying complex uncertainty: The dilemmas of communicating about terror threats.* PhD Thesis. Vrije Universiteit Brussel. Available at: https://cris.vub.be/ws/portalfiles/portal/107978383/BERGERSEN_Stine_Doctoraat.pdf.

Bråthen, K. (2021) *Å dele, eller ikke dele? En sammenlignende casestudie av informasjonsdeling i det forebyggende arbeidet mot radikalisering og voldelig ekstremisme i Skandinavia*. Master thesis. Available at: https://www.duo.uio.no/handle/10852/88592 (Accessed: 11 December 2023).

Brown, G.W., McLean, I. and McMillan, A. (eds) (2018) *The Concise Oxford Dictionary of Politics and International Relations*. Fourth edition. Oxford, United Kingdom: Oxford University Press (Oxford quick reference).

Brown, Z.T. (2020) *What If Sherman Kent Was Wrong? Revisiting the Intelligence Debate of 1949*, *War on the Rocks*. Available at: https://warontherocks.com/2020/10/what-if-sherman-kent-was-wrong-revisiting-the-intelligence-debate-of-1949/ (Accessed: 28 November 2023).

Busmundrud, O. *et al.* (2015) *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. 2015/00923. Kjeller: FFI. Available at: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/1178/15-00923.pdf (Accessed: 6 November 2023).

Clark, A. (2023) ‘Intelligence Failure: What, When, Why and How’, *Grey Dynamics*, 4 September. Available at: https://greydynamics.com/intelligence-failure-what-when-why-how/ (Accessed: 22 April 2024).

Cook, M.B. and Smallman, H.S. (2008) ‘Human Factors of the Confirmation Bias in Intelligence Analysis: Decision Support From Graphical Evidence Landscapes’, *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 50(5), pp. 745–754. Available at: https://doi.org/10.1518/001872008X354183.

Dagsnytt 18 - 13. januar 2023 (2023). Oslo. Available at: https://tv.nrk.no/serie/dagsnytt-atten-tv/202301/NNFA56011323 (Accessed: 4 December 2023).

Davies, P.H.J. (2001) ‘Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services’, *Politics*, 21(1), pp. 73–80. Available at: https://doi.org/10.1111/1467-9256.00138.

Dieckmann, N.F., Mauro, R. and Slovic, P. (2010) ‘The Effects of Presenting Imprecise Probabilities in Intelligence Forecasts’, *Risk Analysis*, 30(6), pp. 987–1001. Available at: https://doi.org/10.1111/j.1539-6924.2010.01384.x.

Duke, M.C. (2023) ‘Probability and confidence: How to improve communication of uncertainty about uncertainty in intelligence analysis’, *Journal of Behavioral Decision Making* [Preprint]. Available at: https://doi.org/10.1002/bdm.2364.

Dunn, K.C. and Neumann, I.B. (2016) *Undertaking discourse analysis for social research*. Ann Arbor: University of Michigan Press.

E-tjenesten (2023) *Fokus 2023*. Oslo: E-tjenesten. Available at: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf/_/attachment/inline/c1a9a458-aa1d-4bf6-a558-9cec57acde8f:9b2050d897a2b2db1bddc8e505db7b666e608b98/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf.

FFI (2022) *Kort forklart: Hva er totalforsvaret?* Available at: https://www.ffi.no/aktuelt/podkaster/kort-forklart-hva-er-totalforsvaret (Accessed: 14 November 2023).

Friedman, J.A. and Zeckhauser, R. (2012) 'Assessing Uncertainty in Intelligence', *Intelligence and National Security*, 27(6), pp. 824–847. Available at: https://doi.org/10.1080/02684527.2012.708275.

Fujii, L.A. (2017) *Interviewing in Social Science Research: A Relational Approach*. 1st edn. New York: Routledge. Available at: https://doi.org/10.4324/9780203756065.

Gallie, W.B. (1955) 'Essentially Contested Concepts', *Proceedings of the Aristotelian Society*, 56, pp. 167–198.

Gerring, J. (2012) 'Mere Description', *British Journal of Political Science*, 42(4), pp. 721–746. Available at: https://doi.org/10.1017/S0007123412000130.

Giddens, A. (1982) 'Hermeneutics and Social Theory', in Giddens, A., *Profiles and Critiques in Social Theory*. London: Macmillan Education UK, pp. 1–17. Available at: https://doi.org/10.1007/978-1-349-86056-2_1.

Goertz, G. and Mahoney, J. (2012) 'Concepts and measurement: Ontology and epistemology', *Social Science Information*, 51(2), pp. 205–216. Available at: https://doi.org/10.1177/0539018412437108.

Hall, P.A. and Taylor, R.C.R. (1996) 'Political Science and the Three New Institutionalisms', *Political Studies*, 44(5), pp. 936–957. Available at: https://doi.org/10.1111/j.1467-9248.1996.tb00343.x.

Halperin, S. and Heath, O. (2020) *Political research: methods and practical skills*. Third edition. New York: Oxford University Press.

Halvorsen, B.O. (2020) *Samme språk eller stammespråk. Åpner etterretningsbrukeres forståelse av etterretningsprodusenters vurderingsterminologi for diskurssvikt?* Master thesis. Forsvarets høgskole. Available at: https://fhs.brage.unit.no/fhs-xmlui/handle/11250/2676984 (Accessed: 15 December 2023).

Hatlebrekke, K.A. (2019) *The problem of secret intelligence*. Edinburgh: Edinburgh University Press (Intelligence, surveillance and secret warfare).

Hood, C. (2011) *The Blame Game: Spin, Bureaucracy, and Self-Preservation in Government*. Princeton University Press. Available at: https://www.jstor.org/stable/j.ctt7tc57 (Accessed: 9 January 2024).

Hovland, K.M. and Holmes, M.C.S. (2022) *Equinor og Gassco lagt under sikkerhetsloven: – Naturlig at vi skjerper beredskapen*. Available at: https://e24.no/i/xg8Awn (Accessed: 20 November 2023).

Hovtun, L.M. (2023) *Næringslivet er ikke rustet for krise og krig*, *Altinget.no*. Available at: https://www.altinget.no/artikkel/naeringslivet-er-ikke-rustet-for-krise-og-krig (Accessed: 10 October 2023).

IFE (no date) *About IFE*, *IFE*. Available at: https://ife.no/en/about-ife/ (Accessed: 17 November 2023).

Indrebø-Langlo, M. and Jacobsen, H.B. (2023) ‘Regjeringen snur - lover 2,6 milliarder til Nammo’, *Regjeringen snur – lover 2,6 milliarder til Nammo*, 13 January. Available at: https://www.tv2.no/nyheter/innenriks/regjeringen-snur-lover-26-milliarder-til-nammo/15422882/ (Accessed: 14 November 2023).

Intelligence Reform And Terrorism Prevention Act Of 2004 (2004). Available at: https://www.govinfo.gov/content/pkg/PLAW-108publ458/html/PLAW-108publ458.htm (Accessed: 1 December 2023).

Irwin, D. and Mandel, D.R. (2023) ‘Communicating uncertainty in national security intelligence: Expert and nonexpert interpretations of and preferences for verbal and numeric formats’, *Risk Analysis*, 43(5), pp. 943–957. Available at: https://doi.org/10.1111/risa.14009.

Jamieson, M.K., Govaart, G.H. and Pownall, M. (2023) ‘Reflexivity in quantitative research: A rationale and beginner’s guide’, *Social and Personality Psychology Compass*, 17(4). Available at: https://doi.org/10.1111/spc3.12735.

Kent, S. (1964) ‘Words of estimative probability’, *Studies in Intelligence*, 8(4), pp. 49–65.

Kibar, O. (2024) ‘PST-veteran kritiserer hysj-tjenestenes hemmelighold – mener næringslivet får for lite informasjon’, *Dagens Næringsliv*, 12 February. Available at: https://www.dn.no/innenriks/pst/nsm/pst-veteran-kritiserer-hysj-tjenestenes-hemmelighold-mener-naringslivet-far-for-lite-informasjon/2-1-1596593 (Accessed: 9 April 2024).

Kibar, O. and Engen, S. (2020) ‘PST hudfletter universitetene: «Fullstendig blåøyde og veldig, veldig naive»’, *Dagens Næringsliv*, 31 December. Available at: https://www.dn.no/magasinet/dokumentar/politiets-sikkerhetstjeneste/ntnu/tekna/pst-hudfletter-universitetene-fullstendig-blaoyde-og-veldig-veldig-naive/2-1-919171 (Accessed: 10 April 2024).

Kristoffersen, F. and Hatlebrekke, K. (2023) *Etterretning - fra innsiden av Etterretningstjenesten,oppdragene, menneskene og faget*. Oslo: Gyldendal Norsk Forlag AS.

LaBelle, M.C. (2023) ‘Energy as a weapon of war: Lessons from 50 years of energy interdependence’, *Global Policy*, 14(3), pp. 531–547. Available at: https://doi.org/10.1111/1758-5899.13235.

Lawless, J. (2023) ‘Global impact: 5 ways war in Ukraine has changed the world’, *AP News*, 22 February. Available at: https://apnews.com/article/russia-ukraine-war-5-things-c183ddfe6c140393464d3e0c3828c328 (Accessed: 14 November 2023).

Lieberman, E. (2020) ‘Research Cycles’, in C. Elman, J. Gerring, and J. Mahoney (eds) *The Production of Knowledge*. 1st edn. Cambridge University Press, pp. 42–70. Available at: https://doi.org/10.1017/9781108762519.003.

Macintyre, B. (2019) *The spy and the traitor: the greatest espionage story of the Cold War*. London: Penguin Books.

Mandel, D.R. (2020) *Assessment and Communication of Uncertainty in Intelligence to Support Decision Making: Final Report of Research Task Group SAS-114*. NATO. Available at: https://doi.org/10.31234/osf.io/vxh9r.

Mandel, D.R. (2022) ‘Intelligence, Science, and the Ignorance Hypothesis’, in R. Arcos Martín, N.K. Drumhiller, and M. Phythian (eds) *The academic-practitioner divide in intelligence studies*. Lanham: Rowman & Littlefield, pp. 79–94.

Mandel, D.R. and Irwin, D. (2021) ‘Uncertainty, Intelligence, and National Security Decisionmaking’, *International Journal of Intelligence and CounterIntelligence*, 34(3), pp. 558–582. Available at: https://doi.org/10.1080/08850607.2020.1809056.

March, J.G. and Olsen, J.P. (2004) ‘The logic of appropriateness’. University of Oslo (ARENA Working Papers, WP 04/09). Available at: https://www.sv.uio.no/arena/english/research/publications/arena-working-papers/2001-2010/2004/wp04_9.pdf (Accessed: 11 January 2024).

Marrin, S. (2008) ‘Intelligence analysis and decision-making: methodological challenges’, in P. Gill, M. Phythian, and S. Marrin (eds) *Intelligence Theory*. 1st edn. London: Routledge. Available at: https://www.taylorfrancis.com/chapters/edit/10.4324/9780203892992-14/intelligence-analysis-decision-making-methodological-challenges-stephen-marrin.

Merriam-Webster (no date) *‘Deduction’ vs. ‘Induction’ vs. ‘Abduction’*. Available at: https://www.merriam-webster.com/grammar/deduction-vs-induction-vs-abduction (Accessed: 20 February 2024).

Natow, R.S. (2020) ‘The use of triangulation in qualitative studies employing elite interviews’, *Qualitative Research*, 20(2), pp. 160–173. Available at: https://doi.org/10.1177/1468794119830077.

Neumann, P.R. and Smith, M.L.R. (2005) ‘Missing the Plot? Intelligence and Discourse Failure’, *Orbis*, 49(1), pp. 95–107. Available at: https://doi.org/10.1016/j.orbis.2004.10.008.

Norwegian Ministry of Defence (2023) *Store investeringer i Forsvaret*. Available at: https://www.regjeringen.no/no/aktuelt/investeringer23/id2970607/ (Accessed: 14 November 2023).

Norwegian Ministry of Defence and Norwegian Ministry of Justice and Public Security (2018) *Support and Cooperation, A description of the total defence in Norway*. S-1025 E. Oslo. Available at: https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/support-and-cooperation.pdf.

NSM (2023) *Sikkerhetsfaglig råd - Et motstandsdyktig Norge*. Oslo: Nasjonal Sikkerhetsmyndighet. Available at: https://nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20r%C3%A5d%20-%20Et%20motstandsdyktig%20Norge.pdf (Accessed: 10 October 2023).

NSR (2021) *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2021*. Oslo: Private Sector Security Council. Available at: https://www.nsr-org.no/uploads/documents/Publikasjoner/Krisino-2021.pdf.

NSR (no date) *Politiets næringslivskontakter*. Available at: https://www.nsr-org.no/om-nsr/politiets-naeringslivskontakter (Accessed: 11 April 2024).

Office of the Director of National Intelligence and National Intelligence Council (2021) *Updated Assesments on COVID-19 Origins*. Washington D.C. Available at: https://www.dni.gov/files/ODNI/documents/assessments/Declassified-Assessment-on-COVID-19-Origins.pdf (Accessed: 1 December 2023).

Petintseva, O., Faria, R. and Eski, Y. (2020) *Interviewing Elites, Experts and the Powerful in Criminology*. Cham: Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-33000-2.

PST (2023a) *Nasjonal Trusselvurdering 2023*. Oslo: Politiets sikkerhetstjeneste. Available at: https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/ (Accessed: 10 October 2023).

PST (2023b) *Ønsker du å bli leder for vårt nyopprettede avsnitt for utadrettet virksomhet?*, *FINN.no*. Available at: https://www.finn.no/job/fulltime/ad.html?finnkode=325009681 (Accessed: 23 November 2023).

PST (no date) 'Hva truer norsk næringsliv?' (Psst). Available at: https://shows.acast.com/psst/episodes/hva-truer-norsk-naeringsliv (Accessed: 22 November 2023).

Reuters (2024) 'Chinese spies target Dutch industries to strengthen military, intelligence agency says', *Reuters*, 18 April. Available at: https://www.reuters.com/world/china/chinese-spies-target-dutch-industries-strengthen-military-intelligence-agency-2024-04-18/ (Accessed: 2 May 2024).

Sartori, G. (1970) 'Concept Misformation in Comparative Politics', *The American Political Science Review*, 64(4), pp. 1033–1053. Available at: https://doi.org/10.2307/1958356.

Schwartz-Shea, P. and Yanow, D. (2012) *Interpretive research design: concepts and processes*. New York, NY London: Routledge (Routledge series on interpretive methods).

Seligman, L. (2023) 'U.S. has "high confidence" Palestinian militants to blame for Gaza hospital blast', *POLITICO*, 24 October. Available at: https://www.politico.com/news/2023/10/24/gaza-hospital-us-israel-hamas-00123365 (Accessed: 1 December 2023).

Stanghelle, H. (2023) 'Verdiløs trusselvurdering', *Aftenposten*, 14 June. Available at: https://www.aftenposten.no/meninger/kommentar/i/gEKAgq/verdiloes-trusselvurdering (Accessed: 4 December 2023).

The Defence Commission (2023) *Forsvarskommisjonen av 2021: Forsvar for fred og frihet*. NOU 2023: 14. Oslo. Available at: https://www.regjeringen.no/contentassets/8b8a7fc642f44ef5b27a1465301492ff/no/pdfs/nou202320230014000dddpdfs.pdf (Accessed: 14 November 2023).

The EOS committee (no date) *The EOS services*, *Norwegian Parliamentary Oversight Committee on Intelligence and Security Services*. Available at: https://eos-utvalget.no/en/home/about-the-eos-committee/the-eos-services/ (Accessed: 22 November 2023).

The Extremism Commission (2024) *Felles innsats mot ekstremisme: Bedre vilkår for det forebyggende arbeidet*. NOU 2024: 3. Oslo. Available at: https://www.regjeringen.no/contentassets/b09f8768c15d4d4f9ac8acfab0bf05e3/no/pdfs/nou202420240003000dddpdfs.pdf (Accessed: 9 April 2024).

The Police Act (1995). Available at: https://lovdata.no/dokument/NL/lov/1995-08-04-53/KAPITTEL_5#%C2%A717d (Accessed: 11 April 2024).

The Security Act (2018). Available at: https://lovdata.no/dokument/NLE/lov/2018-06-01-24 (Accessed: 12 December 2023).

The Total Preparedness Commission (2023) *Nå er det alvor: Rustet for en usikker fremtid*. NOU 2023: 17. Oslo. Available at: https://www.regjeringen.no/contentassets/4b9ba57bebae44d2bebfc845ff6cd5f5/no/pdfs/nou2023 20230017000dddpdfs.pdf (Accessed: 14 November 2023).

The Traavik Committee (2012) *Ekstern gjennomgang av Politiets sikkerhetstjeneste*. Oslo: Ministry of Justice and Public Security. Available at: https://www.regjeringen.no/globalassets/upload/jd/dokumenter/rapporter/2012/ekstern_gjennom gang_av_pst.pdf (Accessed: 9 April 2024).

Torres, M.A.N. (2023) 'Sterke politiske reaksjoner etter 25. juni-rapport: – Dette er rystende lesning', *Nettavisen*, 8 June. Available at: https://www.nettavisen.no/5-95-1145943 (Accessed: 4 December 2023).

University of Oslo (no date) *Peace and Conflict Studies (master's 2-years) – University of Oslo*. Available at: https://www.uio.no/english/studies/programmes/peace-master/index.html (Accessed: 30 April 2024).

Vickers, R. (2001) *Intelligence Warning Terminology*. PCN 40471. Washington D.C: Joint Military Intelligence College. Available at: https://www.hsdl.org/?view&did=7443 (Accessed: 4 April 2024).

Wason, P.C. (1960) 'On the Failure to Eliminate Hypotheses in a Conceptual Task', *Quarterly Journal of Experimental Psychology*, 12(3), pp. 129–140. Available at: https://doi.org/10.1080/17470216008416717.

Appendix:

NVivo codebook:

Name	Description
Confidence	Views on confidence and uncertainty in intelligence
Debate	Views on debate about confidence sharing
Misunderstanding	Mentions of misunderstanding as a consequence of sharing confidence
Private Sector	Views about the private sector
PST	Views about the PST
Information	Views about the information shared by the PST
Organisation	Views on the PST as an organisation
Relationship	Views on the relationship between the PST and the private sector

Overview of interviewees:

Interviewee codename	Details about interviewee
PST 1	PST counterintelligence department employee
PST 2	PST communication department employee
NSR 1	NSR employee
NSR 2	Individual associated with NSR
Industry 1	Individual working for an industry sector company
Energy 1	Individual working for an energy sector company
Finance 1	Individual working for a finance sector company

Interview guide: The Private Sector/ the NSR

Introduction questions:

Can you give me a quick rundown of your career so far, your current job and your responsibilities?

How much/how do you use the NTV and other information which comes from the PST?

Understanding of confidence/uncertainty:

Relationship between probability and confidence

Interpretation of the information the PST currently shares

How certain/uncertain do you think it is?

Why do you think that?

Confidence/uncertainty´s role in your work on security

How had information about high/low confidence impacted analysis and preventive measures?

Thoughts on whether the PST should share confidence:

Advantages and disadvantages for all parties

Is this something which is discussed internally or with people at other companies?

Relationship between the PST and the private sector:

“Ability and willingness to share is lacking” Do you agree with that assessment?

How would you describe your company´s/your sector´s role in the total defence?

Has it changed over time?

How do you think the PST views your role?

Broad impressions of the relationship between the PST and the private sector

Outro questions:

Information about the road ahead (quote check and distribution of final product)

Interview guide: The PST

Introduction questions:

Can you give me a quick rundown of your career so far, your current job and your responsibilities?

How much/how do you think that the private sector uses the NTV and other information which comes from the PST?

Understanding of confidence/uncertainty:

Relationship between probability and confidence

> Can you say something broad about how certain the PST´s information is and what impacts it´s uncertainty?

Interpretation of the information the PST currently shares

> How certain/uncertain do you think the private sector thinks it is?
>
> > Why do you think that?

Confidence/uncertainty´s role in the private sector´s work on security

> How had information about high/low confidence impacted analysis and preventive measures?

Thoughts on whether the PST should share confidence:

Advantages and disadvantages for all parties

Is this something which is discussed internally? What do other people at the PST think?

Relationship between the PST and the private sector:

"Ability and willingness to share is lacking" Do you agree with that assessment?

How would you describe the private sector´s role in the total defence?

> Has it changed over time?

How do you think the private sector views your role?

Broad impressions of the relationship between the PST and the private sector

Outro questions:

Information about the road ahead (quote check and distribution of final product)