

Finn Børre Holen

Sikkerhetskultur: Forståelse som utgangspunkt for utvikling

Hvordan forstå sikkerhetskulturbegrepet for å kunne beskrive, bevisstgjøre seg og utvikle hensiktsmessig sikkerhetskultur for den enkelte organisasjon

Masteroppgave i Operativ Maritim Ledelse

Veileder: Marte Fanneløb Giskeødegård

Mai 2023

Finn Børre Holen

Sikkerhetskultur: Forståelse som utgangspunkt for utvikling

Hvordan forstå sikkerhetskulturbegrepet for å kunne beskrive, bevisstgjøre seg og utvikle hensiktsmessig sikkerhetskultur for den enkelte organisasjon

Masteroppgave i Operativ Maritim Ledelse
Veileder: Marte Fanneløb Giskeødegård
Mai 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for ingeniørvitenskap
Institutt for havromsoperasjoner og byggteknikk



Kunnskap for en bedre verden

Sammendrag

Hensikten med denne oppgaven har vært å skape en bedre forståelse og et operasjonelt og nyttig begrepsapparat for å kartlegge, fortolke og beskrive sikkerhetskultur i organisasjoner. Oppgaven drøfter den relevansen av kultur for sikkerhetsfaget, gitt de særlige utfordringene med denne type arbeid.

Opgaven presenterer en oversikt over sikkerhetsfaget, med de prosesser og den terminologien som benyttes i dag. Gjennom en drøfting av relevant teori, blir sikkerhetsbegrepet og kulturbegrepet drøftet, og resultatet er en definisjon av sikkerhetskultur som:

De delte mentale modellene innenfor en organisasjon, som danner felles meningssystemer for medlemmene innenfor rammene av sosialt samspill og prosessene som påvirker forståelsen for og utførelse av sikkerhet i organisasjonen.

Studiens feltarbeid består av dybdeintervjuer med fem sikkerhetsfaglige eksperter. I empirien er sikkerhetskulturbegrepets definisjon og forståelsen av denne, kartlagt. Intervjuobjektene har reflektert rundt i hvilken grad og hvordan sikkerhetskultur kan måles eller kartlegges, og i hvilken grad man kan utvikle og endre den. Det er gjennom dette feltarbeidet identifisert særlige utfordringer ved sikkerhetsfaget som gjør det kulturelle aspektet særlig relevant.

Analysen av empirien er i hovedsak induktiv, men inkluderer også en deduktiv del som tester en hypotese om at sikkerhetskultur kan fortolkes og beskrives ut fra fem dimensjoner: Sikkerhetsforståelse, Trusselkognisjon, Risikoaksept, Menneskesyn og en Relasjons/konflikt-dimensjon.

Drøftingene av sikkerhetsfagets særlige utfordringer, identifisert som sannsynlighetsberegning og trusselvurderinger av bevisste ondsinnede trusselaktører, samt problematikken rundt å måle sikkerhetens effekt, viser relevansen av det kulturelle. Deretter drøfter oppgaven hvordan man kan benytte seg av en fortolkende kvalitativ tilnærming til sikkerhetskultur, men likevel vurdere sikkerhetskulturen ut fra om den er hensiktsmessig for den aktuelle organisasjonen.

Deretter drøftes de identifiserte sikkerhetskulturelle dimensjonene, og hvordan en leder kan benytte seg av disse både for å bevisstgjøre seg hvilken sikkerhetskultur som eksisterer, men også hva som vil være hensiktsmessig gitt organisasjonens trusselbilde og verdiene som man ønsker å beskytte.

Resultatet peker på at det er behov for en begrepsavklaring og et felles begrepsapparat når man snakker om temaet sikkerhetskultur, da det ikke eksisterer en enhetlig forståelse av hva begrepet betyr eller hvordan man skal kunne bruke det. De sikkerhetskulturelle dimensjonene er validert gjennom intervjuene med fagekspertene, og er et resultat av deres forståelse og vurdering av disse, samt de refleksjonene de gjorde om hva dimensjonene burde inneholde.

Studien konkluderer videre med at det er et lederansvar, å bevisstgjøre seg og å aktivt jobbe for at egen organisasjon skal utvikle en mest mulig hensiktsmessig sikkerhetskultur. Dette er en krevende oppgave der en leder må bruke en stor del av spekteret av ledelsesmetoder og makt for å kunne påvirke kulturen i ønsket retning.

Abstract

The objective of this study has been to create a better understanding and an operational and useful conceptual apparatus to examine, interpret and describe security culture in organisations. The study discusses the cultural relevance in the security field, given the special challenges in this type of work.

The study presents an overview of security as a practice, including the processes and the terminology used today. Through the debate of relevant theories, the terms security and culture are discussed, resulting in a definition of security culture:

The shared mental models within an organisation, which forms common systems of meaning for the members within the framework of social interaction and the processes that affects the understanding and the execution of security in the organisation.

The fieldwork of this study consists of in-depth interviews with five security experts. In the empiricism the definition and understanding of the term security culture is mapped. The respondents have reflected around in which degree and how security culture can be measured or mapped, and to what extent one can develop and change it. Through this fieldwork there are identified specific challenges within security work, which makes the cultural aspect especially relevant.

The analysis of the empiricism is mostly inductive, but also includes a deductive part, testing the hypotheses that security culture can be interpreted and described through five dimensions: Security understanding, Threat Cognition, Risk acceptance, Views on Human Nature and a Relations/conflict dimension.

The specific challenges associated with security, identified as probability calculation and threat assessments of the conscious malicious threat actors, together with the problem of measuring the effect of security, shows the relevance of the cultural aspect. The study discusses how one can use an interpretive qualitative approach to security culture, but at the same time assess security culture on whether it is appropriate for the organisation in question.

The study discusses the identified security cultural dimensions, and if a leader can use these to raise his or her consciousness of the existing security culture, but also what is suitable given the threat situation and the values the organisation needs to protect.

The results point to a need for a conceptual understanding and apparatus when one is talking about security culture, as there does not exist a common understanding of what this term means or how to use it. The security cultural dimensions are validated through the interviews with subject experts, and they are a result of their understanding and assessment of these, and their reflections about what the dimensions should include.

This study concludes further that is a leader responsibility, to make oneself conscious and active work towards the development of an appropriate security culture. This is a demanding task where leaders need to use a wide spectre of leadership methods and power to be able to influence the culture in desired direction.

Innhold

1. Innledning.....	4
1.1. Oppgavens hensikt	5
1.2. Struktur	6
2. Metode.....	7
2.1. Kvalitativ tilnærming	8
2.2. Kilder.....	9
2.3. Intervju.....	10
2.4. Transkribering	12
2.5. Koding og analyse.....	13
3. Sikkerhet – bakgrunnskapittel	14
3.1. Begrepsavklaring, definisjoner	14
3.2. Sikkerhetsfagets bestanddeler.....	16
4. Teori	24
4.1. Essensialistisk og fortolkende tilnærming	24
4.2. Kultur som delte mentale modeller	25
4.3. Utvikling av kultur: Meningsdanning – sensemaking.....	26
4.4. Sikkerhetskultur – en del av organisasjonskulturen.....	30
4.5. Lærende kultur	32
4.6. Ledelsesteori	34
4.7. Sikkerhetskulturelle dimensjoner.....	36
5. Presentasjon av empiri.....	40
5.1. Hvordan brukes sikkerhetskulturbegrepet?	40
5.4. Hvordan forstås de sikkerhetskulturelle dimensjonene?	45
5.5. Hva er særlige utfordringer med sikkerhetsfaget?	55
6. Drøfting	61
6.1. Sikkerhetsfagets kulturelle utfordringer.....	61
6.2. Fortolkende kvalitativ tilnærming til sikkerhetskultur	67
6.3. Hensiktsmessig sikkerhetskultur	71
6.4. Bruk av felles begrepsapparat med inndeling i dimensjoner	74
6.5. Hvordan kan ledere benytte seg av denne tilnærmingen til sikkerhetskultur?.....	86
7. Konklusjon/oppsummering	90
7.1. Studiens begrensninger og forslag til videre arbeid med tematikken.....	92
Litteraturliste:.....	93

1. Innledning

Sikkerhet i betydningen *Security*, er et fagområde og en bransje i eksplosiv vekst, med nærmere 500 trillioner USD omsetning i året pr 2020. 40 land har flere sikkerhetsvakter enn polititjenestepersonell, og det digitale domenet har åpnet for nye trusler og dermed nye sikkerhetssystemer, -tiltak og -virksomheter (Croll 2023, s. v).

Sikkerhetsprofesjonen har utviklet seg fra bibelske vaktmenn beskrevet i andre Kongebok; 9:17, romerske pretorianergardister, hirdmenn, vektere og politistyrker, til dagens sikkerhetsvakter, analytikere og dataingeniører. Tiltakene har utviklet seg fra vaktposter og steinmurer, til kameraovervåkning, bevegelsessensorer, røntgenscanning og digitale brannmurer. Men det er de samme universelle behovene for faktisk eller opplevd trygghet fra ondsinnede trusler, som Maslow beskrev i sin behovspyramide i 1943, som har ligget til grunn fra våre tidlige stammesamfunn til dagens komplekse samfunn og trusselbilde.

Et relativt nytt aspekt innenfor sikkerhet, som de siste årene har fått stadig større plass blant sikkerhetsakademikere så vel som praktikere og kommersielle aktører, er begrepet sikkerhetskultur. Jeg har gjennom min egen vel tjueårige karriere innenfor faget, merket meg hvordan grupper, avdelinger eller organisasjoner har forskjellig tilnærming til sikkerhet i hverdagen. For noen er det en naturlig del av atferden, for andre er det assosiert med ineffektivitet og heft, og for andre igjen gir det skremmende konnotasjoner til overvåkning og kontroll.

Sikkerhetskultur er et «buzz-ord», med millioner treff på et google-søk på søkeordene «sikkerhetskultur» eller «security culture». I søkefeltet kommer konkurrerende definisjoner sammen med kommersielle tilbud om «6 ways to develop a Security culture in your organization», «Four Ways to Create a Security Culture for Your Workplace» eller «What is needed to create a Security culture?» Særlig den galopperende utviklingen innen teknologi og med den, digitale trusler, har både akademikere og praktikere i stadig større grad sett på den organisasjonskulturelle dimensjonen, for å utvikle og påvirke de ansattes kollektive atferd for å sikre seg mot ondsinnede trusler – eller å tjene penger på kommersielle tilbud tilknyttet sikkerhetskulturell måling og utvikling.

I dette stadig økende landskapet av artikler, bøker, foredrag og kvantitative måleverktøy, er det vanskelig for en leder å manøvrere for å finne ut hvordan man kan bevisstgjøre seg sin sikkerhetskulturelle status og drive kulturelt endrings- og utviklingsarbeid.

For å kunne drøfte tematikken må man forstå begrepets to bestanddeler: Sikkerhet og Kultur. Sikkerhet i forståelsen *Security*, er en tematikk som det er knyttet særlige utfordringer til. Sikkerhetsnivået er vanskelig om ikke umulig å måle, da det er avhengig av en uforutsigbar og usikker faktor; nemlig de menneskestyrte forsettlige truslene man ønsker å sikre seg mot. Sikkerhet kan stort sett bare måles i det som ikke har skjedd, og er således et fagfelt «uten suksesshistorier». Vi lever likevel i en virkelighet der det finnes ondsinnede aktører som ønsker å påføre virksomheter, organisasjoner, stater eller individ, en tilsiktet skade. Trusselaktørene ønsker, og lykkes fra tid til annen, med å skade verdier, i spennet fra liv og helse, fysisk eiendom og økonomi, via teknologisk eller personlig integritet, til omdømme og tillitt.

Organisasjoner i betydningen et sosialt system som er bevisst konstruert for å løse spesielle oppgaver og realisere bestemte mål, vil kunne oppleve trusler mot de verdiene

de har. De vil sikre seg gjennom teknologiske og organisatoriske sikringstiltak, vedta sikkerhetspolicyer og sette opp retningslinjer, regler og planverk. Men under disse ytre synlige artefaktene, ligger kulturelle meningsstrukturer i form av grunnleggende antakelser, samt verdier, holdninger og normer, som er styrende for hvordan vi bruker teknologien, hvordan vi samhandler og hvordan vi vektlegger oppgaver, regler og pålegg. Disse underliggende kulturelle premisene vil påvirke hvordan sikkerheten i praksis vil fungere.

Det kulturelle er en essensiell del av organisasjoners sikkerhet, men samtidig så vanskelig å forstå og forholde seg til, så umulig å enes om definisjonen av og funksjonaliteten til, og så krevende å aktivt styre og påvirke. Men blant en leders oppgaver er både det å sikre organisasjonens verdier og medlemmer, og å drive utviklingsarbeid, mot det å oppnå organisasjonens formål. Hvordan skal en leder kunne kartlegge eller bevisstgjøre seg organisasjonens sikkerhetskultur? Og hvis han klarer å forstå den, hvordan skal han kunne klare å jobbe aktivt med den, for å skape en positiv utvikling i en ønsket retning?

1.1. Oppgavens hensikt

Jeg vil i min oppgave søke å rydde i begrepene innenfor tematikken sikkerhet og sikkerhetskultur, og skape en praktisk anvendbar terminologi og verktøy for ledere å aktivt jobbe med og påvirke egen organisasjonskultur mot mer hensiktsmessige og positive sikkerhetskulturer for den enkelt organisasjon. Dette gjør jeg ved å redegjøre for begrepene *Sikkerhet* og *Kultur*, for deretter å etablere en operasjonell forståelse for hvordan man kan tilnærme seg begrepet sikkerhetskultur. Jeg argumenterer for å tilnærme meg kultur på en fortolkende kvalitativ måte, gjennom «tykke beskrivelser» ned på det grunnleggende antagelsesnivået i kulturen, for å oppnå en tilstrekkelig bevissthet og forståelse for sikkerhetskulturen i en organisasjon. Til dette vil oppgaven presentere sikkerhetskulturelle dimensjoner som kan brukes som et felles begrepsapparat, for kartlegging, bevisstgjøring og forståelse for dette vanskelig tilgjengelige temaet.

Jeg vil deretter se på hvorvidt det er mulig, og hvordan ledere kan arbeide aktivt med å kartlegge, bevisstgjøre seg og utvikle sikkerhetskultur. Jeg vil redegjøre for hvordan dette er et kontinuerlig arbeid gitt kulturens dynamiske karakter, og handler om et målfokus på prosessen og ikke en end-state.

Min overordnede problemstilling i denne masteroppgaven, er:

Hvordan kan man tilnærme seg sikkerhetskultur på en teoretisk og analytisk måte, for å skape «tykke», kvalitative, fortolkende beskrivelser som igjen kan benyttes til endrings- og utviklingsarbeid?

Forskningsspørsmål knyttet til denne problemstillingen vil være:

- Hvordan kan sikkerhetskultur defineres og forstås på en måte som gir verdi for sikkerhetsfaglige praktikere?
- Hvordan kan man gjennom et begrepsapparat og et teoretisk rammeverk bestående av kulturelle dimensjoner, forstå og analysere sikkerhetskulturer?
- Hvordan kan man basert på slike analyser, beskrive sikkerhetskulturer på en kvalitativ, fortolkende måte som kan brukes som utgangspunkt for utviklings- og endringsarbeid?

For å besvare disse spørsmålene har jeg benyttet meg av tilgjengelig forskning, litteratur og ekspertkunnskap, som beskriver oppgavens tre hovedelementer; sikkerhets, kultur og ledelse.

1.2. Struktur

Oppgaven består av fem hoveddeler. Den første delen er denne innledningen. Del to er metodebeskrivelsen. Deretter følger et sikkerhetsfaglig bakgrunnskapittel. Dette inkluderer gjennomgang av sikkerhetsbegrepet, hva dette inkluderer, skillet mellom sikkerhet forstått som *Security* og «trygghet» i betydningen *Safety*, og skal bidra til å belyse sikkerhetsfagets særegenheter og utfordringer.

Den neste delen er en teoripresentasjon. Jeg vil først presentere teori knyttet til kulturbegrepet, og drøfte forskjellige perspektiver og tilnærminger til kultur, med fokus på organisasjons- og sikkerhetskultur. Her vil jeg argumentere for en fortolkende, kvalitativ tilnærming til kultur som delte mentale modeller innen en gruppe.

Deretter vil teorikapittelet presentere relevante sikkerhetsfaglige teorier og hvordan disse aktualiserer de kulturelle sidene ved sikkerhetsarbeidet. Denne delen vil foreslå en modell med dimensjoner som synliggjør sentrale og grunnleggende aspekter ved sikkerhetskultur spesielt. Inkludert i denne delen drøftes også ledelses- og organisasjonsteori som vurderes som relevant for denne oppgaven.

Oppgavens femte hoveddel presenterer empirien fra datainnsamlingen. Her presenteres den informasjonen og de vurderingene og refleksjonene som ble hentet inn gjennom fem dybdeintervju med sikkerhetseksperter.

Oppgavens drøftingsdel funnene fra datainnsamlingen opp mot det teoretiske rammeverket jeg har presentert. Oppgaven knyttes også ledelsesteori og prinsipper, basert på de nevnte dimensjonene i sikkerhetskultur, for å finne lederskapsmessige tilnærminger for å kunne jobbe bevisst og aktivt med organisasjonens sikkerhetskultur.

2. Metode

Kleven (2002) sier at forskning alltid starter med undring og konkrete spørsmål som man deretter forsøker å belyse eller å besvare, ved å formulere konkrete forskningsspørsmål. I denne oppgaven har prosessen vært noe mindre lineær. Tematikken med forskjeller i sikkerhetskultur mellom ulike organisasjoner, avdelinger eller team, har opptatt meg lenge. Først som en profesjonsutøver, men også gjennom utdanningsløpet på dette ledelsesstudiet. Undringen var så absolutt til stede da jeg gikk i gang med dette prosjektet, men utfordringen har vært å formulere konkrete spørsmål som en slik oppgave kan belyse. Kultur er fagområde med mange ulike teorier og som tilnærmes ulikt blant forskere, kommersielle aktører og profesjonelle fagutøvere innen f.eks. ledelsesfaget.

Befring (2007) har utledet noen sentrale stikkord for hva forskning er: Oppdage, beskrive, analysere, dokumentere og forklare. Man kan si at forskningsarbeid er preget både av en kreativ og en systematisk tilnærming. Den kreative delen handler om å utforske problemstillinger og tematikk på en ny og oppklarende måte. I denne oppgaven har det handlet om å finne en ny og operasjonelt anvendbar måte å se på sikkerhetskultur på, med forankring i teoretiske modeller, men med en praktisk og operasjonell bruksverdi for ledere og sikkerhetsfaglige praktikere.

Den systematiske tilnærmingen handler om å presentere kontrollerbare funn, etterprøvbare metoder og troverdige konklusjoner. Et hovedkrav i forskning vil alltid være troverdighet, og for å etablere en høyest mulig grad av troverdighet er det derfor viktig å være bevisst i egne valg av forskningsdesign og metoder. Jeg var derfor innovert flere forskjellige retninger for hvordan jeg skulle teste mine teoretiske modeller slik at de kunne drøftes på en troverdig måte.

Forskningsdesignet jeg valgte, ble ut fra disse utfordringene en todelt metodebruk. Jeg har jobbet inngående med litteratursøk for å undersøke og belyse hva som finnes av relevant forskning og faglitteratur innenfor både sikkerhetsfaget og kulturvitenskap. Dette utledet en teoretisk modell, forankret i de fagtekstene og teoriene som jeg så som mest relevante og som gav mulighet for å utlede en teori med en praktisk anvendelse. Denne teorien skapte nye konkrete forskningsspørsmål på hvorvidt min teoretiske modell var relevant, forståelig, logisk, troverdig og anvendbar for praktisk bruk.

For å teste denne teorien, utførte jeg ekspert- eller eliteintervju, for å få en innsikt i fagfolk sine vurderinger av de tre hovedtemaene i oppgaven; sikkerhetsfaget, sikkerhetskultur og ledelse. Disse intervjuene har som formål å belyse sikkerhetsfaget både teoretisk og praktisk, samt teste min teoretiske modellens relevans og anvendelighet.

Den vitenskapsfilosofiske teorien denne oppgaven hviler på, kan nærmest beskrives ved bruk av begrepet hermeneutikk. Hermeneutikk kommer fra det greske ordet hermeneus, som betyr å tolke eller fortolke (Hjardemaal, 2002). Det sentrale i hermeneutikken er synergien mellom del og helhet; å forstå delene av det man undersøker ut ifra helheten. Men helheten blir bare forståelig for oss gjennom forståelsen av delene. Denne vekselvirkningen blir kalt den hermeneutiske sirkel. Man kan også se på denne prosessen som en hermeneutisk spiral, ved at innsikten i delene og helheten skaper en bedre forståelse for det temaet man studerer for hver omdreining. Forståelsen kan derfor beskrives som en dynamisk prosess.

Denne oppgaven spenner over flere fagområder: Kulturvitenskap, ledelsesteori, sikkerhetsteori og sikkerhetsprofesjonen. Å jobbe seg gjennom faglitteratur på alle disse

områdene har skapt en slik hermeneutisk synergieffekt. Videre har intervjuobjektene praktiske og filosofiske perspektiver, bidratt til å drive denne sirkulære frem mot en helhetlig forståelse av temaet sikkerhetskultur. En leders forståelse og mulige påvirkning på sikkerhetskulturen i egen organisasjon, krever innsikt i hva sikkerhet er, men også hvordan man forstår og velger å tilnærme seg kulturbegrepet, samt hva lederskapsteori sier om hvordan man kan påvirke sine medarbeidere. Bare ved å sette seg inn i disse bestanddelene, vil man kunne se helheten, og delene må undersøkes med helheten som bakteppe.

2.1. Kvalitativ tilnærming

«Å forske kvalitativt innebærer å forstå deltakerens perspektiv» (Postholm, 2010, s. 17). Sikkerhet er et begrep det er vanskelig, om ikke umulig, å måle kvantitativt. Som jeg vil komme tilbake til under den teoretiske drøftingen av sikkerhet, er dette et fagfelt og fenomen, der suksess måles ut fra mangel på hendelser og dermed fravær av eller svært begrenset tilgang på objektive data. Kultur er på same måte ikke en objektivt observerbar størrelse, noe jeg vil synliggjøre i drøfting av en fortolkende tilnærming. Ledelse er på same måte vanskelig å måle i tall og skårer, selv om det finnes eksempler der man har forøkt dette – med diskutabelt resultat.

Opgavens formål er dermed ikke å utlede en naturgitt sannhet, som kan bekreftes ut fra kvalitative data, men å vise gjennom kvalitative analyser, hvordan en leder gjennom bevisst tilnærming og med riktige rammer, kan jobbe kontinuerlig med på å påvirke sikkerhetskulturen i sin organisasjon. Kvalitativ metode gir innside-perspektiv fra, i denne oppgaven, sikkerhetsledere eller utøvere av sikkerhetsfaget. Kvalitative data er ofte hensiktsmessig når man har få respondenter og komplekse variabler. Kvalitativ tilnærming gjør det lettere å gå i dybden og studere komplekse og uklare problemstillinger (Leseth & Tellmann, 2019).

Med disse mer eller mindre abstrakte temaene; sikkerhet og kultur, som bakteppe for forskningsprosjektet, er det vanskelig å se hvordan disse kan måles og veies basert på kvantitative data. Datainnsamlingen ble derfor preget av refleksjoner og diskusjoner, fremfor konkrete svar på lukkede spørsmål. Data blir ikke samlet inn, men skapes gjennom en fortolkende prosess, hevder Aase et al (1997). Det vil si at informasjonen ikke ligger der passivt ventende på å bli hentet ut av forskeren. Data skapes i møtet mellom forsker og det han undersøker. Wormnæs (2012) hevder at vi projiserer vår forståelse ut på den verden vi observerer, og at måten vi forstår noe på har stor betydning for hvordan vi forholder oss til den.

Vi stiller med andre ord, med en forforståelse av det vi møter og det vi ønsker å forske på. Og dette er det særlig viktig å ha med seg i arbeidet som forsker. Forforståelsen kan ha sitt opphav i erfaringer, fordommer eller stereotypier, menneskesyn, vanetenkning og i foregående studiet av emnet. Fuglseth (2007) understreker at all forskning må være selvreflekterende, og det er derfor vesentlig at forskeren er bevisst sin forforståelse og hvilket utgangspunkt man har i det man går inn i forskningen.

Dette er spesielt viktig å være seg bevisst i en kvalitativ studie der man skal aktivt delta som en del av informasjonsinnhenting i et dybdeintervju. Hvordan man presenterer tematikken og prosessen vil prege både intervjuobjektet og hvordan denne svarer. Min egen erfaring og kompetanse innenfor sikkerhetsfaget, gjør dette til en spesielt krevende balansegang mellom å stille relevante og engasjerende spørsmål, og det å ikke prege respondentenes svar ut fra min egen forforståelse.

Kvalitativ forskning har også blitt influert av den postmoderne tilnærmingen til utspørring, som avviser den objektive retningen til vitenskapelig bestrebelse ofte sett i kvantitativ tilnærming. Den kvalitative forskeren nærmer seg sin forskning med utgangspunkt i et verdenssyn. Med det menes at man har en forforståelse eller et sett av antakelser som styrer eller rettleider deres forskning (Postholm, 2010).

Jeg har bakgrunn fra drøye 20 år med praksis innen sikkerhetsfaget, og har selvfølgelig gjort meg opp meninger og en mer eller mindre bevisst forforståelse for det denne oppgaven skal handle om, og det jeg skal intervju mine objekter om. Jeg har måttet, gjennom alt arbeide med oppgaven, fra problemstillingsformuleringen, gjennom teoriutvelgelsen og i intervjuene, jobbet med å skille denne realkompetansen fra den informasjonen som danner datagrunnlaget for oppgavens drøftinger og analyser.

Det er ikke bare en ulempe å ha god og bred forkunnskap. I de fleste tilfeller er dette en forutsetning for å kunne forske, og målet er å videreutvikle eksisterende kunnskap til noe nytt. Men som Wormnæs (2012) hevder, vil dette påvirke både datainnsamlingen og tolkningen av dette. Dette avsnittet er en del av den selvreflekterende prosessen som jeg aktivt har jobbet med, for å skille min erfaring og den praksisen jeg kjenner til fra mitt virke, fra de dataene som skal danne utgangspunktet for analysen i denne oppgaven. God veiledning har også bidratt til denne bevisstgjøringen. Dette resulterte i en veiledende intervjuguide, med fokus på åpne spørsmålsformuleringer i form av rammesetting av tema som respondentene skulle reflektere rundt.

2.2. Kilder

Teorien knyttet til sikkerhetsfaget, er omfattende og mangeartet. Som jeg vil vise senere i oppgaveteksten, handler det både om teoretiske tilnærminger til fenomener og statistikk, men også om en praktisk utøvelse ned på mekanisk nivå. Både etterretningsbaserte trusselvurderinger, og statistisk vektete risiko- og sårbarhetsanalyser, er sammen med etablering og bruk av sikkerhetstiltak som gjerder og låser, en del av sikkerhetsfaget og -arbeidet.

Jeg har i denne oppgaven i stor grad basert den faglige redegjørelsen på veiledere som er produsert av f.eks. Nasjonal Sikkerhetsmyndighet (NSM), Forsvarets Forskningsinstitutt (FFI), DNV-GL m.fl. men også fagartikler basert på forskning eller temarapporter fra offentlige myndigheter som Politiets Sikkerhetstjeneste (PST) og Etterretningstjenesten og store organisasjoner eller konsern som Telenor m.fl.

Det er også hentet informasjon fra andre forskningsoppgaver eller fagartikler, funnet via søk i google scholar eller via linkedin og henvisninger bekjentgjort på seminarer og i undervisning. Jeg har parallelt med denne oppgaven gjennomført kurs i maritim digital sikkerhet, og deltatt på seminar og workshops, der det er henvist til relevant forskning eller publikasjoner. Utvelgelsen av litteratur knyttet til sikkerhetsfaget, er gjort fortløpende gjennom hele skriveprosessen. Litteraturstudiedelen av oppgaven har ikke som ambisjon å metaanalysere all tilgjengelig litteratur, men å bruke relevante og aktuelle kilder for å beskrive det teoretiske bakteppet for drøftingen.

Innenfor kulturfaget, er kildene i stor grad hentet fra pensum fra dette masterprogrammet. Det er i tillegg benyttet kilder som jeg har funnet gjennom de samme prosessene som nevnt over. Gjennom å følge aktuelle fagpersoner på linkedin, og gjennom anbefalinger fra intervjuobjektene i denne oppgaven, har det tilkommet nye og dagsaktuelle kilder til oppgaven.

2.3. Intervju

Hoveddelen av oppgavens datainnsamling og det viktigste grunnlaget for oppgavens drøfting, er de kvalitative ekspertintervjuene jeg har gjennomført. Jeg valgte å gjennomføre semistrukturerte intervju, basert på en temastrukturert intervjuguide. Intervjuobjektene er personer jeg kjenner enten fra å følge med i den faglige offentlige debatten, eller personer jeg har møtt i løpet av egen karriere innen sikkerhetsfaget.

2.3.1. Intervjuguide

For å kunne skape en enhetlig om ikke lik, ramme for intervjuene, ble det satt opp en intervjuguide. Kvale og Brinkmann (2015) omtaler flere ulike former for forskningsintervju. Det som benyttes i denne oppgaven, ligger næres opp til kategorien begreps- eller fenomenintervju. Disse har til formål å kartlegge eller utdype nyanser eller variasjoner av et fenomen. Kvale og Brinkmann definerer et semistrukturert intervju som «en planlagt og fleksibel samtale som har som formål å innhente beskrivelser av intervjupersonens livsverden med henblikk på fortolkning av meningen med de fenomener som blir beskrevet» (2015, s. 325)

Intervjuguiden tar utgangspunkt i oppgavens problemstilling og de formulerte forskningsspørsmålene, og ble utviklet gjennom dialog og rettleiding fra oppgavens veileder. I form er guiden oppsatt som en temastrukturert disposisjon. Det er ikke ulikt en vanlig dialogbasert samtale. Men det profesjonelle intervjuet har det formål å samle inn data, og særegne tilnærminger og teknikker er nødvendig (Kvale & Brinkmann, 2015).

I starten på hvert intervju, ble formen, rammene og formålet med intervjuet presisert. Jeg presenterte meg selv og mitt masterprosjekt med problemstilling. Jeg forklarte at jeg ville presentere et tema, og at etter en fri refleksjon ville jeg trolig følge opp med oppfølgingsspørsmål eller presisere uklarheter, før jeg ville oppsummere slik jeg forstod intervjuobjektets svar. Alle intervju ble innledet med at intervjuobjektet presenterte seg selv, sin stilling, funksjon, relevant utdanning eller annen kompetanse, karriere, erfaring og hva som er den sikkerhetsfaglige arbeidshverdagen for objektet pr i dag.

Den neste fasen var temasetting der jeg introduserte et tema. Jeg bad deretter intervjuobjektet reflektere fritt rundt den aktuelle tematikken. Dersom intervjuobjektet misforstod temaet eller ikke kom inn på viktige momenter i forskningsspørsmålene i oppgaven, hadde jeg undertema eller oppfølgingsspørsmål knyttet til hvert tema. Det ble tatt hensyn til å ivareta det kvalitative intervjuets to dimensjoner: den teoretiske, altså relevansen opp mot oppgavens problemstilling og forskningsspørsmål, og den dynamiske i det å skape en god interaksjon mellom intervjuer og intervjuobjekt (Kvale & Brinkmann, 2015).

Intervjuspørsmål har ofte en deskriptiv form med hovedsakelig hva- og hvordan-spørsmål. Man må være bevisst på at hvorfor-spørsmål kan virke konfronterende, hemme spontaniteten og de fyldige beskrivelsene. Dette kan dreie intervjuet fra å være beskrivende til å bli forklarende og argumenterende (Kvale & Brinkmann, 2015). Gjennom rammesetting av tema og deretter å la intervjuobjektene ta styringen over deres egne svar, ønsket jeg å få frem refleksjoner uten hemmende avgrensinger. Dersom jeg opplevde at objektene gikk utenfor rammene for det jeg tematisk ønsket å snakke om, kunne de forhåndsplanlagte oppfølgingsspørsmålene bidra til å styre intervjuet tilbake på rett spor.

Et eksempel er forskningsspørsmålet: «Hvordan kan man basert på slike analyser, beskrive sikkerhetskulturer på en kvalitativ, fortolkende måte som kan brukes som utgangspunkt for utviklings- og endringsarbeid?» Spørsmålsstillingen rundt dette, er i intervjuguiden temasatt på følgende måte: «Jeg ønsker å avslutte med temaet hvordan en organisasjon kan jobbe aktivt med sin sikkerhetskultur. Jeg vil be deg reflektere rundt dette temaet ut fra din erfaring.» Oppfølgingsspørsmål som jeg hadde forberedt for å utdype svarene for dette temaet: «Er det mulig? Kan en leder skape, utvikle eller påvirke sikkerhetskultur? Hvilken fremgangsmåte kan en leder benytte. Er kulturutvikling ledelsesstyrt eller grasrotprosess?»

2.3.2. Valg av intervjuobjekt

Intervjuobjektene ble relevansvurdert og valgt ut fra de stillingene de fyller pr i dag. Jeg ønsket å ha en blanding av personer fra offentlige etater og fra det private. Jeg ønsket å ha representanter fra forskjellige deler av sikkerhetsfaget. Og jeg ønsket både ledere og operative praktikere innen sikkerhetsarbeid, for å belyse ulike sider ved både sikkerhetsarbeid og sikkerhetsledelse. Dette vurderes å kunne gi oppgaven en viss bredde, selv om antallet respondenter ble avgrenset til fem intervjuobjekter. Andenæs hevder at tilliten til det empiriske materialet ikke bare avhenger av hvor mange personer undersøkelsen omfatter, men også av sammensetningen av intervjugruppen man har til rådighet (Andenæs 2001, s. 296). Sammensetningen øker sjansen for at resultatene vil bli noenlunde lik dersom metoden prøves med andre respondenter, og øker således reliabiliteten i studien. Alle er profesjonelle sikkerhetsekspert, og kan derfor si noe faglig begrunnet, både ut fra real- og formalkompetanse innen fagfeltet. Alle fem har jobbet i mer enn 15 år med sikkerhet, og har hatt ulike roller og oppgaver innenfor sikkerhetsfaget. Dette styrker validiteten til dataene som ble samlet inn; altså i hvilken grad resultatene er gyldige for det utvalget og fenomenet som er undersøkt.

Jeg endte opp med tre intervjuobjekt fra statlige institusjoner: Etterretningstjenesten, Kystverket og Nasjonal Sikkerhetsmyndighet. To objekter var fra privat næringsliv. En drev med kommersiell virksomhet i et forsknings- og konsulentfirma som primært arbeidet med digital sikkerhet og sikkerhetsatferd i det digitale domenet. En arbeidet med personellsikkerhet i Norges Bank, og var således i spennet mellom det offentlige og private. To hadde i tillegg til det sikkerhetsfaglige, lederstillinger med personellansvar. En hadde tittelen fagdirektør og en jobbet i en fri rolle med forskning og utvikling. Flere hadde analyseerfaring og kompetanse, og tre hadde jobbet med beredskap. Av objektene jobbet en spesifikt med personellsikkerhet, og en med digital informasjonssikkerhet, og en hadde lang erfaring med fysiske sikkerhetstiltak. Flere hadde militær bakgrunn, og en hadde jobbet i Politiets Sikkerhetstjeneste (PST). I sum skulle dette utvalget representativt dekke en stor del av sikkerhetsbransjen, og de ulike delene av sikkerhetsfaget som jeg vil komme tilbake til senere i oppgaven. Det var et poeng for meg å ha en bredde i respondentutvalget, for å belyse sikkerhetskulturelle ulikheter, men spesielt likhetene i de grunnleggende forutsetningen for sikkerhetsarbeid.

2.3.3. Gjennomføring av intervju

Intervjuene ble gjennomført både fysisk og digitalt. Tre av intervjuene ble gjennomført ved fysiske møter. De to siste ble tatt over teams, pga. avstander fra min bopel og hvor objektene kunne møtes. Fysiske møter skaper en litt annen ramme, og man kommuniserer lettere gjennom non-verbale signaler når man sitter i same rom, kontra gjennom en skjerm. Tjønndal og Fylling (2021) beskriver utfordringen ved slike intervju, ved at de kan medføre at man ikke oppfatter alle typer kommunikasjon i intervjusituasjonen. Men samtalene som ble gjennomført digitalt, opplevdes å ha samme

innholdsmessige kvalitet som de fysiske. Det er en trend med økende grad av forskningsintervju som blir gjennomført på digitale plattformer, og det er viktig å være oppmerksom på de metodiske mulighetene og fallgruvene ved å benytte slike verktøy.

Intervjuene ble startet ved at jeg gjorde kjent at jeg ønsket å ta opp samtalen med diktafon, forklart med at intervjuene skulle transkriberes og kodes for å ha forskningsmessig verdi. Det var ingen av intervjuobjektene som hadde innsigelser mot dette. Tid til rådighet for gjennomføring av intervjuene ble også avklart innledningsvis. Alle intervjuene var avtalt med en tidsramme på 1-1,5 time. Det første intervjuet tok likevel 1 time og 45 minutter, etter at dette var klarert med intervjuobjektet i forkant. Det ble videre gjort rede for oppgavens hovedproblemstilling og forskningsspørsmålene som var ønsket besvarte.

Intervjuenes form og metodikk vurderes som adekvate for å innhente den tilgjengelige informasjonen, både ved fysiske møter og de som ble gjennomført på digitale plattformer. Å gjennomføre digitale intervju kan gjøre det lettere å rekruttere informanter fordi intervjuet kan gjennomføres i arbeidstiden ut fra en tanke om at man kanskje vil bruke noe kortere tid, og/eller at informantene kunne gjennomføre intervjuet hjemme i egen stue, eller andre steder de måtte ønske. I tillegg ble ikke avstand avgjørende for om intervjuobjektene kunne stille opp. Disse fordelene oppveide de eventuelle kommunikasjonehemmende sidene digital kommunikasjon kan ha (Tjønndal og Fylling, 2021).

Selv om intervjuguiden stod seg gjennom hele datainnsamlingen, må jeg i ettertid erkjenne at formen på intervjuene og fokus endret seg noe gjennom prosessen. Spesielt de sikkerhetskulturelle dimensjonene, opplevde jeg fikk god respons og skapte fyldige og relevante svar fra intervjuobjektene. Dette påvirket meg som intervjuer, både i hvordan jeg rammesatte intervjuet, og hvor mye fokus disse temaene fikk. Gjennom den fenomenologiske og hermeneutiske tilnærmingen jeg hadde, er det en del av metodikken at forskeren stiller seg åpen, slik at vedkommende lar seg berøre av det informantene gir uttrykk for. Dette skaper en utvikling i forforståelsen gjennom hele forskningsprosessen, og kan derfor føre til at intervjuenes fokus og prioriteringer endres gjennom prosjektet (Kvale og Brinkmann, 2015). Forskningens krav om konsistens betyr ifølge Agnes Andenæs, (2001), ikke at intervjuer må oppføre seg helt likt i hvert intervju. «Det er nettopp et poeng at intervjueren kan justere seg etter den enkelte informant, og at intervjuet ikke blir likt hver gang» (Andenæs 2001, s. 29). Andenæs trekker også frem fleksibilitet, i form av å flytte oppmerksomhet dit informanten beveger seg for å klare å utforske informantens perspektiv og forståelse, som et kriterium for kvalitative intervju.

Intervjuenes formål, basert på forskningsspørsmålene, var likevel ensartet gjennom hele datainnsamlingen: Å mest mulig upåvirket få frem ekspertenes synspunkt på begrepet sikkerhetskultur, muligheten til å måle eller kartlegge slike, og en leders mulighet til å påvirke eller styre sikkerhetskulturell utvikling i en organisasjon.

2.4. Transkribering

All transkribering ble foretatt av oppgaveforfatter. Med forholdsvis lange intervjuer ble det en tidkrevende prosess. Intervjuene ble så langt som mulig transkribert ord for ord. Noen tilpassinger der intervjuobjekt reformulerte setninger eller på annen måte avbrøt seg selv, ble ikke skrevet fullstendig ut. Lydopptak og transkriberinger lagres til oppgaven godkjennes, men legges ikke ved denne oppgaven. Oppgaven står på egne ben, men med intervjuene og transkriberingen som fundament.

2.5. Koding og analyse

Analyse av kvalitative data handler om å finne mønster i det som blir sagt. Kodeprosessen handler om å prosessere data ved å merke deler av informasjonen med merkelapper eller koder. Som en hovedregel vil kodegruppene danne utgangspunkt for hva vi vil utvikle som temaer i analysen. Disse mønstrene er i praksis tema som svarer på forskningsspørsmåla. Dette arbeidet strukturerer med andre ord undersøkelsens resultatdel, noe som kan ende opp som kapitler eller delkapitler i en rapport, oppgave eller avhandling eller eventuelt som separate vitenskapelige artikler i et større prosjekt (Tjora, 2021). En analysefase dreier seg om å utvikle kategorier for å skape orden i et uoversiktlig og komplekst empirisk materiale ved å avgrense og kategorisere fenomenene jeg skulle undersøke. Dette resulterte det i et eget kapittel hvor empirien presenteres, som sammen med teorien danner grunnlaget for oppgavens drøftingsdel.

Etter at transkriberingen var avsluttet, ble alle dokumentene gjennomgått og kodet ved hjelp av programvaren Nvivo 20, tilgjengelig fra NTNU sin appfarm. Etter en drøfting med veileder, ble det besluttet å primært benytte en kombinert induktiv-deduktiv tilnærming til kodingen av intervjuetekstene. Induktiv metode var aktuelt gjennom at det var mye av empirien fra intervjuene som skapte nye relevante tema for drøfting; f.eks. sikkerhetsfagets utfordringer, og definisjoner og forståelse av sikkerhetskulturbegrepet. Deduktiv metode var relevant ved å at jeg hadde en teori om sikkerhetskulturelle dimensjoner som jeg ønsket å bruke intervjuobjektens ekspertise, til å teste holdbarheten og riktigheten av. Det at sikkerhetskultur i denne formen, er et relativt nytt fenomen innen profesjonen og academia, er induktiv, eksplorerende tilnærming med formål å skape ny kunnskap, hensiktsmessig. På samme tid eksisterer det mye forhåndskunnskap og teorier rundt det organisasjonskulturelle. De sikkerhetskulturelle dimensjonene, blir da å regne som hypoteser for hvordan man kan tilnærme seg tematikken, og deduktiv design både i spørsmålstilling og koding, gir derfor metodisk mening.

I denne oppgaven dannet forskningstemaene en initiell induktiv kodegruppering i det hermeneutiske samspillet med egen forforståelse og kompetanse. Men i gjennomgangen av transkriberingene ble det opprettet nye undergrupper eller egne hovedkoder til bruk i analysen. Som nevnt fikk de sikkerhetskulturelle dimensjonene, basert på intervjuobjektens respons, en stadig viktigere del i intervjuet, og kodingen av disse delene, kan beskrives som hypotesetestende deduktiv koding. Den fleksible samtaleformen i de semistrukturerte intervjuene, krevde en fleksibel koding og analyse.

Agnes Andenæs beskriver to analysenivåer: Tilstandsbilder og forståelsesmodeller. Tilstandsbilder i Andenæs' terminologi viser til tykke beskrivelser av empiriske fenomen, mens forståelsesmodeller er produkt av brytningen mellom empiri og teori (Andenæs, 2001). Denne oppgaven er en kombinasjon av studier av eksisterende teorier innenfor både sikkerhets- og kulturfaget, og en bearbeiding av empiriske data innenfor dette teoretiske rammeverket. Oppgaven er derfor delt inn i et tydelig skille mellom de teoretiske grunnlaget som problemstillingen og forskningsspørsmålene er dannet innenfor, og hva som er det empiriske grunnlaget innhentet gjennom dybdeintervju. Bearbeidingen og analysen av empirien er det som sammenfattes i empiripresentasjonen og som drøftes opp mot teorien, og danner grunnlaget for oppgavens resultater i form av forståelsesmodeller.

3. Sikkerhet – bakgrunnskapittel

I dette kapitlet ønsker jeg å presentere sikkerhetsfaget, sentrale begrep, alminnelig omforent inndeling og hva dette betyr i praksis. Formålet med denne delen er å gjøre leseren kjent med hvordan sikkerhet er definert og hvordan arbeidet innenfor klassisk sikkerhetstenkning, utøves. Slik vil det kunne refereres til sikkerhetsfaglige begrep og terminologi i oppgavens etterfølgende deler, uten behov for ytterligere forklaringer.

3.1. Begrepsavklaring, definisjoner

Allerede fra starten av dette prosjektet, fremstod det som essensielt å begrepsavklare hva jeg mener når jeg bruker ordet *sikkerhet*. *Sikkerhet* brukes i litterær konkurranse med begrepene *trygghet* og *sikring*, blant flere termer som benyttes om hverandre, både i faglitteraturen, offentlig kommunikasjon og dagligtale. Forvirringen er lettest forklart som skillet mellom de engelske begrepene *Security* og *Safety*. DNV GL har i en rapport fra 2019, «Håndtering av insidersisiko», anerkjent at disse varianter av sikkerhetsbegrepet brukes om hverandre, avhengig av hvilket miljø man er i: «Terminologien knyttet til sikkerhet og sikring er på norsk ikke like entydig som de tilsvarende termene på engelsk – som *Safety* og *Security*» (DNV-GL, 2019).

I Oxford Learner's Dictionary, defineres *Security* som: «the activities involved in protecting a country, building or person against attack or danger», og *Safety* som «the state of being safe and protected from danger or harm» (Oxford Learner's Dictionary, ukjent dato). Det latinske etymologiske opphavet skiller mellom *Security* som den psykologiske tilstanden; uten bekymring, og *Safety* som den fysiske; uskadd (Croll 2023, s. vii).

Piètre-Cambacèdes og Chaudet (2010) drøfter at det også eksisterer en tvetydighet mellom de engelske termene *Safety* og *Security*, og hevder at betydningen av også de engelske begrepene er uklare og overlappende. Piètre-Cambacèdes og Chaudet deler skillelinjene inne to dimensjoner. Den første dreier seg om intensjon; om handlingene er ønskede og tilsiktede. Her knyttes *Security* til intenderte, altså tilsiktede handlinger som har et formål; et ønske om å forårsake skade. *Safety* knyttes til uønskede hendelser som er tilfeldige og ikke tilsiktede. Den andre forskjellen ligger i forholdet mellom systemet og omgivelsene, og hvor risikoen stammer fra. *Security*-trusler kommer fra omgivelsene og har potensialet til å påvirke systemet, mens *Safety*-relaterte hendelser skapes i selve systemet og har potensiale til å påvirke omgivelsene (Piètre-Cambacèdes & Chaudet, 2010).

For å betegne *Security* på norsk benyttes flere begreper. I en NOU fra 2006, definerer Finn-Erik Vinje sikkerhet som *Safety*. Vinjes definisjon er: «Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter». Vinje argumenterer for bruk av ordet sikring for *Security* slik: «Sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging» (NOU2006: 6, s. 38). Den norske giganten Equinor har valgt å bruke begrepet sikring som oversettelse for *Security*, på blant annet sine nettsider og i sine retningslinjer for sikring (Equinor, Retningslinjer for sikring, ukjent dato). På den andre siden brukes ordet *sikkerhet* i i de tre søylene innenfor *Security*-faget; *personellsikkerhet*, *informasjonssikkerhet* og *fysisk sikkerhet*, i det meste av faglitteraturen. Equinor har her igjen endret dette til begrepene personellsikring, informasjonssikring og fysisk sikring.

For å legge til denne usikkerheten, defineres ordet *sikkerhet* i ordbøkene.no, som: trygghet (mot fare, angrep eller lignende), og sikring som: «Det å sikre, bli

sikra eller være sikker, trygg». Når du kommer til flyplassen må du gjennom en sikkerhetskontroll, og når du kalles inn til en sikkerhetssamtale, handler det om dine sårbarheter for å rammes av tilsiktede trusler, ikke om du går med hjelm og vernesko. Tilsvarende brukes også ordet sikring der man gjerne omtaler forhold knyttet til det man på engelske ville kategorisere under begrepet *Safety* – som f.eks. barnesikring, branssikring, stillassikring o.l.

Begrepsvalget i denne oppgaven blir derfor basert på hva forfatteren oppfatter som en naturlig forståelig bruk av fenomenet *Security*, og hvordan det blir oppfattet og forstått i hverdagstale. Det er også preget av hvordan intervjuobjektene omtaler *Security* på norsk. Sist, men ikke minst, baseres det på hvordan oppgavens hovedtema, kulturen som påvirker *Security* i en organisasjon. Uten at det er gjort en uttømmende kartlegging av dette, fremstår det som at *sikkerhetskultur* er den foretrukne benevnelsen i både faglitteratur, offentlige skriv og i publikasjoner på nettet.

Som et av intervjuobjektene i denne oppgaven formulerte det:

«Men jeg kjenner mennesker som gjerne skulle brukt et par år og masse ressurser på å forske på om vi skal bruke ordet sikkerhet eller sikring. Og der er liksom kjørt, fordi vi blander dette ordet i så utrolig mye. Og hvis man tror at sikring er enerådende for å beskrive en Security-relatert ting, så er det ikke det. Se på et sikringsskap, hva er det? Altså vi bruker ordet barnesikring som er Safety, ikke Security. Og så er det den virkelige testen på om dette kommer til å bli endra, og det er om vi noen gang kommer til å endre navnet på Politiets Sikkerhetstjeneste og Nasjonal Sikkerhetsmyndighet. Nei, glem det, gå videre.»

Jeg vil i denne oppgaven bruke ordet *Sikkerhet* i betydningen *Security* – altså vern mot tilsiktede handlinger utført av ondsinnede bevisste trusselaktører.

Det jeg så langt har drøftet, handler om hvilken type trusler som definerer bruken av begrepet. Men hva begrepet skal beskrive er også en del av denne drøftingen. Ordet sikkerhet kan beskrive en tilstand. *Security* har som nevnt rot i de latinske ordene *se*-uten og *cure*-bekymring. Altså uten bekymring, i betydningen fri fra fare, eller utsatt for minimal risiko. Eller man kan bruke ordet *sikkerhet* som betegnelse på en organisasjon eller avdeling som har fagansvaret for sikkerhetsarbeid; «dette må sikkerhet se på» eller «dette er sikkerhet sitt ansvar». Til sist kan begrepet benyttes om en prosess, et arbeid for å kartlegge og redusere risiko. Prosess betyr forløp, utvikling eller naturlig utvikling gjennom flere stadier (Gundersen, 2018).

Jeg vil i det påfølgende kapittelet gjøre rede for sikkerhetsfaget, og de elementene som regnes som en del av det, fra analyser og vurderinger til hendelseshåndtering og med overbyggende styring og ledelse. Denne oppgaven velger å se på sikkerhet som en kontinuerlig aktivitet, et tankesett og en tilstand i stadig utvikling – altså en prosess, med det formål å redusere risikoen for tap eller skade som følge av ondsinnede, tilsiktede uønskede handlinger.

Begrepet sikkerhet vil i denne oppgaven defineres som:

Prosesen, inkludert det teoretisk-analytiske, det praktisk-operative, og det administrative-organisatoriske arbeidet med formål å redusere og håndtere risikoen for uønskede tilsiktede hendelser utført av ondsinnede bevisste trusselaktører.

3.2. Sikkerhetsfagets bestanddeler

Når *sikkerhet* nå er definert for denne oppgaven, ønsker jeg å gå gjennom det som innenfor gjeldende praksis og faglitteratur, regnes som denne prosessen hoveddeler. Det er ikke oppgavens formål å redegjøre for alle ulike varianter og praksiser for hvordan dette skjer ute i alle typer virksomheter og organisasjoner. Dette er en redegjørelse for de allment aksepterte og praktiserte grunnprinsippene for hvordan man teoretisk kan dele inn sikkerhetsprosessen bestanddeler. Formålet er å gi leseren en grunnleggende forståelse av prinsipper og begreper, som det vil bli referert til senere i oppgaven.

3.2.1. Risikovurdering/-analyse

I min definisjon av sikkerhet, brukes begrepet risiko. Det er heller ikke for dette begrepet en universell etablert definisjon. Norsk Standard 5814:2008 definerer risiko som et «uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse».

«En risikovurdering er nødvendig for å kunne identifisere behovet for fysiske sikkerhetstiltak som bør implementeres for å redusere risiko og oppnå tilstrekkelig sikkerhet for virksomheten (...) Det er basert på dette arbeidet man utarbeider en plan for utforming av sikkerhetssystemet» (NSM, 2020b, del 1.4).

En annen tilnærmingen er basert på NS 5832:2014 der risiko er omtalt som «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen». Vurdering av sannsynlighet for ulike sikkerhetsscenario er i denne tilnærmingen med hensikt utelatt. I stedet fokuserer denne tilnærmingen på å redusere sårbarheter som igjen reduserer den samlede risikoen. Denne tilnærmingen kalles trefaktormodellen (også kalt «risikotrekanten») hvor verdi, trusler og sårbarheter er faktorene.



Figur 1: Risikotrekanten (DNV-GL, 2019, s. 7).

Risikotrekanten beskriver hvordan man ser for seg sammenhengen mellom de verdiene en aktør innehar som er truet, sårbarhetene som kan utnyttes av en trusselaktør, og trusselen denne motparten representerer. Modellen illustrerer hvordan man kan redusere risiko ved å påvirke den delen av trekanten man kan. Man kan redusere verdien av det har, f.eks. ved å ikke inngå sensitive kontrakter som noen er ute etter. Eller man kan redusere sårbarhetene sine, ved å etablere sikkerhetstiltak innenfor f.eks. adgangskontroll eller IKT-sikkerhet. Man kan også redusere kapasiteten til trusselaktøren, ved å nekte personer å besøke anlegg eller få innsyn i den informasjonen de er ute etter.

Først fordrer det at man vet hvilke verdier som må beskyttes, og at det utarbeides en verddivurdering. Verdi defineres som en ressurs som, hvis den blir utsatt for en uønsket

påvirkning, vil medføre en negativ konsekvens for den som forvalter eller drar fordel av ressursen (NSM, 2014). F.eks. hvilken informasjon organisasjonen besitter som er skjermingsverdi? Hvilken teknologi utvikler bedriften som er verdifull for motparten å få tak i? Verdier kan også være virksomhetens omdømme, nettverksinfrastruktur, spesielle installasjoner, utstyr eller deler som er kritisk for produksjonen. Verdier er alt som har betydning for virksomheten, og som dersom de blir skadet, stjålet, misbrukt eller kompromittert, kan skade virksomheten. NSM skiller mellom primærverdier, som er forretningsprosesser og informasjon, og støtteverdier er de verdier som muliggjør og er avgjørende for primærverdiene, som maskinvare, fysisk infrastruktur og utstyr, lokaler, strøm- og vannforsyning osv. (NSM, Risikovurdering av IKT-systemer). En verdivurdering kartlegger og identifiserer verdiene, og kategoriserer disse ut fra hvor kritisk tap eller bortfall av disse vil være.

Derneft må man være bevisst egne sårbarheter og hvordan disse kan utnyttes. Sårbarheter er forhold som en trusselaktør kan utnytte til å påvirke virksomhetens verdier. Sårbarheter kan være kjente eller latente. Det kan være feil eller mangler i design, prosedyrer, vedlikehold, trening, opplæring og kommunikasjon (NSM, 2020a). Sårbarhetsvurderingen baserer seg på de eksisterende sikkerhetstiltakene, og hvilke mangler eller «hull i barrierene» man klarer å identifisere.

Det siste hjørnet i sikkerhetstrekanten, er truslene. Med en trussel forstås ethvert forhold eller enhver enhet med et potensial til å forårsake en uønsket hendelse (NOU 2000:24). Et trusselbilde er en tidsavgrenset beskrivelse av identifiserte trusler mot en bestemt entitet. En trusselaktør kan være eksterne enkeltpersoner eller grupper, eller en insider, dvs. en som arbeider i virksomheten og som har lovlig adgang til områder og tilgang til systemer. Når man vurderer trusselaktøren vurderer man gjerne vedkommende sine kapasiteter og intensjoner. Analyser av intensjon og kapasitet er vesentlige for å vurdere hvor stor risiko trusselaktør representerer.

Basert på disse vurderingene av de tre hjørnene i trekanten, kan man deretter analysere seg frem til et risikonivå. Dette er ikke en matematisk formel, og det finnes som tidligere nevnt, flere metoder for å beregne og benevne risikonivået.

Aarset (2017) beskriver denne prosessens formål som å beskrive en virksomhet, å identifisere de risikoer som er knyttet til denne virksomheten, å vurdere hvor alvorlig disse risikoene er, og til slutt beslutte hva som så skal gjøres. Skal vi godta den risiko som er knyttet til virksomheten, skal vi forsøke å redusere denne risikoen, eller skal vi rett og slett la være å gjennomføre det vi hadde satt oss fore? Aarset forklarer at det å være bevisst på at noe kan gå galt, ikke betyr at vi nødvendigvis skal forsøke å unngå all risiko. All virksomhet er forbundet med risiko, og risikovillighet vil spille inn som en faktor for hva en organisasjon kan og vil akseptere.

Dette vil videre føre til risikobehandling, der man identifiserer hva som kan gjøres for å redusere de identifiserte risikoer.

3.2.2. Tiltak/sikkerhetsfagets tredeling

Sikkerhetsfaget er tradisjonelt delt inn i tre hoveddeler, som en teoretisk modell for å skille risikotyper og tiltak fra hverandre på en hensiktsmessig og oversiktlig måte. Det finnes også andre inndelinger i faglitteraturen. Spesielt når det gjelder tiltak er det også vanlig å skille mellom teknologiske, organisatoriske eller menneskelige tiltak.

Jeg vil redegjøre for både risikotyper, tiltak og styring under de tre nevnte «grunnpilarene» fysisk sikkerhet, personellsikkerhet og informasjonssikkerhet. Jeg vil i det følgende presentere hva som inngår i disse tre fagområdene både ut fra hvilken type risiko det er snakk om, men også hvilke tiltak eller barrierer som organiseres under disse områdene. Sikkerhetstiltak etableres som balansert sikring i form av barrierer, deteksjon, verifikasjon og reaksjon. Sikringen må etableres slik at det tar lenger tid å gjennomføre en uønsket hendelse (eks. innbruddstid) enn det tar å håndtere den. Dette betegnes "positivt tidsregnskap" (NSM, 2020a, del 2.1).

3.2.2.1. *Fysisk sikkerhet*

NSM beskriver fysisk sikkerhet som grunnleggende sikkerhetstiltak for å hindre uvedkommende fysisk tilgang til skjermingsverdig informasjon og aktivitet. Den fysiske sikkerheten er de konkrete, håndfaste sikringstiltakene som skal sikre og skjerme verdier fra trusselaktører. Dette inkluderer fysiske barrierer, gjerder, porter, dører, fysisk soneinndeling m.fl. som kan hindre eller forsinke adgang til verdier. Videre er det de elektroniske sikkerhetstiltakene; elektroteknisk utstyr og løsninger for å støtte, supplere eller erstatte fysiske sikkerhetstiltak. Elektroniske barrierer kan være etablering av elektronisk adgangskontroll og TV og videoovervåking (TVO) (NSM, 2020b).

Man inkluderer i tillegg de menneskelige sikkerhetstiltakene som påvirker vurderingsevne, kunnskap, adferd og reell evne til å bruke det fysiske sikkerhetssystemet; inkludert fysisk vakthold og adgangskontroll - altså vaktmannskaper som styrer adgangen og kontrollerer de fysiske sikringstiltakene.

Organisatoriske barrierer er tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, adferd og/ eller anvendelser av blant annet de fysiske sikkerhetstiltakene.

Organisatoriske sikkerhetstiltak som en del av den fysiske sikringen kan eksemplifiseres som skilting, opplæring i bruken av adgangskontrollsystemet, og bruk av adgangskort.

Med andre ord handler det om de tradisjonelle sikkerhetstiltakene som fysisk gjør det vanskeligere, eller aller helst umulig, for trusselaktører å ramme eller skade de verdiene man ønsker å beskytte, ved å begrense adgangen til disse. I tillegg vil slike tiltak vil også ha en proaktiv effekt ved at trusselaktøren unnlater å forsøke fordi han vurderer at tiltakene vil redusere sjansen for å lykkes. I alle fall så lenge angriperen er rasjonell, så vil han velge ut de mål hvor han tror han vil lykkes, og velge bort de målene hvor dette fremstår som umulig. I sin rapport om målutvelgelse for politisk motiverte trusselaktører, skriver PST:

«Sikringstiltak som reduserer muligheten for å gjennomføre et vellykket terrorangrep vil gjøre et objekt mindre attraktivt å angripe. Både faktiske og antatte sikringstiltak har betydning for hvor attraktivt et objekt fremstår. Synlige sikringstiltak vil i mange tilfeller virke avskrekkende på en trusselaktør. Sikringstiltak som gjør at objektet blir vanskelig å komme til rent fysisk, f.eks. sperringer, adgangskontroll eller vakthold, vil gjøre objektet mindre attraktivt» (PST, 2020, s.4).

3.2.2.2. *Personellsikkerhet*

Fysisk sikkerhet hindrer uvedkommende å få adgang til verdiene. Men hva dersom trusselen kommer innenfra, fra egne rekker, fra personer som er gitt adgang gjennom sitt arbeidsforhold eller medlemskap i en organisasjon? Forskrift om personellsikkerhet definerer personellsikkerhet som tiltak, handlinger og vurderinger som utøves for å

hindre at personer som kan utgjøre en sikkerhetsrisiko, plasseres i stillinger der de kan ramme verdier (Personellsikkerhetsforskriften, 2001, § 1-2). Forskriften og fagmyndigheten NSM, fokuserer på skjermingsverdig informasjon og verdier som faller innenfor sikkerhetsloven. Men personellsikkerhet kan like gjerne gjelde kommersielle bedrifter, frivillige organisasjoner og alle andre organisasjoner. 8 prosent av virksomhetene svarte i Kriminalitets og sikkerhetsundersøkelse i 2019, at de har avdekket utro tjenere blant egne ansatte i løpet av de siste 2 årene (Næringslivets sikkerhetsråd, 2019).

Personellsikkerhet skiller mellom de som aktivt går inn for å skade egen virksomhet - innsidere, og de som uforvarende eksponerer sårbarheter eller begår handlinger som kan utnyttes av en trusselaktør. NSM definerer innsidere som:

«En insider forstås som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap» (NSM, 2020c, s. 9).

Innsideaktivitet kan gjennomføres direkte og på egenhånd, eller på vegne av en ekstern aktør. Eksterne aktører kan være statlige, ikke-statlig eller andre enkeltindivider (NSM, 2020c, s. 9). Politiets sikkerhetstjeneste (PST, 2020, s. 10) definerer en insider «som en person som utnytter, eller har intensjon om å utnytte, sin legitime tilgang til en virksomhets verdier til uautoriserte formål». Martin (2019, s. 98) definerer en insider som «en person som utnytter, eller har til hensikt å utnytte, sin autoriserte tilgang på uautoriserte formål».

Pr 2023 gir den spente sikkerhetspolitiske situasjonen i verden, rom for omfattende etterretningsvirksomhet. PST vurderer at personer i Norge vil bli forsøkt rekruttert som kilder av andre lands etterretningstjenester (PST, 2023). Økokrim beskriver i tillegg i sin trusselvurdering for 2022, at det er avdekket flere eksempler på profesjonelle aktører som bistår kriminelle med en lang rekke tjenester og utnytter sin rolle for egen eller andres vinning, at flere kriminelle nettverk har tilgang til profesjonelle aktører og utro tjenere, samt at det er meget sannsynlig at enkelte profesjonelle aktører bevisst og aktivt tilrettelegger for kriminalitet» (Økokrim, 2022, s. 64).

Innsideren kjenner virksomhetens rutiner, prosesser og sårbarheter, og kan benytte kunnskapen for å skade virksomheten. Personer med administrasjonsrettigheter i informasjonssystemer eller personer som i kraft av sin stilling har tilgang til en stor andel av virksomhetens verdier, kan sies å ha stor kapasitet. Ikke-statlige aktører som kriminelle nettverk, kan forsøke å rekruttere innsidere eller plassere enkeltindivider på innsiden av en virksomhet for å oppnå egne mål, og vil kunne ha høy kapasitet (NSM 2020b).

Personellsikkerhet er i akademia og ute i virksomheter og organisasjoner, viet lite oppmerksomhet, sammenlignet med informasjons- og fysisk sikkerhet, og omtales derfor som «sikkerhetens Askepott» (Martin, 2019, s. 203). Risikoen for at noen på innsiden av en organisasjon skal ramme dens verdier, er både statisk og dynamisk. Statisk fordi organisasjoner inneholder mennesker, og mennesker med sine sårbarheter og motivasjoner, vil alltid representere en risiko. Dynamisk fordi disse sårbarhetene, motivasjonene, og lojalitet vil endres gjennom menneskers livsløp, slik trusselaktører kan endre sine mål og angrepsmetoder (NSM, 2020b, s. 9-10).

Det kan være flere grunner til at en person begår innsidevirksomhet. Vedkommende kan være motivert av egne interesser eller bli påvirket av en ekstern aktør som forleder, presser, kultiverer eller overtaler en person til å begå innsidevirksomhet. Intensjon om å begå innsidevirksomhet kan også vokse frem som et resultat av personens egne motivasjoner og overbevisninger, uten påvirkning av en ekstern aktør. Det forekommer også tilfeller hvor innsideraktivitet begås uten av personen har en klar motivasjon om å gjennomføre dette, men hvor vedkommende gjennom sin adferd utsetter virksomhetens verdier for risiko (NSM, 2020c, s. 9).

NSM beskriver hvordan negative forhold på arbeidsplassen kan føre til selvmotivert innsidevirksomhet i ved at personen beslutter å hevne seg eller skade virksomheten fordi personen opplever å bli behandlet urettferdig, eller ikke føler at kollegaer og ledere verdsetter, forstår eller ser arbeidstakeren på en tilstrekkelig måte (NSM, 2020c, s. 24-25).

Som nevnt er ikke ansatte nødvendigvis illojale eller bevisste sine handlinger som fører til at verdiene eksponeres. Mangel på kompetanse, forståelse eller sikkerhetsbevissthet, kan medføre at et medlem i en organisasjon, uforvarende eksponerer sårbarheter i sikringsystemet, eller ved uhell eller som følge av manipulasjon åpner tilganger for eksterne trusselaktører (NSM, 2020c, s. 11-12). DNV-GL definerer dette på følgende måte:

«Uforvarende innsider er en som uten å forstå eller ville det, gjennomfører en handling som resulterer i økt sårbarhet, skade eller tap for virksomheten. Vedkommende kan ha blitt manipulert eller forledet eller vedkommende har ikke kompetanse til å forstå konsekvensene av handlingen sin. Eventuelt kan vedkommende være i en sinnstilstand der uoppmerksomhet eller sløvheter medfører at handlingen blir utført uten at dette er tilsiktet» (DNV-GL, 2019, s. 10-11).

3.2.2.3. Informasjonssikkerhet

Den tredje søylen innenfor sikkerhetsfaget, er tradisjonelt omtalt som informasjonssikkerhet. Dette området blir ofte brukt sammen med, som synonym til eller i konkurranse med betegnelser som IKT- cyber- eller digital sikkerhet. Informasjonssikkerhet handler om å beskytte informasjon som av personvern hensyn er sensitive, som gir virksomheter et konkurransefortrinn eller som skjermingsverdig er av nasjonale hensyn.

NSM oppsummerer risikobildet på følgende måte for 2023: «Den hurtige teknologiske utviklingen og digitaliseringen av samfunnet byr på både muligheter og utfordringer. Trusselaktører benytter seg av stadig flere virkemidler for å oppnå sine mål samtidig som våre sårbarheter blir mer komplekse». NSM beskriver videre at vi i Norge fra 2019 til 2021 har hatt en tredobling i alvorlige cyberoperasjoner mot norske myndigheter og virksomheter (NSM, 2023, s. 11 og 18).

Informasjonssikkerhet handler om mer enn passord og brannmurer. Fokuset tidligere var på verdien som informasjonen representerte, heller enn containerne og kommunikasjonslinjene. Så har det i senere år vært et økende fokus på den digitale infrastrukturen. Selv om vi lagrer mesteparten av, men ikke all informasjonen vår, på datamaskiner og kommuniserer via nettverk, så hevder Kessler og Shepard i sin bok *Maritime Cyber Security*, at vi må fokusere mer på innholdet en bare måten vi lagrer og transporterer denne informasjon på. Det er informasjonen som er verdien, det vi ønsker

å beskytte. Informasjonen må beskyttes mot angrep som kan ramme dens integritet, konfidensialitet og tilgjengelighet (2022, s. 31-32).

Ved at informasjonen blir kjent for aktører man ikke vil skal ha denne. Altså informasjonens konfidensialitet – i betydningen behovet for å skjermes den. Det kan være informasjon som synliggjør sårbarheter som fører til at organisasjonen kan rammes på andre måter. Det kan være informasjon som gir et konkurransefortrinn, f.eks. teknologisk. Eller det kan være informasjon som skader medlemmer, kunder eller andre sin personlige integritet, eller organisasjonens omdømme. Når pasientopplysninger kom på avveie fra Helse Sør-Øst, er dette et eksempel på dette. I mai 2022 ble det kjent at informasjon fra Norges offisielle eiendomsregister hos karttjenesten Norkart var kompromittert av en ukjent trusselaktør. Dette inkluderte persondata om 3,3 millioner nordmenn hvor navn, adresser, fødselsnummer og informasjon om hva man eier. «Dersom denne type datasett blir satt i sammenheng med annen tilgjengelig informasjon er det særlig bekymringsfullt» (NSM, 2023, s. 18).

Dernest kan en angriper ramme informasjonens integritet, altså endre informasjonen slik at den ikke fungerer slik den var tenkt. Det var dette norske myndigheter var bekymret for under kommune- og sametingsvalget i 2021. Stemmedelingen var informasjon som hvis den ble manipulert kunne ramme selve det norske demokratiets integritet, slik tilfellet var under det amerikanske presidentvalget i 2016.

Til slutt handler det om å beskytte informasjonens tilgjengelighet. Den eksplosive veksten i datanektangrep eller løsepengevirus, der en angriper overstrømmer en server eller krypterer informasjon, slik at organisasjonen som eier og trenger den, ikke kan bruke den, er eksempler på at trusselaktøren rammer informasjonens tilgjengelighet. Hydro ble utsatt for et avansert tjenestenektangrep i mars 2019, som endte med å koste dem 800 millioner kroner (Stolt-Nielsen & Lysberg, 2021).

3.2.3. Beredskap

«You can't plan for the unexpected, and in many cases, planning actually sets you up to respond incorrectly» (Weick og Sutcliffe, 2007, s. 2).

Når tiltakene ikke lykkes med å stanse trusselaktøren, når det proaktive sikkerhetssystemet feiler, når det dukker opp en trussel som man ikke har forutsett og iverksatt tiltak for å stoppe, er håndteringen av uønskede hendelser avhengig av hvorvidt og hvordan organisasjonen er forberedt på å møte slike kritiske situasjoner. I denne oppgaven brukes beredskap i betydningen de systemer og ressurser som står klare til å takle ondsinnede, forsettlige sikkerhetshendelser. NSM forklarer beredskap på følgende måte:

«Tiltak for påbygging, gjenoppbygging og skadebegrensning skal forberedes som beredskap i tilfelle risikoen for sikkerhetstruende virksomhet øker i forhold til normaltilstanden. Som for grunnsikringstiltakene skal beredskapstiltakene skal etableres som tiltak og prosedyrer i sammenheng» (NSM, Veileder i sikkerhetsstyring, s. 21).

Som Aarset (2017) beskriver det må vi være bevisst på at noe kan gå galt for å kunne oppdage signalene om en vordende krise tidsnok. Først da kan man med de riktige tiltak enten klare å forhindre at den inntreffer, eller redusere konsekvensene av dersom krisen likevel skulle inntreffe. God beredskap bygger på gjennomføring av risikoanalyser som gir en oversikt over aktuelle trusler man står ovenfor. Disse tar gjerne utgangspunkt i både trusler og farer i et historisk perspektiv og mulige fremtidige trusler (Perry &

Lindell, 2003). Videre må god beredskap være bygget opp av ulike aktiviteter på både organisatorisk og operativt nivå inkluderes, herunder risikoanalyser, beredskapsanalyser, utarbeidelse av beredskapsplaner, men også trening og øvelser er sentrale momenter (Engen et al., 2016).

Beredskap brukes gjerne i dagligtale, om de statlige ressursene som en stat, et samfunn eller borgerne stoler på skal komme til unnsetning i en krisesituasjon, som Forsvaret, politiet eller brannvesenet. Men i utvidet forstand kan og bør alle organisasjoner, virksomheter eller grupper ha en beredskap for å håndtere det som kan ramme dem.

Det er denne tidligere beskrevne restrisikoen man må ha et system for å takle, og som skal forstås som beredskap. Beredskap kan være nødprosedyrer, fysisk utstyr, endret organisering og økte personellressurser, som brukes for å håndtere den uønskede hendelsen, og bringe organisasjonen tilbake til normalsituasjonen igjen.

Beredskapsarbeidet bygger på fire hovedprinsipper (Justis og beredskapsdepartementet, 2022):

«Ansvarsprinsippet: Den organisasjon som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området. Ansvarlig instans må ta stilling til hva som er akseptabel risiko.

Likhetsprinsippet: Den organisasjon man opererer med under kriser, skal i utgangspunktet være mest mulig lik den organisasjon man har til daglig.

Nærhetsprinsippet: Kriser skal organisatorisk håndteres på lavest mulig nivå.

Samvirkeprinsippet: Myndigheter, virksomheter og etater har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.»

Et fokusområde for en beredskapsledelse, utover den operative håndteringen, er psykososial støtte. Dette omhandler å ta vare på menneskene som er rammet eller involvert. HR er ansvarlig for å ivareta den psykososiale støtten, inkludert å sørge for at de ansatte og pårørende får den informasjonen de trenger og er lovet, samtidig som de blir holdt oppdatert om utviklingen til situasjonen. Kommunikasjon håndteres i hovedsak av den strategiske kriseledelsen, med mindre det gjelder intern kommunikasjon. Intern kommunikasjon kan håndteres av HR.

3.2.4. Risikostyring/sikkerhetsledelse

«Executive teams and boards of directors need to view Security culture as a critical priority,» (Roer og Carpenter, 2022, s. 22).

I de foregående avsnittene, har jeg presentert sikkerhet som en prosess som inkluderer risikovurdering, sikkerhetsfagets tre hoveddeler og tiltak, samt beredskap for å håndtere sikkerhetshendelser. Sikkerhetsarbeid er et system som påvirker arbeidshverdagen, drift og produksjon. Jo mer kompleks og jo større en organisasjon er, jo mer krever dette av ledelse og styring. Det finnes i faglitteraturen flere benevnelser på dette arbeidet. I denne oppgaven fokuseres det på begrepene risikostyring og sikkerhetsledelse.

Aarset (2017) beskriver risikostyring (Risk management) som at organisasjoner må vite hva man vil, og hva som kan gå galt, slik at man med åpne øyne kan vurdere om vi

virkelig ønsker å gjennomføre sine planer. Eller om vi bør gjøre noe proaktivt for å redusere risikoen. NSM har en mer formålsfokustert definisjon:

«Formålet med risikostyring er å sikre at virksomheten når sine mål og retter fokus mot de aktiviteter som er mest kritisk for å nå målene,» (NSM, Risikovurdering av IKT-systemer, s. 4).

Gjennom en slik bevisstgjøring av hvilken risiko man står ovenfor, og en prosess der man vurderer hvilken risiko man er villig til å ta, operasjonaliserer dette gjennom å sette inn tiltak og deretter styre prosessen videre. Som beskrevet tidligere er risiko en dynamisk faktor i konstant endring, så både fundamentet i risikovurderingen og tiltakenes omfang og effekt, må kontinuerlig adresseres, vurderes og styres. Aarset (2017) definerer styringsdelen som «ledelse»; et samlebegrep for gjennomføring av kost-nytte vurderinger av foreslått tiltak, beslutningstaking og gjennomføring av disse og oppdatering av planverk.

Hvordan man vil beskytte disse verdiene, og hvilke konsekvenser, positive og negative, tiltakene medfører, må altså være ledelsesstyrt. Risikoaksept innebærer at organisasjonen har et avklart og bevisst forhold til hvilken balanse det skal være mellom sikkerhet og produksjon, mellom tiltakene og hvordan de påvirker drift og måloppnåelse. Dette er tillagt det nivået som eier risikoen gjennom ansvarsprinsippet, som krever at den enkelte organisasjon har ansvaret for beredskapsforberedelser og håndtering i tillegg til å vurdere risiko (Justis- og Beredskapsdepartementet, 2022).

Når det er besluttet hvilken risiko som er akseptert og hvilket system av sikkerhetstiltak som skal garantere dette risikonivået, og hvilken beredskap som skal håndtere det som likevel skjer av sikkerhetshendelser, må dette systemet operasjonaliseres og følges opp. Sikkerhetsledelse er i utgangspunktet det samme som annen ledelse og det følger de samme prinsipper.

4. Teori

“Whenever I hear the word culture... I reach for my gun”. Sitatet har feilaktig blitt attribuert både Henry Ford så vel som Hermann Göring som Heinrich Himmler, men er originalt fra et teaterstykke skrevet av forfatteren Hanns Johst. Selv om Johst faller inn i same uheldige politiske kategori som Göring og Himmler, kan uttrykket likevel forstås som en metafor for den frustrasjonen både akademikere og praktikere føler når man skal forstå og bruke kultur som begrep (Cox & Flin, 1998). Fra tid til annen blir kulturbegrepet drøftet og problematisert; hva det skal inkludere og hvordan det skal forstås. Kroeber og Kluckhohn fant i 1952 hele 164 ulike definisjoner bare innenfor antropologi, og definisjoner av kultur varierer med fagfelt, disiplin og retning innenfor disiplinene (Kroeber og Kluckhohn, 1952).

Antropologer, sosialpsykologer, samfunnsvitere, historikere, akademikere og praktikere er ikke enige om en definisjon, men likevel deler de en konseptualisering av kulturer; som et flettverk av trekk, integrerte konfigurasjoner, konstallasjoner av symboler og mening, symbolske sjablonger, nettverk av mening, målbare atferdsmønstre, materielle artefakter, verdier og antagelser, strategier for å oppnå bevisste eller ubevisste mål, og et felt der språk og diskurser utvikles og spilles ut.

Kulturbegrepet er noe vi alle har en forståelse av, en oppfatning av, eller en ide om; som en størrelse, dimensjon eller kraft i våre liv, samfunn og organisasjoner. Kultur er noe som «skaper», eller konstituerer verden rundt oss. Kultur angir retning og preferanser, og motiverer visse handlinger og tanker. Den er med på å fastsette verdier - definerer godt og ondt, bra og dårlig. Og kulturelementet er med på å både skape kollektiver, enhet og fellesskap, og samtidig trekke opp grenser og definere forskjeller mellom oss. I en artikkel av Rune Glomseth (2019), gir Ola Lystad sin beskrivelse, om ikke definisjon av kultur:

«Kultur er bærer av mening. Kultur handler om den fortellingen som organisasjonens medlemmer er en del av og deler. Det er de verdier, meninger og ritualer som preger organisasjonen og understøtter fortellingen om hvem «vi» er, hva som holder «oss» sammen, hvordan dette skjer, og hvorfor vi er til.»

4.1. Essensialistisk og fortolkende tilnærming

Et sentralt skille i hvordan man forholder seg til kulturbegrepet, er hvorvidt man ser på kultur som noe man har, eller kultur som verktøy og erfaringsramme for å forstå. De essensialistiske kulturteoretikerne er ute etter å «fange» kulturen ved å identifisere «mønstre» eller «essensen» som kan beskrive forskjeller og likheter, knyttet til behovet å beskrive og forklare atferd. Dersom man ser en person oppføre seg annleis enn det man selv føler er normalt, trenger man en forklaringsmodell for hvorfor det er slik. Kultur blir derfor en slik forklaring, og fokuset blir på «kontraster heller enn nyanser» (Askehave 2006, s. 10). Kulturen blir oppfattet som noe konkret – en stabil, varig størrelse som er med å prege hvordan du tenker og handler. Dermed kan en positivistisk analysert kunnskap om kulturen, bidra til å predikere atferden til medlemmene i en kultur. Cameron og Quinn (2015) omtaler dette som den sosiologiske tilnærmingen til kultur; at organisasjoner *har* kultur.

Buchanan og Huczynski betegner dette perspektivet som kultur sett på som en variabel. Dette perspektivet fokuserer på konsensus og enhet i en organisasjon, om hva kulturen i organisasjonen er, og en beskrivelse av hvordan forskjellige elementer i en organisasjon virker sammen og støtter hverandre (1997, s. 514). Kultur blir da noe stabilt og konkret,

basert på delte verdier og meninger, forankret i historier og symboler og som kan overføres til nye medlemmer. Dette perspektivet ser videre på organisasjonskulturen som noe som bevisst kan skapes og styres av ledere for å oppnå organisasjonens målsettinger.

Motsatsen er det Cameron og Quinn kaller den antropologiske; at organisasjoner er kultur (2015, s. 18). Buchanan og Huczynski kaller motstykket «kultur som metafor» (1997, s. 515). Da ser man på kultur som et system av delt kognisjon, av kunnskap, antagelser, mening og symboler, som er både produsert og reprodusert gjennom forhandling og deling av disse symbolene og meningssytsemne. Dette perspektivet representerer en «bottom – up» tilnærming (Glendon & Stanton, 2000). Dette betyr at organisasjonskulturen ikke «eies» av en bestemt gruppe, men skapes og gjenskapes gjennom interaksjonene mellom medlemmene i organisasjonen (Richter & Koch, 2004). Dette synet har fokus på mening og hva som ligger til grunn for danning av mening. Holliday argumenterer for at et fortolkende perspektiv setter til side de enkle svarene, og tvinger oss til å se under det overflatiske og komme til bedre funderte konklusjoner (2019, s. 17).

Kultur som noe en organisasjon «har» eller som «variabel» vil i det videre betegnes som det essensialistiske perspektivet. Kultur som noe organisasjoner «er» eller som «metafor», benevnes som det fortolkende perspektivet.

Glomseth (2019) beskriver forenklet skillet med at der det essensialistiske «har»-perspektivet betrakter kultur som en av flere puslespillbiter, vil kultur i «er»-perspektivet, betraktes som selve puslespillet.

4.2. Kultur som delte mentale modeller

På 1970-tallet begynte Daniel Kahneman og Amos Tversky å formulere en teori om hvordan mennesker fatter sine beslutninger. Disse er presentert i verket Tenke, fort og langsomt (2013). Kahneman forklarer menneskelige beslutningsprosesser med to system for kognisjon. System 1 består av mentale modeller, innlærte heuristikker, som konstant tolker og filtrerer sensorisk input, og automatisk medfører atferd. Menneskesinnet må fatte rundt 35 000 beslutninger gjennom et døgn, er basert på effektivitet og ikke nøyaktighet. Derfor kan disse mentale modellene løse oss gjennom hverdagen på «autopilot». System 1 er både tids- og energieffektivt, og står for 95 prosent av de beslutningene vi tar hver dag. Vi har også evnen til å «tenke sakte» ved bruk av System 2. Her bruker hjernen rasjonell, logisk tenkning som inkluderer all tilgjengelig informasjon. Men System 2 er energikrevende, og hjernen vår er programmert til å søke tilbake til System 1 så raskt som mulig. Denne todelingen og preferansen for System 1, er utviklet gjennom den menneskelige evolusjonen, hvor vi fremdeles deler den samme hjernebiologien som mennesker som levde i jeger og sankersamfunn for titusenvis av år siden.

De overnevnte essensialistiske og fortolkende perspektivene, handler om hvordan man tilnærmer seg kultur som fenomen. Men det skaper ikke en operasjonell definisjon for hva man legger i kulturbegrepet. En måte som for meg gir mening når man skal beskrive kulturkonseptet, og som er overførbart til oppgavens hovedtema sikkerhetskultur, er Bradd Shores (1996) tilnærming for å forstå kultur som en overlappende samling av de overnevnte mentale modellene innenfor en gruppe.

Mentale modeller er altså hjernens foretrukne måte å fortolke input og beslutte etter. De mentale modellene danner kunnskapsstrukturer som hjelper mennesker å skape mening

og respondere på de omstendigheten de møter. Den mentale modellen skaper et bilde i individets sinn av hvilke elementer som spiller inn i situasjonen, og hvordan disse elementene påvirker hverandre og henger sammen. I tillegg kan mentale modeller benyttes til å forstå nye omstendigheter basert på det man kjenner til om sammenlignbare andre situasjoner. En mental modell kan slik forstås som en psykologisk representasjon av et domene eller en situasjon som gjør at individet kan forstå og forklare situasjonen, og predikere videre utvikling. Benevnelsen mentale modeller er et samlebegrep for flere betegnelser som i stor grad beskriver slike meningssystemer; kognitive kart (Axelrod, 1976), script (Abelson, 1976), skjema (Fiske & Taylor, 1991; Neisser, 1976; Rumelhart, 1984), og tros- og kunnskapsstrukturer (Fiske & Taylor, 1991). I denne oppgaven drøftes ikke distinksjonene mellom disse termene, men benytter betegnelsen mentale modeller gjennomgående.

Men hvordan kan dette knyttes til kulturbegrepet? Begrepene benyttet for å beskrive mentale modeller, fokuserer i hovedsak på den individuelle meningsdannende prosessen. Men innenfor kulturens sosiale natur, vil det være de mentale modeller som deles innenfor en gruppe, som skaper dette rammeverket og prosessen som en gruppe bruker for å konstruere en kollektiv forståelse av en gitt situasjon (Liu & Dale, 2009). Shore beskriver dualiteten mellom de individuelle og delte modellene på følgende måte, når han beskriver de delte modellene som:

«an extensive and heterogeneous collection of «models», models that exist both as public artefacts «in the world» and as cognitive constructs «in the mind» of members of a community» (Shore 1996, s. 44).

Det er altså forskjell på de idiosynkratiske individuelle mentale modellene, som vi alle er i stand til å konstruere og hele tiden benytter oss av, og de delte konvensjonelle modellene. Men begge er en del av de personlige kognitive ressursene benytter oss av i hverdagen. De delte kulturelle modellene, er altså ikke skapt av våre egne erfaringer alene, men skapt i sosialt samspill og moderert av kollektive normer. Legge oppsummerer det kulturelle samspillet mellom individuell handling og kollektiv meningsdannelse: «It is both the shaper of human action and the outcome of the process of social Creation and reproduction» (Legge 1995, s. 186). Delte mentale modeller er altså ikke bare summen av de individuelle mentale modellene, men inkluderer den synergieffekten i kommunikasjonsprosessen eller sosiale interaksjonen modellene deles i.

Liu og Dale (2009) har derfor definert mentale modeller i sosial interaksjon som «a cognitive network comprised of interrelated informational, relational, and emotional elements of knowledge» og de delte mentale modellene som «the degree of convergence between the individually held mental models». Kultur er altså ikke snakk om identiske mentale modeller innenfor en gruppe, eller «total kognitiv homogenitet» som Shore (1996) beskriver det. Det er en overlappende struktur i de individuelle modellene hos gruppen, som skaper en kulturell enhet. Glomseth (2019) beskriver det med enklere ord: «Menneskene møter problemer, nye kontekster og lærer å løse og beherske disse gjennom intern samhandling. Denne erfaringen blir til kultur.»

4.3. Utvikling av kultur: Meningsdanning – sensemaking

I tillegg til det rent kognitive, så skal disse strukturene av mentale modeller, bidra til å forklare og gi mening til verden rundt oss. I dette ligger et annet viktig grunnprinsipp i min forståelse av kultur: Meningsaspektet. I en artikkel av Rune Glomseth (2019), gir Ola Lystad en definisjon av kultur som beskriver viktigheten av mening:

«Kultur er bærer av mening. Kultur handler om den fortellingen som organisasjonens medlemmer er en del av og deler. Det er de verdier, meninger og ritualer som preger organisasjonen og understøtter fortellingen om hvem «vi» er, hva som holder «oss» sammen, hvordan dette skjer, og hvorfor vi er til.»

Kultur er, i alle fall om man benytter det fortolkende perspektivet, ikke en statisk størrelse. Kultur skapes i et sosialt samspill mellom medlemmene i en nasjon, en gruppe eller en organisasjon. Denne sosiale meningsdannende konstruksjonismen, omtales også med begrepet meningsdanning eller sensemaking. Sensemaking handler nettopp om menneskets fundamentale søken etter mening; eller hvordan individ og organisasjoner finner mening i hendelser og erfaringer. Sensemaking handler om å oppfatte en situasjon mens du simultant deltar og samtidig skaper en best mulig forståelse av situasjonen og hva som kan skje videre.

Sensemaking er delt i tre overlappende prosesser:

- Creation – å oppfatte «cues»
- Interpretation – Tolking av innhentede inntrykk
- Enactment – Handle etter de innspill man har fått og de fortolkninger som er gjort.

For å få i gang sensemaking-prosessen, må «cues» (innspill, hint, signal) først og fremst oppfattes, deretter tolkes og settes inn i kontekst. Oppfattelsen av «cues» leder til en tolkning og forutsigelse av hva som skjer og skal skje. Ut fra dette handles det. Weick (1969) utviklet konseptet enactment for å illustrere hvordan en organisme tilpasser seg omgivelsene, ved å direkte delta i og endre dem. Enactment er selve kjernen av sensemaking-konseptet, og illustrerer nettopp den kulturelle konstruksjonismen. Weick diskuterer enactment som aktiv sensemaking utført av individ i organisasjoner. Dette er med å forklare hvordan individ og sosiale kontekster samhandler. Daft og Weick (1984) argumentere for at individets kognisjon og handlinger gjennom enactment, er med på å skape omgivelsene, altså bidra til å skape nye delte mentale modeller, hvor videre kognisjon og handling finner sted.

Sensemaking handler imidlertid ikke om rasjonelt å finne sannhet og oppnå korrekt forståelse, og er derfor ikke det samme som situational awareness eller situasjonsforståelse. Sensemaking handler heller om å kontinuerlig skrive om en pågående historie, og drives av behov for troverdig mening heller enn nøyaktighet. Brodt og Dietz (1999) går så langt som å hevde at det er viktigere i en gruppe, å etablere en felles forståelse av meningen i situasjonen, enn å kunne drive effektiv problemløsning, fordele ressurser fornuftig, ja, selv det å oppnå enighet. Weick et al formulerte det slik:

«Sensemaking is not about the truth and getting it right. Instead, it is about continuing redrafting of an emergent story so that it becomes more comprehensive, incorporates more of the observed data, and is more resilient in the face of criticism» (2005, s. 415).

Sensemaking-prosessen er således drevet mer av troverdighet enn av nøyaktighet. Boman og Deal (2018, s. 253) uttrykker det som at det viktigste er ikke hva som skjer, men hva dette betyr. Hendelser og handlinger kan tolkes på ulike måter. Det viktigste ved hendelser og prosesser er ikke det som produseres, men det som uttrykkes gjennom historiefortelling, ritualer og seremonier. Kultur bidrar til å binde sammen en organisasjon, skaper mening og engasjement og forener medlemmene mot å oppnå organisasjonens mål.

Uten å fornekte eksistensen til en objektiv virkelighet, så hevder denne teorien at aktørene i et sosialt fellesskap kollektivt etablerer meningsstrukturer som er bygget på interaksjon mellom medlemmene. Edgar Schein (1986) oppsummerer dette enkelt ved å kalle kulturen et delt produkt av delt erfaring. På et gruppe/organisasjon-nivå introduserte Wegner (1987) «transactive memory» for å beskrive delte systemer for koding, lagring og reaktivering av informasjon. Hong og Chiu (2001) argumenterer for at individ i en kultur har tilgang på delte kognitive verktøy som brukes til å styre vurderinger og reaksjoner på situasjoner. Lau et al (2001) deler denne forklaringen, om at sosiale representasjoner, delt kunnskap og antagelser er sentrale innen kultur.

Morris og Gelfand (2004) bruker dette utgangspunktet for å argumentere for at kultur påvirker gjennom sosialisering, sosiale strukturer og symboler, hvor denne konstruksjonen er tilgjengelig og slik former konteksten som aktiviserer visse kunnskapsstrukturer. Denne prosessen eksemplifiseres blant annet ved innlemming av nye medlemmer i en kultur. Nye medlemmer vil mer eller mindre bevisst læres opp og sosialiseres inn i den rådende kulturen. Nye medarbeideren tilpasser seg organisasjonens kultur, tanke-systemer og adferdsmønstre for å «passe inn» i organisasjonen. Dersom det aspirerende medlemmet vil måtte tilpasse seg ved å både bevisst og ubevisst akseptere og internalisere både grunnleggende antagelser og verdiene og normene.

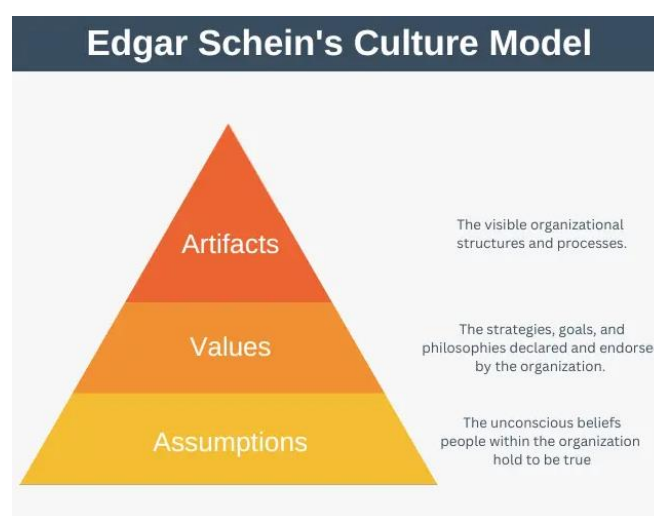
Adrian Holliday (2019) vektlegger ytterligere to aspekt i etableringen og utvikling av kulturer: Rutinisering; det å etablere rutiner som igjen etablerer roller og kobler historier til de mentale modellene, og normalisering; der atferd og atferdsmønstre blir naturlig. Det er avgjørende for organisert aktivitet at det finnes en grad av tatt for gitt. En felles basis i grunnleggende antagelser er nødvendig for å kunne fortsette organisert aktivitet uten at en konstant må tolke og refortolke mening.

Meningsrammeverket i de delte mentale modellene, gir gruppen sitt eget etos – en emosjonell undertone, følelser, stemning og motivasjon (Geertz, 1973). Dette kommer til uttrykk gjennom ideologi, normer og ritualer, språk eller diskurs og andre symbolske former. Diskurser defineres av Holliday (2019, s. 118) som bestemte måter å snakke eller skrive som tilhører en spesifikk gruppe. En diskurs er sosiale konstruksjoner, etablert for å forstå og gi mening, men kan fort få eget liv og kan lett begynne å dominere hva vi tenker er sant om en kultur. Diskurser kan skape et spesialisert språk som gir prestisje til insidere og fremmedgjør de på utsiden. De er ifølge Holliday, en sentral del av «small culture formation».

De delte mentale modellene skapes altså gjennom en kollektiv sensemaking-prosess, og forsterkes gjennom rutinisering og normalisering. Gjennom slike prosesser dannes kognitive delte verktøy som medlemmer nyter godt av og som skaper et meningsfellesskap. Nye medlemmer sosialiseres inn i kulturen, og de mentale modellene etableres som kultur gjennom rutinisering og normalisering. Kulturen uttrykkes som et symbolsk etos og en diskursform som er spesifikk for en gruppe.

De mentale modellene er altså mer enn «bruksanvisninger» for å håndtere situasjoner, men også normative verdier som man deler i en gruppe, for hva som er riktig eller galt, rett eller feil. Meningsdannelse handler derfor om mer enn å samle erfaringer for å finne den beste fremgangsmåten og programmere denne som et mentalt script. Det handler om å gjennom aktiv deltakelse, bidra til en sosial prosess der man etablerer delte grunnleggende antagelser om hvordan verden henger sammen, som igjen danner grunnlaget for delte verdier, holdninger og normer innad i gruppen, som i sin tur styrer de synlige artefaktene som atferd og diskurs.

En slik helhetlig tilnærming til kultur, dekkes av Edgar Schein (1986) sin forklaring av kulturens tre nivåer: Artefakter, verdier og normer, og de underliggende antagelser. Artefaktene er de aspektene ved en kultur som man kan sanse; det menneskene eksplisitt kommuniserer verbalt, måten de snakker på, adferd og handlinger, og fysiske gjenstander (Jacobsen & Torsvik, 2019). Artefaktene er det synlige uttrykket for kultur; det som kan observeres og det som organisasjonen «velger» å omgi seg med; symbolene som formidler kulturelementene i organisasjonen og den informasjonen organisasjonen ønsker å kommunisere gjennom kulturelementene. Visuelle logoer, emosjonelle ritualer, arkitektur og uniformering; alt som kan sanses av alle, men som for kulturens medlemmer, skaper mening. Artefaktene er inngangsbilletten til de dypere nivåene, fordi disse er sansbare, men også gjennom den aktive sensemaking-prosessen, som bygger mening hos medlemmet når han/hun eksponeres for artefaktene (Kaufmann & Kaufmann, 2015).



Figur 2: Edgar Schein's Organizational Culture Model (Denis, 2022)

Artefaktene må tolkes og tillegges en mening. Dette krever at man må dele eller forstå de kulturelle modellene, for å kunne se denne meningen. Gjennom å tilnærme seg kulturen på en fortolkende måte, og gå i dybden eller analysere gjennom thick slicing - tykke beskrivelser, kan man se den sanne symbolikken i artefaktene. Symbolenes sentrale funksjon er å reflektere organisasjonskulturen, påvirke organisasjonsmedlemmenes tenkning, verdivurdering og atferd ved å bringe frem internaliserte verdier og normer. Artefakter skal videre gjøre det enklere for den enkelte i organisasjonene å dele erfaringer og gjøre det klarere hvem organisasjonen er. De handlingsmønstrene, kommunikasjonsformene, diskursen og symbolene en gruppe benytter, er da designet ut fra de mentale modellene medlemmene har, både gjennom bruken, uttrykksformen og ut fra betydningen av disse. Dette skaper en felles mening ut over den verbale meningen i det som blir sagt, eller form og farge på en uniform eller elementene i et ritual. Militære avdelinger er særlig bevisste sine artefakter, i form av uniformering, gradsdistinksjoner, rutiniserte ritualer, rigide hierarkiske struktur og verbal og non-verbal kommunikasjon. Denne tydeligheten bidrar til å tydeliggjøre verdier og normer som skal sosialiseres inn i nye rekrutter gjennom innprenting og demonstrasjon fra eldre soldater og offiserer.

Nivået verdier, holdninger og normer handler om det uttalte om hvilken atferd som kollektivt aksepteres og dermed blir atferdsregulerende. Verdier er hva som er ønskelig og godt, som verdsettes og som man er opptatt av å ivareta. Normer er de uskrevede, men likevel bevisste og formulerbare reglene for hva som er passende i ulike sosiale sammenhenger. Hva som regnes for sosialt akseptert eller passende kan variere mellom ulike organisasjoner og roller innad i disse. I de fleste tilfeller vil normer være forsterket av sanksjoner, der det tildeles en straff for å ha brutt normene (Jacobsen & Thorsvik, 2019). Hvordan man definerer disse verdiene, hvordan man verdivurderer gode eller dårlige holdninger, og hvordan normene utformes og håndheves som rettesnorer for verdier og holdninger, er således også en form for mentale modeller.

Verdi- og normnivået i en kultur, er fundert på de underliggende grunnleggende antakelser gruppen har. Jacobsen og Thorsvik (2019, s. 123), definerer disse på følgende måte:

«Grunnleggende antakelser kan beskrives som oppfatninger eller meninger om noe som gjennom felles fortolkning i sosiale grupper nedfeller seg som sannheter, som ikke er diskutabile, og som derfor er vanskelige å utfordre og vanskelig å endre.»

De grunnleggende antagelsene er de vanskeligst tilgjengelige delen av kulturen. Det er disse som mennesker legger til grunn for virkelighetsoppfatningen sin, herunder antagelser om forhold som menneskers natur, forholdet til omverden, regler for sannhet og virkelighet, tidsbegrep, tro osv. Denne delen av kulturen er ubevisste rammefaktorer for hvordan vi oppfatter, tolker og forstår verden rundt oss. Det er vanskelig å sette ord på dette fordi vi tar det for gitt som rasjonelle, utvilsomme faktum, som vi ikke setter spørsmålstegn ved (Schiefløe, 2021, s 52).

4.4. Sikkerhetskultur – en del av organisasjonskulturen

Kulturbegrepet assosieres ofte med nasjoner eller folkegrupper. Men begrepet slik jeg har drøftet over, handler om meningsfellesskap og delte mentale modeller innenfor alle typer grupper. Denne oppgaven fokuserer på organisasjoner, som også er et generelt begrep, men som man i større grad har en midlertidig tilhørighet til. Organisasjoner kan defineres som «et sosialt system som er bevisst konstruert for å løse spesielle oppgaver og realisere bestemte mål» (Jacobsen & Thorsvik, 2019). I dette ligger et premiss om et formål eller en hensikt med organisasjonen.

En organisasjon er en gruppe som har sin egen sosiale kontekst og sosiale interaksjoner, som danner rammer og etablerer grunnleggende antagelser, verdier, normer og observerbare atferdsmønstre, basert på delte kulturelle modeller innenfor gruppen. Kulturen er det limet som binder sammen en organisasjon, forener mennesker og bidrar til organisasjonen sin måloppnåelse (Schiefløe 2021, s. 54). Typisk for kulturinnholdet, er at dette er forhold som organisasjonsmedlemmene mottar gjennom interne sosialiseringprosesser, som blir tatt for gitt og ikke satt spørsmålstegn ved. Edgar Scheins (1986) oppsummering av organisasjonskulturbegrepet kan gjengis på følgende måte:

«Organisasjonskultur er et mønster av grunnleggende antakelser utviklet av en gitt gruppe etter hvert som den lærer å mestre sine problemer med ekstern tilpassing og intern integrasjon - som har fungert tilstrekkelig bra til at det blir betraktet som sant, og som derfor læres bort til nye medlemmer som den riktige måten å oppfatte på, tenke på og føle på i forhold til disse problemene» (Jacobsen & Thorsvik, 2019).

Organisasjonskultur er et viktig tema for praktisk organisasjonsforståelse og utøvelse av lederskap. Det er også et viktig tema innenfor forskning og utdanning i organisasjons- og ledelsesteori. Kultur har betydning for alle ansatte i organisasjoner, og alle typer organisasjoner uansett sektor. Samtidig er organisasjonskultur et komplekst og krevende begrep, ikke bare fordi det som sitt «morbegrep» kultur, blir hyppig brukt uten at det gis et definert innhold, men også fordi det finnes så mange ulike definisjoner og perspektiver på det blant organisasjonsforskerne.

Det er viktig å skille konseptene organisasjonskultur og organisasjonsklima. Klima består av midlertidige holdninger, følelser og oppfatninger hos individer (Schneider, 1990). Selv om kulturen er plastisk og i konstant endring, er klima basert på holdninger og kan endre seg raskt og dramatisk. Klima kan være en del av artefaktene i en kultur, men handler mer om individuelle perspektiver enn de interpersonale delte kulturelle modellene. Et essensialistisk perspektiv vil kunne forveksle klima med kultur gjennom sin mer overfladiske tilnærming til «måling og veiing» av det som kan sanses.

I et intervju med Roar Thon (Ellestad et al, 2019), fagdirektør for sikkerhetskultur i NSM, forteller han at sikkerhetskultur og organisasjonskultur er sidestilt. Sikkerhetskultur spesifikt, kan ikke skilles fra organisasjonskultur, da det som skiller organisasjonskultur fra f.eks. nasjonskulturer, er organisasjonens formål. Om det er å tjene penger på det kommersielle markedet, fylle et samfunnsoppdrag om å yte helsetjenester, eller å bidra til fysisk fostring eller sosial nettverksbygging, har virksomheter, offentlige etater, idrettslag og arbeidslivsforeninger, klare formål.

Begrepet sikkerhetskultur er som tidligere beskrevet, relativt nytt, men brukes stadig oftere av både akademikere og praktikere. Reason (1997, s. 191) uttaler seg noe negativt om begrepet sikkerhetskultur: «Few things are so sought after and so little understood». I en FFI-rapport innen personellsikkerhetsfeltet, konkluderes det med at «En god sikkerhetskultur og et godt lederskap er viktig for å redusere risikoen for innsidevirksomhet» (Slagnes, 2023, s. 27). Rapporten henviser til faktorer som jobbtilfredshet, sikkerhetsbevissthet, rapportering og kunnskapsutvikling. Noe mer forklaring rundt hvordan forfatteren definerer sikkerhetskultur, eller hvilken betydning sikkerhetskulturen konkret spiller, gir rapporten ikke.

Det var ikke før i begynnelsen av dette årtuset, at forskere først begynte å anerkjenne sikkerhetskulturens betydning i organisasjoner. F.eks. Nosworthy (2000), drøfter hvordan organisasjonskulturen har en sterk innvirkning på en organisasjons sikkerhetsnivå, og Borck (2000) uttaler at utover å benytte den siste teknologien, må effektiv sikkerhet også involvere organisasjonskulturen. Weick og Sutcliffe (2007) viser til studier som sier at organisasjoner med sterk sikkerhetskultur kjennetegnes ved at de er opptatt av desentralisert beslutningstaking, nødvendig reservekapasitet, kontinuerlig trening og en rekke andre sikkerhetselementer.

Nasjonal sikkerhetsmyndighet definerer på sine nettsider, sikkerhetskultur til å være summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd (NSM, Sikkerhetskultur, ukjent dato). Denne definisjonen inkluderer artefakt-nivået gjennom sikkerhetsatferd, og nivået for verdier, holdninger og normer, men mangler inkludering av de grunnleggende antagelsene.

Roar Thon har også publisert det han mener er 11 tegn på en god sikkerhetskultur gjengitt i illustrasjonen under.



Figur 3: 11 tegn på god sikkerhetskultur (Thon, 2022)

Hva sier egentlig slike tegn de om det kulturelle? Disse er observerbare, målbare kvaliteter. De er en del av det Schein (1986) kaller ytre artefakter. Disse tegnene kan måles binært; om de finnes eller ikke. Men de sier ikke noe om hvorfor de er implementert, eller om de faktisk oppfattes slik de er tenkt i organisasjonen de gjelder for. Hvis ansatte hjelper hverandre til å bli sikrere, hvorfor gjør de dette? Gjør de det alle sammen, eller er det bare noen få? Hva er de grunnleggende antagelsene om verden og organisasjonen som deles av medlemmene, som danner grunnlaget for en slik atferd?

De nevnte utfordringene med å definere begrepet sikkerhetskultur, søkes å imøtekommes i denne oppgaven. Jeg har tidligere definert sikkerhet som:

Prosesen, inkludert det teoretisk-analytiske, det praktisk-operative, og det administrative-organisatoriske arbeidet med formål å redusere og håndtere risikoen for uønskede tilsiktede hendelser utført av ondsinnede beviste trusselaktører.

Ovenfor har jeg argumentert for å tilnærme seg kultur som delte mentale modeller innenfor en gruppe, dannet gjennom sosiale prosesser som sensemaking, rutinisering og normalisering, og skaper meningsstrukturer på tre kulturelle nivåer; både de synlige artefaktene, verdier, holdninger og normer, og de grunnleggende antagelsene.

Jeg vil derfor i denne oppgaven foreslå en definisjon av sikkerhetskultur, som:

De delte mentale modellene innenfor en organisasjon, som danner felles meningssystemer for medlemmene innenfor rammene av sosialt samspill og prosessene som påvirker forståelsen for og utførelse av sikkerhet i organisasjonen.

4.5. Lærende kultur

Som nevnt over, henvises det ofte til sikkerhetskultur i faglitteraturen. Men hvordan begrepet skal forstås i teorien og omsettes i praksis, er i mye mindre grad omhandlet.

Det er imidlertid gjort en del akademisk arbeid knyttet til organisasjoners resiliens og evne til å lære og utvikle seg, der det kulturelle er undersøkt nærmere.

Rosness et al (2010) skriver i sin rapport om «Organisational Accidents and Resilient Organisations» at den kulturelle dimensjonen i organisasjoners evne til å stå imot uønskede hendelser, handler om evnen og viljen til å utveksle informasjon, gi tilbakemeldinger, revurdere beslutninger og si ifra for å stanse feil og misforståelser. Videre argumenterer rapporten for hvordan kultur kan bidra til høy grad av orden og forutsigbarhet. En kultur som er villig til å lære kan erstatte formelle kontrollstrukturer og detaljerte operasjonsprosedyrer. Dette henvises til lærende kulturer.

Her trekkes teorien om High Reliability Organisations (HRO), eller høypålitelighetsorganisasjoner, frem som eksempel på organisasjoner med særskilte kulturelle trekk som fremmer sikkerhetsarbeid. Teorien rundt dette er basert på inngående studier av organisasjoner som har vist en særlig god evne til å håndtere komplekse utfordringer uten at det fører til flere eller større uønskede hendelser. Weick og Sutcliffe (2007) trekker frem beredskapsorganisasjoner eller -avdelinger/-team, som f.eks. akuttmottak på sykehus eller kjernekraftverk, som må forholde seg til ekstraordinære situasjoner på regulær basis. Disse organisasjonene som har lært seg å håndtere utfordrende, uønskede, alvorlige krisehendelser, gjennom å reagere hensiktsmessig på det uventede. De anerkjenner at planlegging og prosedyrer bare kan ta høyde for så mye.

For å bygge en slik høyt pålitelig organisasjon vektlegger Weick og Sutcliffe det de kaller «informed culture» med de følgende subkulturelle trekkene:

- En rapporterende kultur der medlemmene deler deres forståelse for hva som har gått galt.
- En rettferdig kultur som behandler medlemmene saklig og forutsigbart basert på definerte retningslinjer for akseptabel eller ikke-akseptable atferd. Feil som følge av akseptabel atferd straffes ikke. Når noe går galt søker man å finne grunner til det, ikke syndebukker.
- En fleksibel kultur som fremmer individuelt skjønn og variasjon foran uniform konformitet.
- En lærende kultur som fokuserer på å øke alle medlemmenes kapasitet og skaper rammer for erfaringsdeling.

Analysen i en studie av beredskap og erfaringslæring, viser at en viktig faktor for læring var knyttet til erfaringsdeling gjennom skriftlige rapporter: Avviksbehandlinger fra hendelser som ble utformet som teoretisk kunnskap i form av f.eks. nye tiltakskort i beredskapsplanen i forkant av ny trening og øvelse (Berger 2021, s. 68). Rosness et al skriver i sin rapport om kultur og systemer for læring, at: «Kulturelle trekk ved organisasjonen kan påvirke evne og vilje til å «tenke utenfor boksen» eller å tilegne seg ny kunnskap» (2013, s. 24). På den andre siden vil manglende kultur for evaluering og læring føre til negative sikkerhetsmessige konsekvenser. I rapporten fra 22. juli kommisjonen ble det kritisk påpekt at flere aktuelle organisasjoner hadde unnlatt å gjøre grundige evalueringer av egen beredskap. En av grunnene kunne ha vært frykten for å avdekke pinlige svakheter ved egen organisasjon. Slike organisasjoner deler også sjelden negative erfaringer med omgivelsene, hevdet kommisjonen (NOU 2012:14).

Teorien om HRO, informed culture og innsikt i beredskapsorganisasjoner, synliggjør viktigheten en organisasjons evne og kultur for læring, innenfor sikkerhetsarbeidet.

Jacobsen og Torsvik (2019) støtter også opp under påstanden om at kultur er basert på læring. Læring, her forstått i betydningen «en relativt varig endring i opplevelse og atferd som følge av tidligere erfaring» (Svartdal, 2022). Læring viser til hvordan en tilpasser en organisasjon til nye erfaringer som f.eks. forandringer i arbeidssituasjonen. Dette skjer gjennom ekstern tilpasning, hvor man vektlegger forholdet og tilrettelegging til omgivelsene; kunder, leverandører, konkurrenter og andre eksterne parter – og intern integrasjon, hvor intern kommunikasjon og samarbeid er i fokus. Den interne integrasjonen er også viktig for at alle i fellesskap kan bidra til realisering av organisasjonens mål (Jacobsen & Torsvik, 2019). Rosness refererer til læring gjennom historiefortelling som en av de viktigste interne integrasjonsmidlene for «kulturell koordinering» siden naturlig tale er en rikere kommunikasjonsform enn formelle prosedyrer, avviksrapportering eller statistikk (Rosnes et al, 2010, s. 58-60).

Organisatorisk læring blir dermed å regne som en del av sensemaking-prosessen, og dannelsen av delte mentale modeller gjennom rutinisering og normalisering. Organisatorisk læring skjer gjennom psykologiske prosesser som intuisjon, fortolkning, integrasjon og institusjonalisering (Rosnes et al, 2013, s. 23). Weger (1987) hevder at vi lærer av andre gjennom interaksjon og observasjon. Som i vennskap og romantiske forhold, kan kognitiv atferd for å klassifisere, beskrive og evaluere informasjon, effektiviseres til et nivå av likhet – altså delte mentale modeller, eller det Weger kalte «transactive memory». Hong og Chiu (2001) argumenterer for at individ som medlemmer i en kultur, har tilgang på slike delte kognitive verktøy som brukes til å styre vurderinger og reaksjoner på situasjoner. Lau et al (2001) deler denne forklaringen, om at sosiale representasjoner, delt kunnskap og antagelser er sentrale innen kultur.

Læring fra andre medlemmer, av erfaringer og av ny kunnskap, inngår altså som en del av den meningsdannende prosessen. Å legge til rette for systematisk erfaringslæring er en måte å etablere både effektive tiltak og formålstjenlig beredskap, men bidrar også til utvikling av sikkerhetskulturen i organisasjoner.

4.6. Ledelsesteori

Det er stor enighet om at organisasjonskultur er sentralt for atferd og resultater i enhver organisasjon. Likevel er det liten enighet om hvordan begrepet skal forstås. Det samme gjelder om og hvordan ledere kan påvirke kultur (Glomseth, 2019). Organisasjoner har som et grunnpremiss, at de skal oppfylle et formål. Northouse definerer lederskap som: «a process whereby an individual influences a group of individuals to achieve a common goal» (2019, s. 5). Det er altså et lederansvar å påvirke medlemmene mot organisasjonens måloppnåelse, herunder også å oppnå en hensiktsmessig sikkerhetskultur som skal bidra til å sikre denne måloppnåelsen fra hindringer i form av sikkerhetshendelser. I en studie fra Malaysia konkluderer man med at ledelse har en påvirkningskraft på sikkerhetskultur og sikkerhetsatferd:

«Leadership styles play an important role to enhance employee's information Security awareness and may lead to proper information Security compliance behaviour.» (Balakrishnan & Humaidi, 2015, s.311.)

En ledes påvirkning på sikkerhetskulturen, kan sees i sammenheng lederens påvirkningsmulighet på den organisatoriske læringen. Rosness et al (2013, s. 15) oppsummerer organisatorisk læring som endring i organisatorisk kunnskap og påfølgende endringer av atferd. Dette kan sees i sammenheng med den kollektive sensemaking'ens tre overlappende prosesser: Creation-fasen er da å regne som en del av intuisjonen,

Interpretation blir det samme som fortolkning, og Enactment er integrasjonen som over tid blir institusjonalisert i organisasjonens kultur. I denne kulturelle konteksten er da læring å skape nye meningssystemer ved å påvirke de grunnleggende antagelsene som i sin tur endrer verdier, holdninger og normer, og i siste instans de synlige artefaktene, i denne oppgaven forstått som sikkerhetsatferd.

Der sensemaking omtales som en naturlig, uformell prosess, konkluderer Rosness et al med at organisatorisk læring forgår både spontant og kan styres (Rosnes et al, 2013, s. 23). Dette taler for at ledere har en viss grad av mulighet til å aktivt påvirke sikkerhetskultur i ønsket retning. Kultur utvikles som beskrevet gjennom sensemaking-prosessen, og inkluderer uformelle prosesser som sosialisering av nye medlemmer, rutinisering, skapelsen av gruppens etos og bruk av diskurs, men også gjennom organisatorisk læring. Kultur er i konstant endring gjennom disse prosessene. En leder som identifiserer uønskede kulturelle trekk i sin organisasjon, bør som en del av sitt lederansvar, forsøke å påvirke denne kontinuerlige endringsprosessen, og utvikle kulturen i ønsket retning.

I Rosnes et al sin rapport om lærende kulturer, beskrives maktaspektet som underkommunisert. Dette er paradoksalt fordi «det knapt er mulig å tenke seg sikkerhetsstyring, tilsynsvirksomhet eller organisatorisk læring uten å forutsette bruk av makt i en eller annen form» (Rosnes et al, 2013, s. 27). Rapporten konkluderer med at forhold knyttet til makt kan på flere måter påvirke en organisasjons evne til læring. Her skiller det mellom fire former for makt; innflytelse, styrke, dominans og disiplin.

Eksempelvis vil en leder i en lærende kulturs utviklingsfaser kunne bruke forskjellige makttyper. Makt i form av innflytelse vil kunne være mest effektiv i fortolkningsfasen. I integrasjonsfasen, eller det som er betegnet som rutinisering, vil maktformen styrke kunne fungere godt, gjennom å begrense alternativer tilgjengelige for medlemmene. Dominans og disiplin er systemiske former for makt som påvirker læring gjennom rutineringsprosessen i de daglige praksisene i organisasjoner. Innflytelse igjen er en maktform som kan påvirke normaliseringsprosessen i kulturutviklingen. Å klare å manøvrere mellom lederstil og maktutøvelse, er selvsagt en vanskelig øvelse som krever bevissthet, erfaring og kompetanse.

Northouse presenterer en fullskala-ledelsesteoretisk modell, som rangerer lederskap i to dimensjoner: På spekteret passiv til aktiv og på spekteret ineffektivt til effektivt. «Laissez-Faire» eller «la-det-skure» lederstil, er motsatsen til aktiv, deltakende og involverende ledelse, beskrevet som transformasjonsledelse (Northouse 2019, s. 170). Rosness et al hevder at passivitet er et hinder for systematisk læring. Motsatt vil en leders evne til å aktivt og involverende, se innovasjoner i en strategisk sammenheng og evne til iverksetting, kunne være positivt for læring i organisasjoner (Rosnes et al 2013, s. 26).

Transformasjonsledelse blir i en studie fra Sverige fra 2014, definert som når lederen utvider og opphøyer de underordnede sine interesser, slik at de fokuserer på det som er bra for organisasjonen, genererer bevissthet og aksept for gruppa sine mål, og motiverer de tilsette til å se ut over sine egne interesser til det beste for gruppen. Transformasjonsledelse er orientert mot de knytningene mellom leder og medlemmer, for å øke motivasjon og moral hos begge parter. Dette gjøres ved «å øke bevisstheten rundt verdien og viktigheten av spesifikke idealmål, å overføre egeninteresse for organisasjonens gode, og fokusere på høyerestående behov» (Ekstedt, Flores 2014).

Transaksjonsledelse som skårer middels på både effektivitet og aktiv-passiv spekteret, fokuserer på motivasjon ut fra belønning og sanksjoner. Leder kan påskjønne eller straffe medlemmer ut fra hva lederen tenker er ønsket atferd (Northouse, 2019, s. 164-165). Transformasjonsledelse handler om at man i større grad bruker innflytelsesmakt, mens transaksjonsledelse handler om disiplinærmakt.

Det er et viktig element å ikke sette de forskjellige lederstilene i lukkede siloer. «Path-goal Theory» handler om hvordan ledere kan velge lederstil som møter medarbeiderne sine motivasjonsbehov, og sørger for best mulig måloppnåelse. En leder skal ifølge denne tilnærmingen, velge lederstil ut fra både det som kjennetegner de ansatte, og det som kjennetegner oppgaven eller utfordringen (Northouse, 2019, s. 123). Skal en leder kunne påvirke de sikkerhetskulturelle dimensjonene, må denne derfor kunne tilpasse lederstil til både oppgaven og sine medlemmer. Dette krever fleksibilitet også i forhold til hvilken type makt som benyttes.

I denne sammenheng er det verdt å eksemplifisere dette gjennom de tidligere nevnte høypålitelighetsorganisasjonene (HRO). Rosness forklarer i sin rapport om organisatoriske ulykker og resiliens, at det ikke er mulig å bygge en «HRO-kultur» gjennom holdningskampanjer eller atferdstrening. Medlemmer i HRO'er rapporterer feil og tar initiativ til å fordre prosedyrer, fordi det er etablert en forventning om av slike handlinger fører til forbedringer (Rosnes 2010, s. 64). En slik høypålitelighetskultur krever at ledere fasiliteter for læring, evaluering og avviksrapportering, og aktivt og involverende synliggjør positive effekter av dette for medlemmene.

4.7. Sikkerhetskulturelle dimensjoner

En utfordring for en leder som ønsker å jobbe aktivt med sin organisasjons sikkerhetskultur, er at det i tillegg til en manglende felles definisjon av sikkerhetskultur, også mangler et felles begrepsapparat som kan benyttes i bevisstgjøring, kartlegging og forståelse av egen sikkerhetskultur.

En metode som man finner igjen hos flere aktører, både blant de kommersielle og de akademiske aktørene innen fagfeltet, er å beskrive organisasjons- og sikkerhetskultur med utgangspunkt i dimensjoner. Dimensjoner danner et rammeverk for identifisering og vurdering eller fortolkning, og fungerer som et begrepsapparat man kan benytte for å beskrive det som ellers kan virke vanskelig å sette ord på. Som et eksempel har den norske forskeren Kai Roer og selskapet KnowBe4, definert sikkerhetskultur som «ideene, vaner og sosial atferd i en organisasjon som påvirker sikkerheten», og har listet opp syv dimensjoner som man kan vurdere en sikkerhetskultur ut fra: Holdninger, Atferd, Kognisjon, Kommunikasjon, Etterleving, Normer og Ansvar. Gjennom KnowBe4 sitt analytiske verktøy, blir organisasjoner målt på en skala fra 0-100, ut fra skåren på disse dimensjonene (The Security Culture Report 2021).

Dette er måleverktøy designet for salg på det kommersielle markedet. Tilnærmingen gjennom disse dimensjonene tilsier at sikkerhetskulturen er et «produkt», noe man har eller mangler i større eller mindre grad, og noe som kan observeres, måles og vurderes på en skala fra god til dårlig. Dette kan sammenlignes med måten de store essensialistene Hofstede, Hall og Trompenaar ser på kultur, med utvalgte, målbare dimensjoner som gir skår og et grunnlag for på predikere atferd. Det som måles gjennom spørreskjema, er i større grad de eksplisitte synlige kulturelle artefaktene i en kultur, fremfor de vanskeligere tilgjengelige, grunnleggende antagelsene som ligger bak og danner de meningskapende delte kulturelle modellene for en organisasjon. Dette er en

tilnærming som ønsker å beskrive essensen i en kultur, som igjen fører til verdivurdering på en normativ skala.

På den andre siden kan man se på Schein (1986) og Deter et al (2000) sine dimensjoner for organisasjonskultur. Disse dimensjonene kan ikke måles ved utsending av spørreskjema, og fordrer en fortolkende kvalitativ tilnærming til kulturbegrepet. Schein har listet syv dimensjoner som han mener er sentrale i dannelsen av de minst tilgjengelige aspektene ved kulturen; de grunnleggende antagelsene:

1. Hvordan forholdet mellom organisasjon og omgivelser oppfattes
2. Hvilket syn en har på menneskets handlinger
3. Hvordan organisasjonen kommer frem til sannhet
4. Hvordan organisasjonen betrakter tid
5. Hvilke antagelser en har om menneskets natur
6. Hvilket syn man har på relasjoner mellom mennesker?
7. Hvilket syn man har på konflikt

Deter et al har på sin side utledet åtte dimensjoner for organisasjonskultur:

1. Fundamentet for sannhet og rasjonalitet: Det fokuserer på hav som oppfattes om sannhet og prosessen frem til dette. Denne dimensjonen påvirker om medlemmene følger normative eller pragmatiske ideal.
2. Tidshorisont: Hvorvidt organisasjonen tenker langsiktig, strategisk og målrettet, eller om den fokuserer på her og nå og reagerer på korte tidshorisonter.
3. Motivasjon: Indre eller ytre motivasjon, om medlemmene er grunnleggende onde/late/sårbare eller grunnleggende gode, om de bør belønnes eller sanksjoneres, og hvorvidt motivasjon kan manipuleres.
4. Stabilitet kontra endring/innovasjon/personlig vekst: Noen individ er risikovillige og åpne for endring, mens andre foretrekker stabilitet og har aversjoner mot å leve med risiko/usikkerhet. Dette gjelder også for organisasjonskulturer. Risikovillige organisasjoner beskrives ofte som innovative og i konstant utvikling, mens risikoaversive organisasjoner beskrives som stabile og konservative.
5. Arbeidsorientering: Balansen mellom produktivitet og sosiale relasjoner. Er arbeidet målet i seg selv, eller et middel for å oppnå det man ønsker seg og å utvikle sosiale relasjoner. Roller på arbeidsplassen og ansvar er viktige element i denne dimensjonen.
6. Isolasjon kontra samarbeid/samhandling: Hvordan ønsker man å jobbe; alene selvstendig, eller i team eller grupper. Er samhandling positivt eller undergraver det autonomien hos den enkelte?
7. Kontroll, koordinering og ansvar: Organisasjoner varierer i hvor stor grad ansvar og kontroll er konsentrert eller delegert. Er prosedyrer og retningslinjer toppstyrt eller er det tillitt og rom for skjønn og fleksibilitet. Sentralisert kontroll gir bedre styring, men mindre initiativ og ansvarstaking hos medlemmene.
8. Internt eller eksternt fokus: Hvordan en organisasjon forholder seg til verden og miljøet rundt. Hva kan man styre selv og i hvilken grad blir man styrt av eksterne forhold. En organisasjon kan ha internt fokus gjennom å fokusere på egne medlemmer og prosesser, eller eksternt fokus ved å fokusere på ytre påvirkningskrefter; premissleverandører, kunder, konkurrenter og miljø.

Schein og Deter et al sine dimensjoner er ikke direkte sammenlignbare, men har flere likhetstrekk. Både Deter et al og Schein har en dimensjon som omhandler hvordan organisasjonskulturen oppfatter tid og tidshorisonter, herunder spekteret mellom lange,

strategiske tidshorisonter eller reaktivt korttidsfokus. Dette er også overførbart til Hofstedes dimensjon for maskulinitetsorientering slik han har definert det. Dette vurderes som relevant for sikkerhetskulturen, ved at det indikerer noe om hvordan organisasjonen forstår og prioriterer sikkerhetsarbeid mellom å ha et forebyggende perspektiv, eller om man fokuserer på beredskap og reaktiv hendelsehåndtering.

Deters første og Scheins tredje dimensjon handler om sannhet og rasjonalitet; hvordan medlemmer i en kultur kommer frem til at noe eksisterer og er sant. Schein har videre en dimensjon som beskriver forholdet mellom organisasjon og omgivelser oppfattes, som til en viss grad overlapper med Deter et al sitt skille mellom internt eller eksternt fokus. Disse dimensjonene er direkte overførbare til sikkerhetskulturen, gjennom hvordan medlemmene oppfatter, forstår og erkjenner trusler og risiko og hvordan man aksepterer relevansen for deres organisasjon.

Det Schein beskriver som synet på menneskers handlinger er også til en viss grad overførbart til Deter et al sin dimensjon stabilitet kontra endring. Hvordan ser kulturen på endring og risiko kontra stabilitet og trygghet. Endrings- og risikovilje i organisasjoner kan skape innovasjon, vekst og forbedringer mens risiko- og endringsaversjon som kulturtrekk, skaper stabilitet og kontinuitet. Dette kan også relateres til Hofstedes dimensjon usikkerhetsunnvikelse. Dette kan ut fra et sikkerhetsperspektiv, sees på som en organisasjons kulturelle risikovillighet. Hvordan oppfattes risiko blant medlemmene? Som noe negativt som skal unngås, som noe nødvendig man må leve med, eller som noe positivt som kan skape utvikling?

Deter et al har en dimensjon som går på motivasjon som til en viss grad handler om det samme som Scheins dimensjon om menneskets natur. I en sikkerhetskontekst, vil dette kunne omskrives til hvorvidt man ser på medlemmene som potensielle sårbarheter eller trusler, eller som ressurser eller garantister i sikkerhetsarbeidet. Er menneskets natur å «ta snarveier», er mennesker late og det «svakeste leddet» i sikkerhetssystemet? Eller er medlemmene og deres sunne fornuft og motivasjon, garantister for å opprettholde et akseptabelt sikkerhetsnivå?

Schein har to dimensjoner som går på relasjoner og konflikt. Deter et al har to dimensjoner som går på isolasjon kontra samhandling og en kontroll- og ansvarsdimensjon. Her er Hofstedes (1980) dimensjoner maktdistanse og individualisme kontra kollektivismen også relevant. Sett i et sikkerhetskulturelt perspektiv, handler dette om en organisasjons nivå av psykologisk trygghet: I hvor stor grad er det aksept for å komme med innvendinger, nye ideer, ta opp ubehageligheter, rapportere avvik som svikt i egen sikkerhet, men også trygghet til å selvrapporthere feil eller sårbarheter.

Jeg har gjennom dette, identifisert forslag til fem kulturelle dimensjoner innenfor de grunnleggende antagelsene i en organisasjon, som har relevant for den samlede sikkerhetskulturen. Disse dimensjonene vil kunne bidra til et felles rammeverk som kan brukes for å fortolkende beskrive sikkerhetskultur.

Schein	Deter et al	Sikkerhetskultur
Hvordan organisasjonen betrakter tid	The nature of time and time horizon	Sikkerhetsforståelse Sikring i forebyggende eller reaktivt beredskaps-perspektiv. Hva er den grunnleggende antagelsen om hva sikring er/skal være i tidsmessig forhold til hendelser?
Hvordan organisasjonen kommer frem til sannhet	The basis of truth and rationality	Trusselkognisjon Hva er den kulturelle modellen i organisasjonen for å forstå trusselbildet og hvordan oppleves relevansen for organisasjonen?
Hvordan forholdet mellom organisasjon og omgivelser oppfattes	Orientation and focus – internal and/or external	
Hvilket syn en har på menneskets handlinger	Stability versus change/innovation/personal growth	Risikoaksept Hva er den grunnleggende antagelsen om risiko i organisasjonen: Er risiko forstått som negativt eller som noe potensielt positivt?
Hvilke antagelser en har om menneskets natur	Motivasjon	Menneskesyn Hva er den grunnleggende antagelsen i organisasjonen om egne medlemmer: Personell som trussel, sårbarhet eller som ressurs/sikringstiltak?
Hvilket syn man har på relasjoner mellom mennesker?	Orientation to work, task, co-workers	Relasjoner, konfliktaksept Hva er den felles mentale modellen om relasjoner og psykologisk trygghet i organisasjonen: Er det greit å si ifra? Kan alle gjøre det? Hva er holdningen til avviksrapportering? Hvordan oppfattes friksjon/konflikter?
Hvilket syn man har på konflikt	Isolation versus collaboration/cooperation Control, coordination and responsibility	

Tabell 1: Sikkerhetskulturelle dimensjoner

Jeg vil i oppgavens neste del, presentere funnene fra feltarbeidet, der jeg har introdusert disse dimensjonene for sikkerhetskultur, for fageksperter innenfor sikkerhet. I oppgavens drøftingsdel vil jeg knytte sammen de teoretiske premisene slik de er presentert ovenfor, med empirien fra del 5, og etablere en forståelse for disse dimensjonene, og vurdere denne tilnærmingens relevans og bruksverdi.

5. Presentasjon av empiri

Empirien innhentet i denne oppgaven er fra dybdeintervjuene med de utvalgte intervjuobjektene. Intervjuobjektene fikk rammesatt tema som de deretter skulle reflektere rundt. Funnene må derfor beskrives kvalitativt ut fra omfanget og hvordan objektene valgte å fokusere i sine svar.

Den tematiske inndelingen i intervjuene, er basert på hvordan besvarelsene fra intervjuobjektene belyste oppgavens problemstilling:

Hvordan kan man tilnærme seg sikkerhetskultur på en teoretisk og analytisk måte, for å skape «tykke», kvalitative, fortolkende beskrivelser som igjen kan benyttes til endrings- og utviklingsarbeid?

Tematiseringen i denne presentasjonen av empirien tar utgangspunkt de forskningsspørsmålene jeg hadde formulert på forhånd: Hvordan kan sikkerhetskultur defineres og forstås på en måte som gir verdi for sikkerhetsfaglige praktikere? Hvordan kan man gjennom et begrepsapparat og et teoretisk rammeverk bestående av kulturelle dimensjoner, forstå og analysere sikkerhetskulturer? Hvordan kan man basert på slike analyser, beskrive sikkerhetskulturer på en kvalitativ, fortolkende måte som kan brukes som utgangspunkt for utviklings- og endringsarbeid?

Det var videre en grad av styrt struktur i intervjuene, knyttet til de sikkerhetskulturelle dimensjonene og intervjuobjektene refleksjoner rundt hvordan de forstod dimensjonene, deres relevans og potensielle nytteverdi. Det teoretiske rammeverket for å benytte dimensjoner for å beskrive sikkerhetskultur, var å regne som en overordnet «tom» struktur. Intervjuobjektene refleksjoner, vurderinger og forståelse er det som fyller dette rammeverket med innhold.

Til slutt er det gjennom en induktiv analyse av empirien, avdekket noen tema som går igjen som relevante for oppgavens helhet, og problemstillingen spesifikt, som dreier seg om sikkerhetsfagets særegenheter, og hvordan dette påvirker og påvirkes av kulturelle forhold.

Funnene fra datainnsamlingen kategoriseres derfor i følgende tre kategorier:

- Sikkerhetskulturbegrepet, forståelse herunder målbarhet og mulighet for styring
- Felles begrepsapparat; sikkerhetskulturelle dimensjoners relevans og nytteverdi
- Sikkerhetsfagets særlige utfordringer med kulturell relevans

5.1. Hvordan brukes sikkerhetskulturbegrepet?

Åpningstemaet i intervjuene var begrepet sikkerhetskultur og hvordan intervjuobjektene forstod, definerte og brukte denne termen. Intervjuobjektene var ganske samstemte i at de opplevde at sikkerhetskulturbegrepet er vanskelig å definere. Det ble blant annet henvist av et av intervjuobjektene, til en undersøkelse der over 1000 sikkerhetsledere fra hele verden, som ble spurt hvor viktig sikkerhetskultur var. 90 % svarte at det var viktig eller veldig viktig. Men på spørsmålet hvordan definerer du sikkerhetskultur, fikk man nesten like mange forskjellige svar som det var respondenter. Et av intervjuobjektene hadde en definisjon som han mente fungerte:

«Vi brukte Oxford sin definisjon på kultur: «ideas, customs and social behaviours of a group, of a people». Og også Oxfords definisjon på sikkerhet: «staying free from threats and danger» eller noe sånt. Så da endte vi opp med den definisjonen som vi bruker til normale folk, om du vil. «Security culture is the ideas, customs

and social behaviours of a group that influences the Security of the group.» Og etter å ha holdt på med dett her i 11-12 år og prøvd å komme opp med en bedre definisjon inn mot den målgruppa, så har vi ikke klart det enda.»

Et annet intervjuobjekt reflekterte rundt definisjonen av sikkerhetskultur, på følgende måte ved å legge vekt på det kollektive, det sosiale og at kultur er en dynamisk størrelse:

«Kultur, da tenker jeg «slik er vi her». Dette er det vi omgir oss med. Slik er vi med hverandre. Som er dette «vi'et» satt sammen. I motsetning til organisasjon eller satte organisasjonsprosesser, eller hva du kan flytte vekk fra det begrepet. Dette «sik gjør vi det her», så betyr det at det ligger sterke sosialiserende faktorer, som i hvert i de fleste moderne enheter i arbeidslivet, til enhver tid er litt i flux.»

Et av intervjuobjektene mente at begrepet i seg selv var til en viss grad misvisende. Han hadde f.eks. hørt hos en av Norges største etater, at de ikke hadde implementert sikkerhetskultur enda. Han opplevde at det ble sett på som et eget produkt man måtte produsere og implementere. Men hans tilnærming var at man må inkludere sikkerhet som en del av virksomhetskulturen – ikke noe eget på siden. En annen illustrerte det med å fortelle om grunnlagsdokumentet i virksomheten han jobber i, der det stod at «alle ansatte, innleide og tredjepart har ansvar for god sikkerhetskultur.» Men det stod ingen steder kva som menes med sikkerhetskultur og heller ikke hvilke kriterier man har for god eller dårlig sikkerhetskultur. Han reflekterte på følgende måte rundt begrepet:

«Det innebærer for meg, god sikkerhetskultur, at alle har den samme grunnforståelsen for hvorfor ting er som de er. Det dreier seg om at alle har noenlunde felles bakgrunn innenfor en sektor eller en utdanningsgren, og hvor forståelsen, da er vi litt inne på Safety-begrepet, hvor alle som et lag i marinejegerkommandoen, vet at hvis de ikke følger normen så kan det gå ut over sidemannen. Og hvor de godtar det. Det innebærer også oversatt til banken, en god sikkerhetskultur her, innebærer at folk er klar over hvilke forventinger som er stilt til dem med tanke på daglig sikkerhetsmessig atferd.»

Denne respondenten fokuserer på felles grunnforståelse eller grunnleggende antagelser, både hvorfor man gjør ting og hva som er forventet sikkerhetsmessig atferd. Et annet intervjuobjekt formulerte det som at god sikkerhetskultur, er at alle har den samme grunnforståelsen for hvorfor ting er som de er. Og at de godtar det. En tredje formulerte det på følgende måte:

«Jeg tenker at sikkerhetskultur er å ha en bevissthet, en sosial bevissthet i egen enhet eller hvor du nå har denne kulturen hen, om hvordan du skal ivareta Security. Og den må være preget av at du faktisk klarer å lage en slags plattform som alle står på, felles, og som alle også opplever et felles ansvar for å opprettholde. Ikke fordi det er et regelverk, men fordi det er en større grunn til det. Og da klare å både håndtere regelverk og rammer som pålagt, men også å operere innenfor en intensjon om å opprettholde det «Level of Security» som vi søker å oppnå.»

Denne respondenten fokuserte på sosial bevissthet, eller delte mentale modeller for sikkerhetsarbeid. Han skiller også kultur fra formelle strukturer, ved at det ligger en intensjon, en hensikt bak sikkerhetsarbeidet.

Alle intervjuobjektene trakk frem det kollektive, delte; både forståelse og den faktiske utøvelsen av sikkerhetsatferd, eksempelvis gjennom formuleringen: «Vi snakker om sosial atferd, ikke bare atferd.»

Et intervjuobjekt henviste til dette som psykologiske kontrakter. Innenfor dette var de fleste inne på den sosialiserende uformelle mekanismen i etableringen av og ved inkludering av nye medlemmer, inn i en kultur. Det var også gjennomgående fokus på kulturs dynamiske natur, at det er en prosess som aldri tar slutt.

Som i den overnevnte undersøkelsen blant over 1000 sikkerhetsledere, så fremstod svarene og refleksjonene fra intervjuobjektene rundt sikkerhetskulturbegrepet, som forskjellige, men likevel innenfor det samme rammene. Felles elementer i intervjuobjektene refleksjoner, var delte ideer, verdier, normer, holdninger og den faktiske sikkerhetsatferden.

En av lederne blant intervjuobjektene fortalte at han hadde fokusert på fundamentene i virkelighetsoppfatningen til medlemmene i hans organisasjon. Han hadde etablert det han kaller «ritualer» der man blant annet gjennom faste avdelingsmøter og hvordan de ble gjennomført, tilnærmet seg de mer abstrakte perspektivene som trusselbildet og hvordan det kan påvirke avdelingen.

Oppsummert så trakk intervjuobjektene fram det kulturelle innenfor sikkerhetsfaget, som en viktig bestanddel. Det kollektive, delte, skapt og utviklet gjennom sosiale prosesser, var gjennomgående i alle respondentenes svar. Både de synlige artefaktene som atferd og etterlevelse, var en del av alle objektene refleksjoner. I tillegg benyttet de formuleringer som verdier, normer og holdninger som bestanddeler av sikkerhetskulturen. Til en viss grad ble de grunnleggende antagelsene tatt med i refleksjonene; formulert som «grunnforståelse», «plattform», «ideer» eller virkelighetsoppfatning. Kulturers dynamiske natur var også gjennomgående i svarene fra intervjuobjektene.

5.2. Kan sikkerhetskultur måles?

Refleksjoner rundt hvordan man kan måle eller kartlegge sikkerhetskulturen, var mer delte. Intervjuobjekter trakk frem at det vil henge sammen med hvordan man definerer sikkerhetskultur. Er det heftet opp i enkle parametere, som hvor mange har gjennomført e-læringskurs eller antall avvik ut fra et system vil det kunne gi «enke svar».

«Det er jo veldig enkelt å måle en del av disse oppfylingskravene. F.eks. hvor mange har gjennomført e-modul «X, Y, Z, innen ABC». Vi mangler to stykker. Da er det kjeft. Eller har vi lykkes i å nå fram med budskapet om hvilke land man ikke skal ta med seg mobiltelefon til? Det lar seg jo gjøre å avdekke ofte. Eller hvilke land man ikke skal søke om å besøke. Eller andre sånne veldig enkle parametere. Vi har jo masse sensorer på systemene våre som oppdager irregulariteter. Disse er veldig lett å avdekke. Denne type handlinger er lette å avdekke. Avviksregistrere en rekke ting, er veldig enkelt. Problemet er at da vrir du organisasjonen mot å følge med på det, mot å oppfylle det som er enkelt å avdekke.»

Respondenten uttrykker altså at man kan måle sikkerhet på en rekke kriterier, men de som er enkle å måle beskriver ikke nødvendigvis det kulturelle. Slike målinger vil styre fokuset og man går dermed glipp av de meningsbærende årsakssammenhengene.

Et av intervjuobjektene mente at det var essensielt for å kunne jobbe med sikkerhetskulturen, at man målte og skapte en baseline for å finne ut hvordan du skal komme deg fra der du er, til dit du ønsker å være. Et annet intervjuobjekt uttrykte at han fikk en helt klar «temperaturmåling» når han holdt foredrag og presenterte problemstillinger ute i avdelingene. Han vurderte det som positivt de gangene han fikk henvendelser på e-post eller når noen kom inn på kontoret hans i ettertid for å snakke om sikkerhetsrelaterte tema. Disse uttalelsene handler om viktigheten av bevisstgjøring av hva som er den kulturelle nå-tilstanden.

Respondenten som jobbet med forskning og utvikling innenfor digital informasjonssikkerhet, hadde laget et måleverktøy for sikkerhetskultur. Han har formulert egne dimensjoner for sikkerhetskultur og hevder at hans datagrunnlag med over en million respondenter, gjør det mulig å måle disse dimensjonene på et ganske detaljert nivå. Men han problematiserer også hva det er man måler og relabiliteten til slike data:

«Hvis du vil måle kultur, da må du måle alle. Hvis ikke så sier du bare noe om de menneskene du har målt. Så det er en viktig forutsetning. Men du kan godt måle de og snakke om de. Men jeg tror at du er nødt til å måle alle. Om ikke annet så i den gruppa eller det teamet eller hva det er for noe. For da kan du si noe om de som team, som gruppe, og si noe om kulturen deres. Hvis ikke sier du bare noe om deg som individ. For en av de tingene du ønsker å fange opp, jeg var inne på det i sted med self-report bias; du vil alltid svare sånn at du høres bedre ut enn det du er. Ved å stille spørsmålet, hva ser du i gruppa di, og stille det spørsmålet til alle i gruppa, så er du nærmere kjernen.»

Her problematiserer respondenten måling av individer for å si noe om kultur, og han utfordrer sin egen metodikk ved å vise til det kollektive aspektet ved kultur. Dette kan sees i sammenheng med den tidligere siterte respondentens problematisering av kvantitative målinger for å beskrive kultur. Et annet intervjuobjekt problematisere videre det å samle inn store mengder kvantitative data, f.eks. i form av spørreskjema:

«Men jeg er veldig skeptisk til spørreundersøkelser. Fordi folk har en tendens til å svare på en måte som gjør at de kommer veldig godt ut. Og det gir ikke et reelt bilde av hva den reelle situasjonen er. Når man kommer i den praktiske delen da. Det å måle den reelle atferden er et av den vanskeligste delen av dette her. Og det får du ikke gjort, mener jeg, troverdig med å bare gi ut et spørreskjema.»

Respondenten mener altså at måling gjennom spørreskjema ikke gir et reelt, troverdig resultat som sier noe om sikkerhetskulturen i en organisasjon. Flere trakk her frem utfordringen med self-report bias ved slik selvrapporing.

Oppsummert så var intervjuobjektene syn på måling av sikkerhetskultur, delt. Det er vanskelig å finne parametere å måle ut fra, som gir en forståelse av det kulturelle og som kan tillegges kulturelle trekk. Man kan gjøre seg opp en mening, en «temperaturmåling», som gir et inntrykk av sikkerhetskulturen, men dette er ikke måling, bare kvalifisert synsing. Andre respondenter viste til at ved å velge ut gitte parametere, så kan man få data som kan kvalitativt analyseres, og dermed gi en måling av sikkerhetskulturen.

Påliteligheten til slike data, opp mot den reelle situasjonen ble problematisert av flere andre. Man definerer selv hva man måler som de relevante kulturtrekkene. Og ved å innhente slike data gjennom spørreskjema, får man utfordringer med self-report bias

som kanskje ikke gjenspeiler den reelle atferden og kulturen i organisasjonen. Som sagt var respondentene delte i synet på i hvilken grad det var mulig, og hvordan det kan gjøres. Men den samlede tendensen i svarene peker på at det er viktig og riktig å forsøke skape seg en forståelse av den sikkerhetskulturelle «statusen» eller nå-tilstanden, for å kunne jobbe videre med kulturutvikling.

5.3. Kan sikkerhetskultur utvikles og styres?

Et av forskningsspørsmålene i denne oppgaven, er hvorvidt en leder kan påvirke eller styre utviklingen av sikkerhetskultur. Dette var et naturlig oppfølgingstema til sikkerhetskulturens målbarhet. Når det gjaldt å utvikle sikkerhetskultur, var alle intervjuobjekt enige om at det var mulig. Men flere pekte på at det er en vanskelig og tidkrevende oppgave. Dette blant annet fordi det er snakk om individer i en gruppe:

«La oss si at vi snakker om 20 mennesker. Så kan du alltid forsøke å påvirke de menneskene slik at du får en så god kultur som mulig. Men du kommer ikke bort fra at det er 20 selvstendige individer, hvor det er noe grunnleggende ved de individene, som gjør at den reisen fra A til B, ikke nødvendigvis er så enkel.»

Respondenten uttrykker her utfordringen ved kulturers kollektive natur, og at påvirkning av grupper er vanskelig. Fokuset hos intervjuobjektene var at det er en kontinuerlig prosess; «det man sier og gjør i det daglige». Ledelse som et premiss for slikt arbeid, ble omtalt av flere, og definert av det ene intervjuobjektet på følgende måte:

«Å påvirke en gruppe mennesker mot å oppnå organisasjonens mål, der sikkerhet handler om mulige hindringer mot å nå disse målene.»

Et intervjuobjekt med lederfunksjon så på sikkerhetskultur som en del av sitt ansvar:

«Ja, det er jo en viktig del av jobben. For meg så er det jo riktig å etablere en felles plattform. Det går fra det sosiale i forhold til å ha en trygghet i sin egen base og trygghet ligger ikke bare faglig, men også sosialt gjennom relasjoner. Som en forutsetning egentlig har for å kunne ha faglige, tverrfaglig interaksjon med hverandre.»

Et av intervjuobjektene trakk frem en felles kulturell bevissthet, som han omtalte som delte mentale modeller, som en grunnforutsetning for å kunne utvikle kulturen i hensiktsmessig retning:

«Tenker man på kultur som delte mentale modeller, så er ledelse en av forutsetningen for å skape eller sikre et slik sosialt fellesskap.»

Å bygge yrkesstolthet gjennom fremheving av verdier eller dyder, ble trukket frem som en lederoppgave som kan brukes til å utvikle kultur i ønsket retning. Et eksempel som ble benyttet, var profesjonalitet:

«Vi må fremstå som om vi har peiling, ergo bruker vi ganske mye tid på å innprente profesjonalitet i ulike deler av organisasjonen, knyttet til alt mulig, alt fra kleskode, normal høflighet, hvordan man titulerer andre, hvordan man skriver, snakker, når man er eksternt i hvert fall. Hvordan vi behandler hverandre. Hvordan vi fremstår på jobb. Vi hekter ganske mye av sikkerhetskulturen vår på det samme. På profesjonalitet. Det er ikke sosialt akseptabelt for oss å fremstå som uprofesjonelle.»

Respondenten eksemplifiserte her en type påvirkning på verdi-, norm- og holdningsnivået som han mener fungerer i sin organisasjon.

For å sikre etterlevelse reflekterte intervjuobjektene rundt insentiver, både positive og negative, for å påvirke de sosiale prosessene som bygger den kulturen man ønsker. Både eksplisitte og implisitte rammer for sosialt akseptabel atferd kan benyttes for å bygge under de verdiene eller dydene man ønsker å utvikle.

«Utvikling av kultur er ikke vanskelig,» uttrykte et av intervjuobjektene. Sosialisering og mellommenneskelig påvirkning skaper og videreutvikler kultur kontinuerlig. Men han understreket at det er ikke sikkert at man får den utviklingen man ønsker og planla med. Og det ble av andre understreket at det er viktig å være bevisst at man ikke kan etablere systemer, f.eks. for avviksrapportering, uten å fokusere på de sosiale aspektene som påvirker hvordan systemet benyttes; hvordan policyer etterleves. Uten slik bevissthet vil det kunne gi resultat som går på tvers av det man ønsket. I dette trakk flere frem behovet med en felles forståelse, en «plattform» som både er entydig og trygg. Trygghet ble benyttet som en viktig verdi, både faglig, at man forstår hva som kreves og forventes, men også sosialt gjennom relasjoner. Den tidligere nevnte lederen blant intervjuobjektene, som fokuserte på fundamentene i virkelighetsoppfatningen til medlemmene, forklarte at «ritualer» som faste avdelingsmøter, kunne skape slike trygge rammer.

Oppsummert så mente intervjuobjektene at sikkerhetskultur kan påvirkes, og at ledelse er en påvirkningsfaktor, samt at kulturutvikling er et lederansvar. Ledelsesverktøy som påvirkning, å legge til rette for trygge relasjoner, og fremelske ønskede verdier, samt insentivmakt ble foreslått. Positive og negative insentiver ble trukket frem, sammen med sosialiseringprosesser intern i organisasjonene, som verktøy som påvirker sikkerhetskulturen. Dette ble beskrevet som krevende, både i form av tid og ressurser, men også fordi man ikke kan garantere for at påvirkning fører til ønsket utvikling.

5.4. Hvordan forstås de sikkerhetskulturelle dimensjonene?

Intervjuobjektene ble bedt om å reflektere rundt de dimensjonene jeg på forhånd hadde vurdert som relevante for å kunne fortolke en sikkerhetskultur. De fikk så få inngangsverdier som mulig når disse begrepene ble rammesatt slik det er beskrevet i metodebeskrivelsen, for at de skulle reflektere fritt rundt både relevans og hva de selv la i de forskjellige begrepene.

5.4.1. Forståelse

Intervjuobjektene ble bedt reflektere hvorvidt forståelsen av sikkerhetsfaget som noe proaktivt eller reaktivt, var relevant som dimensjon for å kunne fortolke og forstå sikkerhetskulturen.

Alle intervjuobjektene uttrykte at de forstod dimensjonen, og beskrev at dette er kjente skillelinjer innenfor sikkerhetsarbeid. Et intervjuobjekt understreket at det ikke er et motsetningsforhold mellom proaktiv og reaktiv tilnærming til sikkerhet. Begge forståelsene kan sameksistere i en organisasjon. Men han vektla tendensen til at det utvikler seg egne subkulturer inne i organisasjoner ut fra hvilken side av spekteret man befinner seg, og hvilke oppgaver man er satt til. Han beskrev fallgraven ved at de som driver de analytiske, teoretiske delen av sikkerhetsarbeidet, som risikovurderinger og sårbarhetsanalyser, ikke samhandler med de som faktisk skal håndtere de hendelsene som faktisk finner sted.

«Ja, fordi du risikerer egentlig en sånn bås-setting hvor du har noen driver forebyggende, som ikke gjør annet enn å drive holdningsskapende arbeid. Så har du noen som driver trussel- og risikovurderinger i et mer teoretisk perspektiv. Og holder dokumenter oppdatert og alt mulig sånt. Men de er helt løsrevet fra den operative delen. Det gjør at du garantert kommer til å få, ikke vanntette skott, men du får båser som gjør at det ikke er optimalt når situasjonen oppstår.»

Respondenten beskriver altså viktigheten av å være bevisst denne dimensjonen, og å bygge ned eventuelle kulturelle skillelinjer som forstår sikkerhet forskjellig innenfor samme organisasjon. Et intervjuobjekt oppsummerte sin refleksjon rundt dette med å slå fast at det er organisasjonen som bestemmer hvor man vil fokusere på sikkerhetsarbeidet, og så gjøres aktiviteter tilpasset der man har bestemt at man skal være.

«Men jeg har brukt ofte eksempelet på at veldig mange utfører veldig mange sikkerhetsoppgaver uten at de definerer det som sikkerhetsoppgaver. De definerer det som noe annet. Hvis jeg ringer til en virksomhet til økonomiavdeling eller lønnskontoet og sier at det er NN fra Oslo som ringer. Og jeg ber om liste på de 20 best betalte i denne virksomheten her, så får jeg jo ikke det. Jeg håper i alle fall jeg ikke får det. Og selv om jeg da argumenterer og krangler litt, så er det noen der som viser til en paragraf for ikke å gjøre det. Andre sier bare at det er bare sånn vi gjør det at du får ikke det. Men når de har lagt på den samtalen der, så er det veldig få som tenker at nå har jeg utøvd informasjonssikkerhet.»

Her reflekterte respondenten rundt nettopp bevissthet på sikkerhetsarbeid, ved at det eksiterer som en del av andre oppgaver som man kanskje ikke ser på som sikkerhetsprosedyrer.

Et av intervjuobjektene konkluderte i sitt svar at denne dimensjonen er relevant innenfor en sikkerhetskulturell vurdering:

«Vi behandler den i alle fall som en helt egen dimensjonerende faktor. Som henger sammen med viktigheten av målet vi til enhver tid søker å oppnå. Og det er en veldig viktig faktor fordi den styrer hvor mange tiltak du må sette inn som bidrar til å gjøre evnene dine til å oppnå mål.»

Intervjuobjektet beskriver her at hvordan man forstår sikkerhet, som proaktivt eller reaktivt, vil være relevant for hvilke om hvor mange sikkerhetstiltak man velger å sette inn.

Under dette temaet fremkom det at i forståelse av hva sikkerhetsarbeid er, ligger elementer av implisitt kontra eksplisitt kunnskap. Et objekt forklarte hvordan hans enhet som hadde eksistert i 80 år, var mye som ble sosialisert inn i nye medlemmer at «slik gjør vi det her», og slik mistet sin «hvorfor». Den tause kunnskapen basert på erfaringen og bevissthet, blir når den blir overført, uten forklaring og rasjonale for de som mangler disse erfaringene.

«En faktor som jeg tenker mye på, er eksplisitt versus implisitt. For det er veldig mye av organisasjonskultur som er implisitt. Taus kunnskap som bare ligger der. Når den, i en enhet som min som har eksistert siden 1943, og har utviklet seg åpenbart. Men ikke gjennom revolusjon, men evolusjon, da er den en viss fare for at den tause kunnskapen, eller «slik gjør vi det her», mistet sin «hvorfor». Den bare seiler av gårde.»

I forlengelsen av dette, forklarte et av de andre intervjuobjektene hvordan noen organisasjoner er veldig proaktivt orienterte. De legger vekt på å forebygge og forhindre uønskede hendelser. Men hvis en hendelse inntreffer, så har de ikke referanser eller prosedyrer til å kunne håndtere dem. På den andre siden blir noen organisasjoner reaktivt orienterte, i form av at de fokuserer på ensidig på hvordan de skal håndtere uønskede hendelser, og bruker mindre eller ingen ressurser på å evaluere og lære slik at de i fremtiden kan forebygge at dette skjer igjen.

Flere responderte med at dette trolig ikke var noe hverken individer eller organisasjoner hadde et bevisst forhold til, men at det kunne gi store utslag i hvordan man som gruppe forholdt seg til sikkerhet i det daglige. Det ene intervjuobjektet understreket at det handlet mye om å bevisstgjøre medarbeidere om «hvorfor» man handler på den eller den måten, «hvorfor» man har satt inn et sikkerhetstiltak, «hvorfor» det er en prosedyre for den ene eller andre operasjonen. I denne bevisstgjøringen vil man også som leder få et forhold til om man tenker reaktivt eller proaktivt. Det handler om å bevisstgjøre seg hvilken restrisiko man er villig til å operere med.

Det ble trukket frem at å forklare hvorfor, både øker motivasjon, men også skaper felles kulturelle mentale modeller. «*Det er begynnelsen på en kultur*», formulerte intervjuobjektet.

«Og jeg sa at hvorfor er dette tiltaket på plass? Hvorfor gjør vi dette? Og så skjønner jeg etter hvert at de greier ikke helt å forklare hvorfor tiltaket er der. Hva skal tiltaket gjøre? Da sier jeg at det får jeg et problem med. For jeg kommer til å møte nå godt skolerte mennesker, politikere, beslutningstakere, som jeg skal si til at dette må de gjøre. De kommer til å spørre meg hvorfor de også. Og når jeg ikke kommer til å være i stand til å forklare dette, så kommer det til å forringe kvaliteten på alt det jeg meddeler på hva de skal gjøre og ås vridere. For de får ingen god forklaring.»

Flere av intervjuobjektene var tydelige på at for noen organisasjoner er det mest hensiktsmessig å fokusere på det proaktive, for andre er det viktigere å ha en beredskap og et hendelsesstyrt fokus. Men hvilke grunnleggende antagelser man har om sikkerhetsarbeid, om det er det forebyggende eller hendelsesstyrt, trenger ikke ha sammenheng med behovet, men kan være etablert som en «kulturell sannhet», også omtalt som taus implisitt kunnskap.

Bevissthet hvor man ønsker å sette fokuset i sikkerhetsarbeidet, vil kunne føre til en mer hensiktsmessig tilnærming til sikkerhet. Bevissthet handler altså om å gjøre det implisitte eksplisitt, eller sagt på en annen måte; kartlegge å forstå de grunnleggende antagelsene innenfor en organisasjon. Når dette gjøres eksplisitt vil det kunne danne grunnlaget for en leders endrings- eller utviklingsarbeid.

5.4.2. Trusselkognisjon

Det neste temaet som intervjuobjektene ble bedt å reflektere rundt, hva hvorvidt kognisjon rundt trusler eller trusselbevisstheten blant medlemmene, er en relevant dimensjon innenfor sikkerhetskulturen i en organisasjon.

Trusselbevissthet eller -kognisjon, ble av flere objekter forstått og beskrevet som en dimensjonerende faktor, både for hvordan man tenker sikkerhet i det proaktive eller reaktive sporet, og hvilke og hvor omfattende tiltak man må sette inn og er villig til å akseptere. En respondent formulerte relevansen i trusselbevissthet og -kognisjon, ganske enkelt som:

«Jeg tror det er veldig viktig. Det er der ting starter, med trusselen.»

Samtidig handler det om å ikke sette inn sikkerhetstiltak for tiltakets skyld. Et intervjuobjekt snakket om «gammel trusselforståelse» om reisesikkerhet, som preget de ansette sin atferd på reiser, og gjorde dem mer bekymrede enn de behøvde. Derfor må trusselforståelsen være så «lokal» som mulig, formulerte et annet intervjuobjekt. Han reiser rundt og snakker med store organisasjoner, forretningskonserner og offentlige myndigheter, om sikkerhetskultur og sikkerhetsstyring. Hans mantra var:

«Jeg kan ikke fortelle dere hvor dere befinner dere her. Det må dere best vite selv. Dere må kjenne detaljene i virksomheten deres selv. Hvilke verdier dere har, hvilke kunder dere har, hvilke detaljer er med og påvirker. Har dere kontrakt i utlandet, alt det der. Jeg har ikke oversikt. Jeg kan gi dere et blikk og tanker om hvordan dere kan nærme dere det. Men dere må gjøre jobben selv.»

Respondenten mener derfor at trusselkognisjon må baseres på organisasjonens egne risikovurderinger og hva som er hensiktsmessig for den enkelte organisasjon. Et at intervjuobjektene formulerte viktigheten av bevissthet og felles tekning rundt trusler, på følgende måte:

«Og så kommer en liten kjepphest fra meg. At de ansatte får vite hva virksomheten utsettes for. Slik at de faktisk forstår nåsituasjonen (...) Men man fratar seg selv så utrolig mye, for å få alle med ombord og være med og slåss litt på vegne av arbeidsgiveren sin. For folk flest er jo både stolte av arbeidsgiver og merkevare og hva man leverer. Det er ikke bare lønn som driver mennesker. Så man fratar seg selv ganske mye omkring sånne ting om man ikke deler sånn type informasjon. Og det opplever jeg veldig fort på de spørsmålene jeg får fra både leder og andre når jeg er ute. At det tydeligvis ikke deles hva virksomhet utsettes for. De har ikke anelse om verdenssituasjonen, og enda mindre peiling på sin egen situasjon. Hva de faktisk rammes av.»

Medlemmene i en organisasjon må altså dele den samme kognisjonen eller virkelighetsoppfatningen – de samme grunnleggende antagelsene om trusler, for å skape en hensiktsmessig kulturell trusselbevissthet.

«For meg så er det den at vi har den greia på at de ansatte gjerne vil vite litt mer, på en måte få en indre/ytre motivasjon hvorfor det er riktig i denne situasjonen her og nå. At vi har en slik stakeholder-tilnærming. Det er jo også en glimrende anledning til faktisk å kunne forklare hvorfor vi gjør dette, og hvorfor vi må gjøre det. I stedet for å si at loven er loven og sånn må vi gjære det. Det gir en glimrende mulighet for dialog.»

Kort oppsummert, var alle objektene samstemte om viktigheten av en slik dimensjon.

«Jeg tror det er kjempeviktig men veldig vanskelig for mange der ute å forstå hva vi mener med det, Risiko, det skal man vel ikke akseptere. Det vil kreve litt opplæring av de du snakker med. Men helt klart at vi alle driver med det konstant. Jeg tror det er en kjempeviktig og interessant dimensjon på organisasjonsnivå, helt ned på team. Men at folk nok trenger å forstå hva vi mener med det.»

Respondenten mener altså at bevissthet rundt trusler krever aktiv innsats i en organisasjon. Men at det er nyttig å bevisstgjøre seg dimensjonen på alle nivå i en organisasjon.

Et intervjuobjekt knyttet dette opp mot grunnmotivasjonen for å drive sikkerhetsarbeid, og få folk til å følge sikkerhetsrutiner. Bevissthet eller forståelse av potensielle trusler mot dine verdier, vil begrunne et system, regelverk og prosedyrer, som ellers bare gir ulemper i hverdagen. Han understreket at det var snakk om det delte nivået av bevissthet. Og at det ikke er nok å tilegne seg faktakunnskap. Det er når kunnskap blir omsatt i aktiv handling, at man kan snakke om bevissthet eller kognisjon som objektet syntes var et bedre ord.

«Ja, så er det andre elementer av dette og det går på kognitivitet. Kognitiv tilnærming til dette for det går jo på at den enkelte analytiker eller organisasjonens ferdighet til å vurdere trusler og blant annet den boken tenke fort og sakte av Khaneman som vant Nobelprisen for adferdsmønstre og psykologi.»

Respondenten trekker her frem akkurat de mentale modellene som dimensjonerende for hvordan man kognitivt skaper mening rundt trusselbildet

Et intervjuobjekt stilte spørsmål ved om alle i en organisasjon bør dele en trusselbevissthet eller kognisjon. Han tenkte seg en matrise med roller, erfaringer, eksponering for ulike scenarioer osv. som dimensjonerende faktorer for hvem som bør ha hvilken grad av trusselbevissthet. Dette ble utfordret av en annen respondent som fremla følgende synspunkt:

«For det første må man i hvert fall forvente et nivå av bevissthet. En slags felles erkjennelse av at det er noen trusler og at vi dermed må fatte noen tiltak, og at de her er de tiltakene vi lander på.»

Respondenten fokuserte altså på det kollektive; felles bevissthet eller erkjennelse. Med andre ord de delte mentale modellene for hvordan man oppfatter trusler.

Oppsummert vurderer respondentene på dimensjonen som relevant og nyttig. Den må forankres i gjeldende og «lokale» trussel- og risikovurderinger, som engasjerer medlemmene og skaper forståelse. Og trusselbevissthet gjennom felles kognisjon, må deles på alle nivåer i en organisasjon. Selv om en respondent stiller spørsmål ved verdien av at alle skal ha den samme trusselbevisstheten, er den samlede trenden for en mest mulig kollektiv forståelse og delte mentale modeller for hva som er trusselbildet organisasjonen står i. Det trekkes frem av et av intervjuobjektene at det handler om mer enn hva vi vet om trusselbildet. Det handler også om hvordan vi tenker; vår kognisjon knyttet til trusseldimensjonen.

5.4.3. Risikoaksept

Intervjuobjektene ble så bedt om å reflektere rundt risikoaksept som en dimensjon innenfor sikkerhetskultur. Det var gjennomgående aksept for at dette er en viktig del av det sikkerhetskulturelle i en organisasjon, men at der var noen utfordringer.

Flere intervjuobjekter understreket at risikoaksept inkluderte både individuelle, psykologiske faktorer så vel som det kulturelle elementet. Individuelle premisser som forpliktelsesgrad og alder, ble trukket frem som relevante for hvor stor risiko en person er villig til å ta. I tillegg til psykologiske prosesser, trakk flere respondenter frem at dette også må sees i sammenheng med organisatoriske prosesser.

Flere av intervjuobjektene forklarte sin forståelse av dimensjonen gjennom å eksemplifisere forskjellene i hvordan organisasjoner forholder seg til risiko. Det ble referert til at noen ledere mangler innsikt og forståelse for sikkerhetsfaget, har ifølge et

intervjuobjekt, «gjemt» seg bak begrepet risikoaksept. I stedet for å gjøre faktisk sikkerhetsarbeid, så sier de bare at de aksepterer risikoen. Da forholder du deg egentlig ikke til risikoen, men bare «velger» å overse den. Flere objekter problematiserte en organisasjons evne til å vurdere og forstå risikobegrepet. Ikke alle gjennomfører risikoanalyser, og ikke alle forstår de sikkerhetsteoretiske modellene som skal beskrive risikoen etter f.eks. en risikovurdering. Reell kulturell risikoaksept handler derfor, ifølge intervjuobjektet, om den kollektive forståelsen av hvor mye risiko organisasjonen er villige til å ta. Et intervjuobjekt forklarte at dette var IT-sikkerhetsbransjens store utfordring. Ledere forstår ikke hvilke verdier en digital trusselaktør kan og vil ramme, og hvilke sårbarheter som kan utnyttes og hvordan. Men de har ringt en IT-konsulent og da må vel ting være ivaretatt.

«Men er det da organisasjonen som aksepterer eller er det «IT-duden»? Og de aller fleste virksomheter forstår ikke hva de gjør når de sier til «IT-duden» at dette fikser du. De aksepterer risikoen, men de forstår den ikke. Det er ikke en risiko for oss. Og hvis ikke de har den forståelsen, så mener jeg at de aksepterer de den på feil premisser.»

Dette ble forklart av en respondent ved at risiko er et vanskelig tilgjengelig begrep, og noe som krever forståelse for hva begrepet innebærer:

«Risiko i seg selv er et abstrakt begrep (...) Det er en ide som står opp mot andre ideer, og hvis jeg ikke forstår hva de står for, kan jeg ikke vite hva jeg aksepterer.»

Det ble trukket frem at organisasjoner aksepterer risiko, men på feil premisser, fordi de ikke forstår trusselen, sårbarheten eller verdien involvert. Risikoaksept skjer med andre ord, ikke nødvendigvis på et analytisk, faktabasert grunnlag, men basert på kulturelle antagelser. Men likevel aksepterer alle risiko i alle livets små og store avgjørelser. Et intervjuobjekt snakket om at «*enhver beslutning vi gjør er en form for risikovurdering. Hoppe ut foran trikken f.eks..*». Altså beskriver respondenten hvordan man har mentale modeller for å vurdere og akseptere risiko, selv om man ikke har et bevisst forhold til det. En respondent beskrev balansegangen mellom risiko sett på som trusler men også som muligheter:

«Slik jeg forstår begrepet, så betyr sikkerhet fravær av fare. Og så lenge du har en aktivitet, så kan du ikke unngå en viss form for risiko. Altså risiko betyr her både truslene, men det kan også bety muligheten. Så du har muligheten til å kunne styre det. Men du kan ikke ha fravær av noen av elementene, så lenge du driver med noe.»

Respondentene trakk frem skillet mellom det å se på risiko som noe utelukkende negativt og det å se på risiko som mulighetsvinduer for nyskapning, en sjanse til å ta markedsandeler eller til å ny verdiskaping.

Objektet viste til forskning som sa at ledere eller personer i administrative stillinger som forvalter andres verdier og ikke personlige verdier, er villigere til å ta høyere risiko. Eksterne entiteter uten eierskap til verdien, måloppnåelsen eller omdømmet, vil ikke føle på det samme ansvaret, og dermed akseptere høyere risiko.

«Ja, og ikke minst når vi kommer til dimensjonen knyttet til risikovillighet. Hvis du har eksterne entiteter, så vil de ikke nødvendigvis være inn i operasjonsplanleggingen din og være med å vekte. Så hvis du ikke har ansvaret

for det selv, men bare ansvar for måloppnåelsen, så vil du ha veldig sterke intensiver for å pushe fordi det er noen andre som ivaretar sikkerhetsaspektet, og de er ikke med her.»

Intervjuobjektet trekker her frem elementer som nærhet og eierskap til risiko, som deler av de mentale modellene som inngår i denne dimensjonen.

«Jeg tror for en organisasjon så handler det jo om å identifisere seg med oppdraget, ikke bare hva man gjør i vårt tilfelle, å regulere forskrifta om sikring av havneanlegg. Men hvorfor vi regulerer disse forskriftene?»

Respondenten sier her at risikoaksept handler om eierskap til oppdraget og bakgrunnen for at man utfører oppdraget, så vel som de konkrete verdiene til en organisasjon.

Oppsummert så viste respondentenes svar at risiko og hvordan vi forholder oss til og aksepterer restrisiko, er en naturlig del av all virksomhet. Men det å forstå hva risiko er og hvilken risiko vi lever med, er ikke nødvendigvis en bevisst aktivitet. Selv om det mangler en faglig forståelse av sikkerhetsarbeidets risikovurderingsdel, så forholder vi oss alle til risiko gjennom alle hverdagens beslutninger. Det kulturelle handler ifølge intervjuobjektene, i stor grad om man assosierer ordet risiko med noe positivt eller utelukkende med fare.

Ved å fokusere på hvilke mentale modeller som deles i en organisasjon knyttet til om risiko er utelukkende negativt eller også kan assosieres med utvikling eller muligheter, vil man kunne bevisstgjøre seg hva som er det reelle risikobildet og hva som er basert på ubevisste og kanskje feilaktige antagelser. Individuelle faktorer blant medlemmene som erfaring og kompetansenivå, og ikke minst den opplevde nærheten og eierskapet til verdier er trukket frem som elementer som virker innenfor denne dimensjonen.

5.4.4. Menneskesyn

Jeg forklarte intervjuobjektene menneskesynsdimensjonen med hvordan en organisasjon ser på sine medlemmer i et spekter fra trusler, sårbarheter eller garantister for sikkerheten, og bad dem reflektere rundt relevansen som en sikkerhetskulturell dimensjon. Det var en ganske omforent forståelse av denne dimensjonen som relevant. Et av intervjuobjektene konkretiserte denne dimensjonen med å trekke spekteret fra tillitt til kontroll.

Det var forskjeller i de grunnleggende antagelsene hos respondentene, på denne tematikken. Det ene intervjuobjektet uttrykte det på følgende måte:

«Trusselen er jo mennesker, tenker jeg da. Det er de ansatte. De er liksom den største resursen og den største trusselen vi har.»

På den ene siden kan man altså se på medlemmene som «det svakeste ledd», mens på den andre siden uttrykte en respondent at man også kan se på dem som «the last line of defence». Det var flere som hadde engasjert seg i det de så på som en tilnærming styrt av sikkerhetsbransjen, om mennesker som det svakeste ledd og den største sårbarheten i en organisasjon. Flere var provosert av denne tilnærmingen. En respondent slo fast at ansatte i en virksomhet er mennesker, og at mennesker kan ha sårbarheter som kan utnyttes av en trusselaktør:

«Du og jeg vet hva man gjør med trussel. De tas ut på en eller annen måte. Men du kan ikke snakke sånn om dine ansatte. Ansatte er mennesker. De har sårbarheter. Gjennom det er det risikoer. Og de kan utnyttes av trusselaktørene.»

Så jeg blir skremt når man setter i gang med å bruke en sånn terminologi. Og jeg tror bakgrunnen er rett og slett at man ser på trussel som ne mer sexy og spennende å snakke om enn risiko og sårbarheter. Som gjør at man tar noen sånne tabloide grep og snur dette på hodet.»

De fleste intervjuobjektene så på menneskelig feil som årsak til sikkerhetshendelser, som i bunn, en systemsvikt. Det ble trukket frem at det at mennesker mangler kompetanse til å følge prosedyrer, er organisasjonens sitt ansvar å utbedre. Det at mennesker kjenner til trusselen, og ikke eksponerer seg for situasjoner en trusselaktør kan utnytte, er også ansvaret til organisasjonen. En respondent uttrykte det slik:

«Men jeg tilnærmer meg slik at det var ikke den personen som gjorde en feil. Det var systemet vårt som tillot at dette kunne skje.»

Det kulturelle menneskesynet vil skape artefakter gjennom hvordan organisasjonen utøver sikkerhetsfaget, slik en respondent eksemplifiserte det:

«En annen ting er hvordan tar man imot nye ansatte, altså onboarding. Også på opplæring av sikkerhetsrutiner, regler, og atferdsdelen av det. Hvordan følger man opp ansatte over tid i forhold til alt fra å lære dem opp. Ikke bare phishing delen, men hvordan er kulturen i det at man bruke ressurser på å lære opp ansatte i nye verktøy, systemer, hele den greia der, vil også ha påvirkning i forhold til den totale sikkerhetsdelen av dette her da.»

De delte mentale modellene for hvordan man ser på sine medlemmer, vil altså ha praktiske konsekvenser for hvordan organisasjonen håndterer dem, helt fra de starter.

I tillegg ble det vektlagt, at menneskesyn er nært tilknyttet tillitt, og at tillitt i en organisasjon, går begge veier. En ting er å ha tillitt til sine medlemmer, en annen ting er at medlemmene har tillitt til sine ledere og sin sikkerhetsorganisasjon, til å melde fra dersom de har gjort noe feil, bevisst eller ubevisst. Trygghet på systemene innad i organisasjonen, og særlig oppover til ledelsen, på at man faktisk kan si ifra om sårbarheter eller feil hos en selv, og kanskje enda vanskeligere, å rapportere på en nær kollega og venn, ble av alle objektene trukket frem som betydningsfullt innenfor denne dimensjonen. Denne tillitsdimensjonen til egen ledelse eller eget sikkerhetssystem, ble beskrevet som veldig vanskelig og noe ledere ikke kan ta for gitt.

«Så må du kunne komme og si ifra uten at du blir kappet hodet av. For vår del er det slik at hvis du anses som ikke sikkerhetsmessig skikket, så mister du autorisasjonen og til syvende og sist jobben. Og det i seg selv gir jo alene et veldig sterkt insentiv til å ikke si ifra om en del avvik. Hvis du kan komme unna med det. Hvis du jobber for å finne insentiver og forsikringer til folk slik at de kommer med disse avviksmeldingene, by their own free will, uten å bli kappet hodet av, det er en interessant utfordring.»

Her illustrerer respondenten hvordan kulturen for tillitt i en organisasjon, påvirker hvordan man kan bevisstgjøre seg sårbarheter hos medlemmene. Han fremhever at tillitt til systemet vil kunne fungere som insentiver hos medlemmene, til å melde fra om noe i eget liv som kan utnyttes av en ekstern trusselaktør. Dette vil medføre at medlemmene opplever at den informasjonen man deler om egne feil og sårbarheter, blir behandlet på en saklig måte som ikke gir andre konsekvenser ut over det sikkerhetsmessige.

En annen respondent formulerte den samme nytteverdien på følgende måte ved å uttrykke at grunnleggende antagelser om menneskers sårbarhet og «sikkerhetsmessig egnethet», vil påvirke om man tør å rapportere om slike.:

«Ja, det dreier seg om det der «sikkerhetsmessig egna». Hvorfor skal du komme til meg og si fra om at du ikke har sovet på elleve døgn fordi du har kolikkbarnet, og vært hos legen og har fått sovepiller. Fordi det er en sårbarhet hos deg som kan medføre at den jobben du gjør, ikke blir like bra, eller at det vil være større sjanse for at du gjør feil, som igjen kan få større betydning for bedriftens ve og vel, litt avhengig av hvor du sitter.»

Det ble anmerket av et intervjuobjekt, at ekstremisituasjoner oppstår, hvor det er påkrevd å gå utenfor regler og normer for sikkerhetsatferd.

«For «in extremis» oppstår jo, altså situasjonen hvor man må gå på tvers av satte regler og normer for Security. Men da forventer jeg av mine, at de kan forklare hvorfor. Og er den grunnen god nok, og da er vi tilbake til det med då kappe hodet av de som melder fra, så er det et klapp på hodet i stedet for.»

Respondenten uttrykker her at har man etablert tillitt og forståelse hos sine medlemmer, så kan man håndtere slike hendelser og konsekvensene i ettertid. En formålstjenlig håndtering er kanskje påkrevd for å minimere skadefølger, og da må medlemmer kunne gå utenfor prosedyrer uten at det får negative konsekvenser.

«Det er i hvert fall sikkert at hvis folk ikke opplever at de har noen grad av tillitt, er sannsynligheten for at de kjøper sikkerhetskulturen sammen med andre kulturelle trekk i din organisasjon, den synker ganske dramatisk. (...) Hvis de blir gitt tillitt, så har veldig mange mennesker, en tendens til å være mer ansvarlige. Mens andre faller helt gjennom. På den andre siden så, som hos oss, vi har ikke lov til å unngå kontroll. Kontroll er jo en sikkerhetsmekanisme.»

Respondenten viser her at tillitt fra organisasjonen vil ansvarliggjøre enkeltmedlemmene. Men at samtidig må det finnes kontrollmekanismer og at disse må balanseres.

Oppsummert knyttes intervjuobjektene forståelse seg til hvorvidt mennesker sees på som en potensiell trussel eller «det svakeste» ledd, eller om man har tillitt til at medlemmene kan håndtere situasjoner basert på egne evner. Tillitsaspektet ble fremhevet som noe som går både fra ledelse og system ned til medlemmene, men også fra medlemmene og til systemet. Et system forankret i et positivt menneskesyn, vil dermed medføre at medlemmer stoler på at systemet vil behandle rapportering om egne og andres sårbarheter, på en god måte. Men tillitt betyr ikke det samme som at man ikke parallelt utfører kontroller.

5.4.5. Relasjoner/konfliktaksept

Den siste dimensjonen handler om vektlegging av relasjoner og aksept for konflikter, som grunnleggende antagelser delt i en organisasjon, kan være dimensjonerende for sikkerhetskulturen. Det gikk igjen hos alle intervjuobjektene at de forstod denne dimensjonen som nærhet i relasjoner og hvordan relasjoner påvirker yrings- og tilbakemeldingsklimaet i en organisasjon.

Relasjonsdimensjonen ble understreket av flere intervjuobjekter, som viktig for sikkerhetskulturen. Som et av intervjuobjektene formulerte det kort og konsist:

«Alt i alt kan man si at totalt sett, skal man ikke undervurdere et godt arbeidsmiljø som et veldig godt sikkerhetstiltak.»

Det ble av to intervjuobjekter referert til kulturen i norske spesialstyrker, for å gi tilbakemeldinger og korrigere hverandre på en veldig konkret og direkte og «ekstremt røff» måte. Men i dette ligger en felles forståelse av at dette gjøres for å ta vare på hverandre og å oppnå organisasjonens formål. Intervjuobjektene knyttet denne dimensjonen tett opp til arbeidsmiljø og psykologisk trygghet. Det forstås som at nærhet i relasjoner og ytringsklima er en del av denne dimensjonen.

Det ble formulert av en respondent, som at hvis du som leder er bekymret for å gå i dialog eller i en konfrontasjon, da legger du opp til at det skal bli alternative mentale modeller for hvordan ting skal være hos oss. En leder må med andre ord selv praktiskere den relasjonsformen, den tillitten og kontrollen han ønsker at være kulturen i organisasjonen. Men samtidig hvis hver gang du oppdager et avvik, så blir det negativ kommunikasjon og konflikter, så kan man oppleve dette som hemmende på avviksrapportering, eksemplifiserte det ene intervjuobjektet.

I dette ligger bruken og forståelsen av avviksrapportering i en organisasjon sentralt. Blir det sett på som noe positivt, et erfaringsregister, en metode for å utvikle organisasjonen, eller blir det sett på som en «svarteliste» der det føles negativt og skamfullt å registreres.

«Bevisstheten rundt dette med å skrive avviksmeldinger er kanskje like viktig for å ha en kultur i bunn, som bare det at vi skal ha et styringssystem alene. Det skal være med på å forme hvordan vi tenker, hvordan vi samarbeider på det som identifiserer oss som en avdeling. Så det er på en måte status, der vi er nå.»

Et av intervjuobjektene i lederstilling, oppmuntret til det han kalte «konstruktiv uenighet». Han ønsket ikke et ekkokammer av det de var selvtilfredse med. Han ønsket å utøve tillitsbasert ledelse, der leder peker ut en retning, men at den enkelte har ganske stor grad av frihet til å velge veien fremover. Det han kalte sosial trygghet, så han på som en forutsetning for å kunne optimalisere ressursene i sin avdeling. Når det gjaldt avvikshåndtering, var han alltid årsaksfokuseret.

«Jeg vil gjerne ha en kultur dersom noen ser at en annen gjør noe feil, at vi skriver en avviksmelding på hverandre. Men at vi opplever dette som positivt. Takk for at du hjelper meg. Takk for at du påpeker feilen jeg gjør så jeg kan bli flinkere mens. Men jeg tilnærmer meg slik at det var ikke den personen som gjorde en feil. Det var systemet vårt som tillot at dette kunne skje.»

Med dette ønsket respondenten å ufarliggjøre det at man er sårbare og feilbarlige som mennesker, og gjøre det til noe konstruktivt som man kan bruke til å utvikle og forbedre seg. Dette er nært knyttet til menneskesynsdimensjonen, og begge aspektene er knyttet til tillitt. Men her skal sitatet eksemplifisere ytringsklimaet for å kunne si ifra, mer en tilliten til systemet som skal håndtere det.

Tilliten til systemet som skal ta imot avviksmeldinger eller andre meningsytringer, ble også trukket frem av en av de andre respondentene:

«Og det siste jeg har er ekstremt viktig, ikke minst fokuset på når vi begynner å snakke om sikkerhetsgraderte ting, personellsikkerhet osv., at det eksisterer et miljø og en trygghet der man føler at man kan gå og melde fra og rapportere ting,

sågar rapportere på seg selv om ting som kan være negativt, men at det er faktisk et miljø til å gjøre det.»

Respondenten bruker begrepet «miljø», men kunne benyttet kultur for å beskrive de delte modellene for relasjoner og konfliktaksept som skapertrygge rammer.

Relasjonsdimensjonen ble oppsummert av intervjuobjektet som jobbet med personellsikkerhet, på en argumentasjon for at nære relasjoner kan være en del av en hensiktsmessig sikkerhetskultur:

«Og det jeg vil at folk skal bli flinkere til, er å bli kjent med kollegaene sine, sånn at hvis det skjer noe så kan de se det. Og kanskje vi klarer å ta det i starten i stedet for å komme etter med kost og brett. Vi burde ha sett det vi burde ha sagt noe, vi burde ha skjønt det.»

Men et av intervjuobjektene problematiserte også for nære relasjoner, og reflekterte rundt at det kan skape subkulturer med egne lojaliteter som kommer i konflikt med organisasjonens formål og verdier. Der relasjoner blir veldig viktige, kan også avviksregistrering oppleves som negative for relasjonene. Man unnlater derfor å si ifra på grunn av lojalitet til en kollega, eller for å bevare de gode relasjonene innad i et kollegium.

«Hvis det er for tett miljø, og for åpent, så kan også det innebære at en utvikler en egen kultur med en egen lojalitet. Hvis kollegaene og jeg er bestevenner, og kollegaen min dummer seg ut eller bevisst gjør det. Det har jeg vært bort i mange ganger det det har fått lov å gå for lang tid. Men du gjør ikke noe med det, fordi dere kjenner hverandre. Så til slutt melder jeg ifra, men da er det for seint, da har skaden allerede skjedd.»

Dette sitatet formulerer viktigheten av bevissthet rundt relasjonsdimensjonen, og den effekten relasjonelle forhold og de kulturtrekkene som påvirker disse, kan ha på den totale sikkerheten.

De mentale modellene som skaper mening rundt de interne relasjonene i en organisasjon, vurderes altså av intervjuobjektene som relevante. Psykologisk trygghet til å si ifra, men også det generelle arbeidsmiljøet er vurdert som relevant av respondentene. Flere trekker frem hvordan dette synliggjøres gjennom spesielt avviksrapportering, men også i det generelle ytringsklimaet i en organisasjon. Graden av nærhet i relasjoner innad i organisasjoner, er et element som trekkes frem, der nærhet kan skape trygghet og godt kommunikasjonsklima, men at veldig nære relasjoner kan gjøre det vanskeligere å si ifra eller melde avvik på andre.

5.5. Hva er særlige utfordringer med sikkerhetsfaget?

Sikkerhet som fag, både teorier og modeller, og praksis i utøvelse på både operativt nivå og som ledelse, har noen særegenheter som gikk igjen i refleksjonene til flere av intervjuobjektene. Disse forholdene kom frem i intervjuobjektene refleksjoner og ble identifisert under analysen av empirien, som relevante for denne oppgaven. Disse utfordringene og særegenhetene vil drøftes videre i oppgavens drøftingsdel som grunnlag for kulturens relevans i sikkerhetsarbeid. Disse utfordringene som synliggjør viktigheten av de kulturelle mekanismene i en organisasjon i et sikkerhetsperspektiv, kan oppsummeres i tre overskrifter:

- Lav frekvens på hendelser skaper et abstrakt risikobilde som det er vanskelig å begrunne sikkerhetsarbeid ut fra.
- Sikkerhet lar seg vanskelig måle
- Sikkerhet vil alltid stå i et motsetningsforhold til produksjon eller annen måloppnåelse

5.5.1. Det abstrakte risikobildet:

Det første elementet som gikk igjen i flere av intervjuene, var at det er vanskelig å basere sikkerhetsanalyser, både trussel- og risikovurderinger, på statistiske data. Skillet mellom sikkerhetshendelser, forstått som bevisste handlinger utført av ondsinnede aktører som vil ramme organisasjoners verdier, og *Safety* forstått som uintenderte, tilfeldige uønskede hendelser, ble trukket frem av alle intervjuobjektene. Sammenlignet med *Safety*-hendelser er det veldig få sikkerhetshendelser å basere analysene på. Det er nevnt fra intervjuobjektene at det f.eks. er svært lav frekvens på antall terrorhendelser, men konsekvensene av slike angrep er så høyt at man må forholde seg til dem og vurdere disse. Det eneste unntaket, bemerker det ene intervjuobjektet, er digitale angrep, som det er svært mye empiri rundt fra de siste årene.

Intervjuobjektet fra etterretningstjenesten, viser videre til at en del sikkerhetshendelser aldri blir kjent for den som blir angrepet:

«Det er ingen tvil om at en sentral utfordring er at man må forvente, i hvert fall mot oss, at en del av aktørene som jobber mot oss er så kompetente at de ikke blir tatt - veldig enkelt. Det gjør at vi ikke har så mye empiri å vise til.»

Respondenten viser her hvordan en sikkerhetstrussel kan forekomme uten at man får informasjon om det som kan benyttes til å forebygge fremtidige lignende hendelser.

Sikkerhetshendelser som ligger til grunn for risikovurderinger, blir derfor i stor grad konstruerte størrelser, ikke konkrete erfaringer. Sammenlignet igjen med *Safety*, så bemerket intervjuobjektene at innenfor *Safety* kan man relatere til konkrete erfaringer så vel som relativt hyppige hendelser. Igjen er unntaket digital sikkerhet der det forekommer stadig hyppigere sikkerhetshendelser og i alle typer virksomheter og organisasjoner. Et intervjuobjekt eksemplifiserte forskjellen på *Safety* og sikkerhet og måten man forholder seg til empiri for risikovurderinger, på følgende måte:

*«Altså, når en mann detter ned fra en oljeplattform fordi det ikke var et gjerde der, så setter de opp et gjerde her, så unngår vi at det skjer igjen. Det er litt som «Darwin Awards». Får du noe i hue når du går på jobb, så tar du på deg hjelm. Så slipper du å få hjerneskode. Det er veldig konkret og veldig intuitivt, særlig for nye, som kommer inn i anleggsbransjen, for å bruke det som en greie: Her gjør vi det sånn, og da gjør vi det da.(...) Det er så basic, og du ser du på alle byggeplasser du skal inn på. Så er det en plakat med piktogrammer, med bilde av en hjelm på med bilde av kanskje dynamitt, eksplosjon og så videre. Her er det farlige ting. Det er ingen som blir fornærma. Det er det en vanesak. De blir påvirket av det hele tida, og de ser en direkte konsekvens dersom noen ikke gjør det. Det er fordelene *Safety* har. Her ser vi ikke en konsekvens hvis en eller annen går uten kort. De snakker om, ikke nødvendigvis graderte ting etter sikkerhetsloven, men hemmeligheter som at oljefondet skal merge med ett eller annet firma. Så sitter de i kantina og prate om det som om alle her ville dem godt. Det blir veldig sånn naivt. Men vi ser ikke konsekvensene av feil som ble gjort, eller ting som skjer fordi det er ikke noen kultur for å fange det opp.»*

Respondenten uttrykker altså at en *Safety*-trussel er enklere å forholde seg til, enn en sikkerhetstrussel, fordi førstnevnte er lettere å forstå og mer konkret i sin form og i sine konsekvenser.

Dette forsterkes av en annen respondens sine betraktninger rundt digital sikkerhet som en del av informasjonssikkerhet, og hvordan informasjon er en abstrakt størrelse:

«Informasjon er abstrakt, mens i den virkelige verden når vi snakker om Safety-biten av dette her, så er det veldig til stede – veldig lite abstrakt. Ramler denne steinen her ned og treffer deg i hodet så er det veldig konkret, ikke abstrakt. Blåser denne oljebrønnen ut så er ikke det abstrakt i det hele tatt. Mens informasjon; nummer en: Det er abstrakt selv om du har det på en papirbit, selv om den er fysisk, de tingene du skriver der er til en viss grad fysiske, det er noe blekk og sånt. Men det er ikke verdien. Verdien er der når du leser det og behandler det på et eller annet vis.»

Respondenten beskriver altså at selv om det skrives på papir med blekk, eller lagres som 0 og 1 i et datasystem, så er verdien i informasjon, det som skjer når den gjøres kjent for mennesker. Dette gjør både verdien, sårbarhetene og truslene til abstrakte størrelser som det ikke er lett å forholde seg til.

Når sikkerhet er arbeid for å hindre noe tilnærmet en abstrakt størrelse, noe vi ikke ser for oss skal skje, eller som vi mangler empiri på har skjedd tidligere, blir analyser og vurderinger gjort med en stor grad av usikkerhet. Et intervjuobjekt kaller dette stor spredning i subjektiv usikkerhet.

«Med subjektiv sannsynlighet mener jeg at det finnes ikke en objektiv sannhet. Du kan ikke si at en pluss en er lik to når det gjelder faren for terrorisme. Og hvis ikke det finnes en objektiv sannhet, så kan det heller ikke finnes en subjektiv sannhet. Du har ikke rett, og jeg har ikke rett. Det eneste vi kan vite, det er vår subjektive usikkerhet. Vi må beskrive vår organisasjon eller det enkelte saksbehandlers grad av usikkerhet knyttet til detaljer, som f.eks. de åpne trusselvurderingene prøver å angi med ulike sannsynlighetsord, hvordan de tror faren for at noe skal skje. Og det legger et ganske stor det ansvar på oss i forhold til blant annet verktøyene vi har, som de åpner trusselvurderingene.»

Respondenten beskriver altså at det er vanskelig å utlede objektive faktabaserte vurderinger av abstrakte, subjektive input, som er det man faktisk må gjøre i vurderinger av sikkerhetsrisiko.

Den neste, men nært beslektede utfordringen med sikkerhetsfaget, er at gitt den lave frekvensen hendelser og de nærmest abstrakte truslene, så er det vanskelig å rettfærdiggjøre sikkerhetstiltak som oppleves som hemmende på effektivitet og til hinder i daglig drift. Fysiske sikkerhetstiltak som krever kort og koder for å komme fra A til B, tilgangsbegrensninger på informasjon eller systemer slik at man ikke kan jobbe hjemmefra, å måtte legge fra seg mobiltelefoner og smart-klokker utenfor gitte soner, alle disse eksemplene som intervjuobjektene kom med, kan være med å gjøre arbeidshverdagen vanskeligere og å gjøre det vanskeligere å oppnå de formålene som er grunnen til at du er ansatt i den jobben du har.

Det bemerkes fra flere av intervjuobjektene at det derfor er vanskelig å skape forståelse hos medlemmene i organisasjoner som igjen skaper etterlevelse av de sikkerhetsregler

og prosedyrer som er vedtatt. Et intervjuobjekt bemerket hvor vanskelig det var å legitimere personellsikkerhetsmessige tiltak, kontra de digitale sikkerhetsprosedyrene:

«(...) det er ingen som går til IKT og sier at det passer meg dårlig at jeg må taste inn 28 bokstaver og 15 tall i passet mitt. Kan jeg få slippe det? Men det hører du aldri. Men det å henge på seg et kort rundt halsen for enkelt det er jævlig vanskelig, og det vil vi gjerne krangle på, og det vil vi gjerne liksom opponere mot. Sikkerhet blir så flytende.»

Respondenten sier altså at det er vanskelig å legitimere sikkerhetstiltak, når bakgrunnen blir «flytende» eller abstrakt slik det ble beskrevet tidligere. Det ble derfor vektlagt av flere intervjuobjekter, at det må eksistere en forståelse for hvorfor sikkerhetstiltak er vedtatt:

«Så må folk til enhver tid forstå hvorfor. Hvorfor skal vi gjøre dette her. Hvorfor skal vi ikke gjøre sånn. Hvis dette her «vi er nødt å gjøre sånn» ikke følges av et «fordi», da mister du folk veldig fort. Jeg tror det er begynnelsen på en kultur. At du klarer å så fast at sånn er det, fordi. Sånn er det bare hos oss, fordi... Sånn at dette «fordi vi vil unngå», at det blir en veldig klar og åpenbar greie. Da er det ikke bare en regel du bryter. Da er det på en måte hvorfor den regelen er der.»

Respondenten beskriver altså et behov for å legitimere sikkerhetstiltak, gjennom å skape en forståelse av hva tiltaket skal forebygge.

5.5.2. Sikkerhetens målbarhet

Det ble tatt opp av flere intervjuobjekt at sikkerhet ikke er målbar. Dette ble eksemplifisert av respondentene ved at om man ikke har hatt sikkerhetshendelser, så betyr det ikke at sikkerhetsarbeidet fungerer slik det skal.

«Så det er egentlig slik at «alt er grønt» selv om alle vet at det ikke er grønt? Men det ser veldig bra ut om du skal levere fra deg en rapport, eller stå i «rett» foran styret og kan si «ja, her er allting bra».

Respondenten beskriver her at ingen hendelser, ikke nødvendigvis betyr god sikkerhet. Det kan like gjerne bety at man ikke har verdier som en trusselaktør er ute etter. Det kan bety at trusselaktøren mangler kapasiteter eller intensjon til å ramme deg og dine verdier. Eller det kan bety at du ikke har oppdaget at du er angrepet, som et tidligere sitat beskriver. Dette gjør det vanskelig å for ledere som skal rapportere og stå til ansvar for målbare enheter som produksjon og drift og økonomi. Og fravær av hendelser fordrer et system som fanger opp sikkerhetshendelser, og hvor man har det, betyr ikke det at alle bruker det eller bruker det slik det er tenkt.

Dette problemet blir synlig på alle nivåer i en organisasjon, helt opp på ledelsesnivået:

«Det er litt sånn at jeg har møtt ledere som sier at jeg måles ikke på sikkerhet, så det er ikke så interessant for meg. Og så har man da en bransje som respondere på det, som sier at da må vi begynne å måle ledere på sikkerhet. Jeg har vært en av de som er ganske uenig i det. For jeg sier at det er ikke hensikten. For sikkerhet i seg selv er ikke målet. Det du skal være flink til å gjøre, er å ta de tingene en leder måles på og så skal du kunne argumentere hvor sikkerhet kommer til å påvirke de målene eller ikke. Dersom man trår feil, får en hendelse eller ikke. Der hvor man forstår at sikkerhet er grunnleggende og kommer til å få en rolle.»

Respondenten beskriver altså at sikkerhet ikke kan eller bør måles alene, men heller som en del av måloppnåelsen eller resultatkrav for organisasjonenes definerte formål.

Respondenten forklarer at dette har medført at innenfor sikkerhetsbransjen er det nå aktører som ønsker å tilby denne typen målinger. Spørsmålet er om det er riktig tilnærming. For som sitatet over sier så er sikkerhet i seg selv, ikke målet. Respondenten forklarte at det en leder skal være flink til å gjøre, er å ta de elementene som en leder måles på, og så klare og se hvor sikkerhet kommer til å påvirke de målene. F.eks. hvorvidt en sikkerhetshendelse vil kunne påvirke produksjonen, eller mulighetene til å inngå en kontrakt.

5.5.3. Sikkerhetens konkurranse med annen måloppnåelse

På den andre siden vil sikkerhet påvirke produksjon, og ofte stå i et motsetningsforhold til produksjon eller annen måloppnåelse:

«Hvis du maksimerer sikkerhet, så vil du på et tidspunkt ikke klare å gjøre noe av det andre. Så sikkerhet er en basisfunksjon som du må ha som en plattform for alt det andre du gjør. Men hvis den blir for total, hvis du makser det for mye, så vil det gå ut over alt det andre du gjør. Så å finne balansen mellom hensiktsmessig sikkerhet, juridisk bindende, legal, forvente og hensiktsmessig sikkerhet, det er en ganske sentral ledelsesoppgave. Å klare å manøvrere sånn at vi ikke ender opp med å ha så mye at det går ut over det vi driver med. Men heller ikke så lite at vi risikerer at alt blir for ingenting.»

Respondenten forklarer at det er en balanse mellom å redusere risiko, og hvordan sikkerhetstiltak påvirker produksjon eller annen måloppnåelse. En annen respondent uttrykte god sikkerhetskultur som noe som skjer i samspillet med virksomheten eller organisasjonens utvikling.

«At virksomheten bevisst eller ubevisst har en kontinuerlig utvikling og diskusjon og prosesser knyttet til trusler, sårbarhet eller risiko, etter hvert som virksomheten utvikler seg. At de har en helt klar tanke om at den nye kunden som vi akkurat har fått kontrakt med nå, den endrer trussel og risikobildet vårt i betydelig grad. Og at det noe som nærmest skjer neste automatisk, er illustrasjonen på en god kultur. Hvor det er forstått at sikkerhet ikke er noe statisk.»

Men når sikkerheten kommer i konflikt med den daglige driften i virksomheten, vil dette virke kontraproduktivt, både på måloppnåelsen, men også på hvordan sikkerhetsarbeidet oppfattes. En respondent eksemplifiserte det ved å beskrive hvordan sikkerhetspersonell oppfattes enkelte steder:

«Man bor bak stengte dører i kjelleren, og dukker opp en gang iblant og er bare sur og pålegger folk en masse forskjellige ting som man selv ikke er i stand til å forklare hvorfor man trenger, og som bare vanskeliggjør hverdagen deres.»

Et annet intervjuobjekt delte den samme erfaringen av hvordan sikkerhetspersonell ble oppfattet:

«Og jeg har også en slik arv; at sikkerhet skal være så jævla hemmelig og vanskelig og tungvint og gnagsår. Bare vi sier trynet vårt, så går folk i ring rundt oss.»

Et intervjuobjekt begrunnet denne konflikten mellom sikkerhets og måloppnåelse, med et manglende helhetsbilde:

«Det er den samme diskusjonen man setter i gang, om kan Forsvarsansatte eller folk i sensitive stillinger, kjøpe en kinesiskprodusert smart-bil. Jeg syns det er en håpløs diskusjon, for det er helt uvesentlig om den bilen er produsert i Kina, USA eller i Tyskland. Problemet er teknologien som er i den bilen og hvordan den kan misbrukes. Det er det vi må forholde oss til, og det er det vi må finne tiltakene mot. For jeg har ikke tenkt å tillate den amerikanske bilen en meter nærmere sensitiv informasjon, enn jeg har den kinesiske. Så vi løper etter det ene produktet, ene problemet, så glemmer vi litt helhetsbildet ved å se risikoen vi faktisk tar.»

Oppsummert så trekker intervjuobjektene frem at sikkerhet kan oppfattes som å stå i direkte konkurranse med produksjon, drift eller organisasjonens måloppnåelse. Til en viss grad er dette riktig, men det handler også om hvordan sikkerhetsarbeid oppfattes; hva som er de grunnleggende antagelsene om dette arbeidet. Dette handler om hvordan sikkerhetsarbeid presenteres, blant annet av sikkerhetspersonelle, men også fra ledelsens side. Og det det handler om hvordan man helhetlig vurderer sikkerhet som en av flere faktorer i et totalt bilde av organisasjonens formål.

6. Drøfting

Det teoretiske grunnlaget satt opp mot den empirien som er innhentet i denne oppgaven, danner utgangspunkt for drøftingen for å besvare studiens problemstilling:

Hvordan kan man tilnærme seg sikkerhetskultur på en teoretisk og analytisk måte, for å skape «tykke», kvalitative, fortolkende beskrivelser som igjen kan benyttes til endrings- og utviklingsarbeid?

Jeg vil i denne drøftingen først ta for meg sikkerhetsfagets særegenheter som gjør at de kulturelle aspektene er relevante å drøfte innenfor dette dagfeltet. Jeg vil deretter drøfte hvordan man bør forholde seg til sikkerhetskultur gjennom en fortolkende tilnærming, men likevel kunne vurdere det kulturelle ut fra hva som er hensiktsmessig for sikkerheten i forskjellige organisasjoner.

Deretter vil oppgaven redegjøre og forklare de identifiserte sikkerhetskulturelle dimensjonene ut fra intervjuobjektene reflekser rundt disse, som et begrepsapparat og en fortolkningsmetode for å kartlegge, bevisstgjøre seg og vurdere nettopp denne hensiktsmessigheten.

Drøftingen vil deretter ta for seg hvordan ledere kan benytte seg av disse dimensjonene i en slik analyse, og hvordan ledere kan jobbe aktivt med å påvirke og utvikle sikkerhetskultur i en hensiktsmessig retning for best mulig å kunne oppnå organisasjonenes formål.

6.1. Sikkerhetsfagets kulturelle utfordringer

For å kunne drøfte sikkerhetskultur som en del av organisasjonskulturen, er det en nyttig øvelse å forsøke skille ut de faktorene innen sikkerhet i en organisasjon, som ikke er kulturelle – det denne oppgaven har definert som sikkerhetskultur. Schifloe (2021) har utarbeidet en modell for organisasjonsanalyse, som sammenfatter de organisatoriske elementene i fem hoveddeler. Denne modellen kaller han pentagonmodellen.

De to første elementene kaller han formelle og materielle strukturer. Dette er de aspektene ved en organisasjon, som ledelsen kan beslutte og betale for, og er den administrative, formelle management-delen av en organisasjon. De formelle strukturene innen sikring, vil være spennet fra risikovurderinger, etablering av policyer, compliance-krav, formelt nedfelte roller og funksjoner knyttet til sikkerhet, etablering av et sikkerhetssystem og en sikkerhetsorganisasjon osv. Dette kan ledelsen vedta og formulere i skriftlige retningslinjer og styringsdokumenter.

I tillegg har man de materielle strukturene, beskrevet spesielt i oppgavens del om fysisk sikkerhet; det fysiske sikkerhetsutstyret inkludert teknologi og lokaliteter, gjerder og porter, datasystemer, programvare, overvåkingssystem osv., som bidrar til sikkerhetsarbeidet.

De andre elementene i pentagonmodellen kan ikke besluttes av en sjef eller en ledergruppe, men må forhandles frem gjennom uformelle prosesser, i samspill med medlemmene i organisasjonen. Den første av disse er arbeidsprosessene; hvordan man arbeider og samhandler; den faktiske praksisen som ikke er den samme som de nedskrevne prosedyrene. Her snakker vi om sikkerhetsatferd; i hvilken grad regler og retningslinjer følges, sikkerhetssystem brukes etter hensikten, eller om man tar «snarveier» og lurer systemet og barrierene.

Deretter kommer relasjonene; det sosiale nettverket, knytningene mellom personer og grupper som ikke følger et organisasjonskart, et arbeidsflytdiagram eller prosedyrer. Hvem har påvirkningskraft, hvem styrer normene, hvilke konstellasjoner av medlemmer eller grupper fungerer godt eller dårlig? Er det tillitt til systemet og ledere som skal behandle avvik i sikkerheten eller adressere sårbarheter hos enkeltmedlemmer eller grupper?

Den siste siden i Schifloes pentagondiagram, er det organisasjonskulturelle. Dette er noe annet det formelle og det materielle, men også noe ut over arbeidspraksis og sosiale relasjoner. Alle sidene i modellen påvirker hverandre gjensidig. En organisasjons struktur og policyer vil kunne påvirke kulturen og hvordan denne utvikler seg. Det samme vil de materielle arbeidsbetingelsene; altså de fysiske mulighetene og begrensningene.

Respondentene i denne oppgaven var samstemte i at kultur spiller inn på hvordan ledelse utøves og dermed sikkerhetsstyringen i en organisasjon; hvordan en organisasjon prioriterer sikkerhetsarbeid og vektlegger risikovurderinger. Kultur vil påvirke hva man prioriterer ved innkjøp av f.eks. fysisk sikkerhetsutstyr, hvordan man jobber, og hvordan medlemmer i organisasjonen forholder seg til hverandre.

Schifloes modell er relevant og et nyttig verktøy for å identifisere drivere i en organisasjons tilstand og utvikling, men kan oppfattes som å inkludere et skarpt analytisk skille mellom kultur og de øvrige dimensjonene. Det modellen illustrerer godt, er at kultur ikke kan besluttes på et ledermøte, eller kjøpes for penger, ei heller beskrives i en oppgaveprosedyre. Den blir til i det uformelle samspillet presentert som sensemaking og organisatorisk læring.

Men siden det kulturelle er en viktig del av sikkerhetsarbeidet, viser empirien utvetydig at en leder må forholde seg til og ta ansvar for også dette aspektet og de utfordringene som er trukket frem av intervjuobjektene i denne oppgaven. Den videre drøftingen vil vise hvordan kultur påvirker de øvrige sidene i pentagonmodellen, og den vil vise hvordan en leder gjennom både lederskap og formelle strukturer, kan i sin tur påvirke kulturen.

6.1.1. Sannsynlighet og trusselvurderinger som premiss for grunnleggende antagelser

Det er i empirien fremhevet den særlige forskjellen mellom sikkerhet og *Safety*, ved at risikoen for *Safety*-hendelser i større grad kan beregnes, mens sikkerhetsrisikoen er avhengig av en menneskelig faktor som er vanskeligere eller umulig å kvantifisere. Dette er et gjentagende tema i flere av intervjuene, og et av hovedpoengene fra den empiriske analysen.

Sikkerhet slik denne oppgaven definerer det, står i et motsetningsforhold til *Safety*. Selv om begge begrep handler om å unngå uønskede hendelser, så er *Safety* knyttet opp mot mye mer konkrete og håndfaste eksempler og dermed lettere å forholde seg til. Som intervjuobjektene har eksemplifisert: Hvorfor man skal bruke hjelm, vernesko og synlighetstøy på en anleggsplass, trenger ingen forklaring. Hvorfor man må autoriseres for adgang og etterpå bruke kort og kode for å komme inn på denne anleggsplassen, er ikke like lett å forstå og akseptere. Både sikkerhet og *Safety* gjør ofte arbeidsprosesser, forflytning og andre deler av driften, mer tungvint og mindre effektiv. Og det er i det det ligger en utfordring hvis man ikke forstår hensikten bak dette forsinkende tiltaket. Her ligger det en sårbarhet hvis da medarbeidere omgår tiltakene, tar «snarveier» eller rett og slett motarbeider dem, fordi de ikke ser hensikten med dem.

«Å ta risikobaserte beslutninger er subjektivt» (Dillon et al., 2009, Risk Analysis 29 (3) 321–335). Utfordringene med å begrunne sikkerhetstiltak ligger ofte i den lave frekvensen sikkerhetshendelser, og igjen ofte sammenlignet med uønskede *Safety*-hendelser. I vurderinger eller analyser med et *Safety*-fokus, benyttes i stor grad kvantitative metoder, hvor en beregner risiko ut fra et statistisk tallmateriale og analyserer og vurderer sannsynlighet og konsekvens. Som det bemerkes i empirien, har de fleste sikkerhetstrusler har en lavere frekvens og det foreligger dermed et mindre statistisk tallmateriale å analysere denne ut fra. Sannsynlighet blir da mindre egnet, og risiko identifiseres og analysert helles basert på vurderinger av konsekvenser, sårbarheter og målets attraksjon (Reniers et al., 2011).

Kvantitativ sannsynlighet betyr at man har tilstrekkelig med data til å utføre numeriske beregninger og komme fram til et numerisk uttrykk for sannsynlighet for at en hendelse kan inntreffe. Men der det ikke er tilstrekkelig data for å kunne regne seg frem til en slik numerisk verdi, kan man benytte kvalitativ sannsynlighet. Det betyr at man baserer seg på kunnskap og skjønn, studerer begreper og egenskaper og trekker slutninger ut fra disse elementene. Sannsynlighet må da beskrives med ord og formuleringer, kontra matematiske formler og prosenter. En slik beskrivelse kalles semantisk sannsynlighet (Busmundrud, 2019).

PST benytter seg av denne type semantisk sannsynlighetsforklaring, i sine årlige trusselvurderinger. De bruker vi et sett med standardiserte sannsynlighetsord med formål å skape en mer ensartet beskrivelse av sannsynlighet i vurderingene og derigjennom redusere uklarhet og misforståelser. Begrepene og de tilhørende beskrivelsene av begrepenes betydning er utarbeidet i et samarbeid mellom politiet, PST og Forsvaret (PST, NTV 2023).

Sannsynlighetsordene som benyttes, som f.eks. «mulig», «sannsynlig» og med støtteord som «svært lite» eller «meget», kan naturlig forstås ulikt, både internt og eksternt. Konfidens er annet moment som enkelt forklart er kvaliteten på vurderingen, ut fra antall kilder og uavhengighet mellom disse. Selv om en ensartet og konsekvent bruk av en enkel, forståelig og visuell matrise, slik den benyttes i Norge i dag, på sikt vil kunne bedre diskursen og redusere usikkerhet knyttet til trusselkommunikasjonen, er det likevel mye rom for individuell oppfatning og tolkning. Det kan kobles til epistemologi – vår egen holdning, ståsted, vurdering, overbevisning, bakgrunn, utdanning, og så videre (Røhjell, 2022). Men hvilken forståelse skaper slik semantisk sannsynlighetsberegning i en kultur?

Enklere sagt kan man si noe om risikoen for at et tau skal ryke ut fra undersøkelser og analyser av tauets styrke, slitasjepunkter og ytre faktorer som påvirker slitasjen. Det er ikke relevant å vurdere friksjonens intensjoner, eller verdien av det tauet holder oppe. En sikkerhetsrisiko vil på sin side være avhengig av hva f.eks. en terrorist ønsker å oppnå og hvordan han rasjonaliserer sin målsetning og hva han er villig til å gjøre for å oppnå dette. Det er også avhengig av hva denne terroristen ser på som verdifulle mål, noe som også er avhengig av terroristen egne tanker og vurderinger. Intensjonen vil heller ikke være konstant. Menneskers mål og rasjonale for hva de er villige til å gjøre, vil konstant utvikle seg – i motsetning til de statiske faktorene i tauet og det som sliter på tauet.

Denne usikkerheten, blant annet med utgangspunkt i intensjonsvurderinger, er et kjennetegn med tilsiktede uønskede hendelser der vi ikke kan si hvor, når og med hvilke metoder en trusselaktør slår til (NSM, 2015, s. 10). Usikkerhet forstås her som mangel

av kunnskap om ukjente størrelser (Flage et al., 2009). I empirien eksemplifiseres dette blant annet ved å vise til at ikke alle sikkerhetstrusler blir gjort kjent for organisasjonens medlemmer. Enten ved at trusselaktøren skjuler sin aktivitet, eller ved at trusselinformasjon ikke deles i organisasjonen.

Intervjuobjektene beskriver denne utfordringen ut fra at det er vanskelig å basere analyser og vurderinger på de få reelle erfaringene man har. Oppsummert beskriver intervjuobjektene at det svake empiriske grunnlaget for å vurdere sannsynlighet, skaper et abstrakt risikobilde. Dette fører til at det er vanskelig å etablere hensiktsmessige grunnleggende antagelser som skaper forståelse hos medlemmene i en organisasjon, for hvorfor man vedtar og innfører sikkerhetstiltak.

I risikotrekanten er trussel det ene hjørnet, med verdier og sårbarheter som de to andre. Flere intervjuobjekter henviste til at trusselen er dimensjonerende og utløsende faktoren for den totale risikoen. Trusselbildet pr 2023 er i hurtig utvikling. 2022 inkluderte den russiske invasjonen av Ukraina og en økt etterretningstrussel mot Norge fra Russland som følge av norsk deltakelse i internasjonale sanksjoner, våpeneksport til Ukraina, medlemskap i FNs sikkerhetsråd og NATO, og den delte grensen i de strategisk viktige nordområdene (PST, 18.03.22). Det skjedde et islamistisk terrorangrep i Norge i juni 2022. NSM registrerte en tredobling av antall rapporterte dataangrep (NSM, 2023). Psykisk ustabile trusselaktører utførte handlinger som førte til dødsfall to ganger høsten 2021. Denne oppgaven skal ikke redegjøre for trusselbildet hverken i Norge eller globalt. Men de nevnte trusselfenomenene viser bredden og kompleksiteten i trusselbildet, som organisasjoner må forholde seg til.

Trusselvurderinger har følge Kjetil Hatlebrekke (2021), et iboende problem med kognitiv lukking og induktiv tenkning som gjør det vanskelig å oppdage og vurdere nye trusselfenomener, modus og aktører som man ikke har erfaring og empiri på. Det er truslene som eksisterer utenfor vår erfaring og vanetenkning, som er vanskeligst å erkjenne. Disse er de farligste ifølge Hatlebrekke.

«Den største trusselen mot god tenkning om beredskap er troen på at fortiden gjentar seg. Det gjør den aldri. Men fordi fremtiden fremstår som variasjoner av fortiden, ser det ofte slik ut. På samme måte som skyggers utseende forandres i takt med avstanden mellom et objekt og en lyskilde, vil tilsynelatende like trusler variere i tid og kontekst. God trusselforståelse er derfor å vurdere i hvilke variasjoner av fortiden fremtidens trusler vil fremstå. Slik blir vi bedre rustet til å forutse hva som kan ramme oss i fremtiden. Dette gjør det enklere å anta hvem som kan komme til å angripe oss og i hvor stor grad de har vilje og kapasitet til å gjennomføre sine planer. Trusler handler altså om motpartens intensjon, vilje og kapasitet til å angripe eller ramme oss» (Hatlebrekke & Smith, 2010).

Innen sikkerhet er det slik at man ikke vet hvilken angrepsmetode eller modus trusselaktøren planlegger eller opportunistisk, velger å benytte. Trusselvurderinger skal vurdere både hvilke aktører, men også hvilke modus som er aktuelle for at brukere av vurderingen skal kunne iverksette forebyggende sikringstiltak og planlegge beredskap for håndtering. Gitt at «initiativet» ligger hos trusselaktøren og at det som beskrevet over, ligger i trusselens natur å skjule dette for å bedre kunne lykkes, vil det alltid ligge en større usikkerhet over disse vurderingene enn i *Safety*-vurderinger.

Noen trusselaktører, angrepsmodus og fenomener vil være historisk kjente. Trusselbildet monitoreres av etterretnings- og sikkerhetstjenester, og vil også til en viss grad være

kjente. Det vil likevel være mange trusler og mange måter å angripe på, som ikke er oppdaget og kjent for de som skal sikre oss mot dem. Denne dimensjonen med det kjente og ukjente, illustreres i en versjon av Joharis vindu (Žižek, 2006).

Trusler man kjenner til og er bevisst, som f.eks. flykapring, kan beskrives som kjente-kjente. Flere historiske hendelser har ført til at man er bevisst og jobber aktivt mot denne trusselen. Trusler man har kunnskap om, men ikke er bevisst kan beskrives som kjente-ukjente trusler. Et eksempel er modusen som ble benyttet under 11. september-angrepet på USA. Her hadde FBI og CIA informasjon som de ikke klarte å dele og nyttiggjøre seg av før angrepet materialiserte seg.

Ting vi ikke vet at vi vet, beskrevet som ukjente-kjente, er den tredje kategorien. I denne sammenheng er det snakk om trusler man vi ikke kjenner til hvordan vil inntreffe, men som man er bevisst. Et eksempel er den stadig endrede cybertrusselen, hvor organisasjoner vet at det finnes trusselaktører som er ute etter å ramme dem, men man vet ikke når eller hvordan det kommer til å finne sted.

Mens det også vil finnes trusler man ikke har forestilt seg, og som man ikke vet at man er blinde for; ukjente-ukjente. Dette beskrives også som «sorte svaner» (Hatlebrekke 201, s. 61); hendelser som er utenkelige for de fleste før de inntreffer. Her benyttes ofte eksempelet som massakren på Utøya 22. juli 2011. Terrorisme var man bevisst, men ikke fra en høyreekstrem anti-islamisk akslerasjonistisk solo-aktør, og ikke mot et norsk ungdomsparti.

Denne utfordringen understrekes av intervjuobjektene i denne oppgaven. Denne kombinasjonen skaper en det som blir beskrevet som en «abstrakt trusselsituasjon». Der man kan analysere sannsynligheten for at et uhell skjer gjennom analyser av tidligere hendelser, materialers slitasje og et statistisk tallmateriale som er overførbart til nye hendelser, er den ondsinnede intensjonen hos andre mennesker, umulig å kvantifisere. PST benytter begrepene intensjon og kapabilitet for å si noe kvantifiserbart om trusselaktørens potensiale. Men intensjonen vil også henge sammen med verdiene trusselaktøren ønsker å ramme, og hvordan trusselaktøren verdivurderer slike.

Slik blir vurderingen av trusselen, et produkt av en kvalitativ analyse, uten matematiske parametere eller resultater. Dette abstrakte og vanskelig håndgripelige fundamentet, er det organisasjoner må forholde seg til når de skal jobbe med sine risikovurderinger og rettfærdiggjøre sine sikkerhetstiltak ovenfor sine medlemmer. Men ikke minst er det inngangsværdien for de grunnleggende antagelsene hos medlemmene i en organisasjon, om hvorvidt det finnes noen trusler, og hvem som ønsker å påføre dem bevisst ondsinnet skade.

6.1.2. Sikkerhetens målbarhet og konkurranse med produksjon

Formålet med sikkerhet gjennom en etablert risikostyring og sikkerhetsledelse av organisasjoner, er å ha en «riktig balanse mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap» Aven (2007, s. 15). Reason (1997) formulerer det slik at en organisasjon står ovenfor to verdener i så henseende: Sikkerhet på den ene siden og produksjon på den andre. Der organisasjoner måles på styringsparametere som effektivitet, produksjonsvolum, økonomi eller andre konkrete størrelser, trekkes det frem både i de litterære kildene og hos intervjuobjektene, at sikkerhet er et fagfelt uten suksesshistorier. Reason (1997) beskriver i sin teori Unrocked boat, sammenhengen mellom produksjon og sikkerhet med at produksjon er noe håndfast og forståelig, mens sikkerhet bare blir målt ut fra fravær av hendelser. Informasjon om hvorfor slike

uønskede hendelser ikke skjer, er ofte usikre og diffuse. Fravær av hendelser er et derfor et vanskelig om ikke umulig måleparameter å bruke. Intervjuobjektene beskriver dette problemet som en vanskelig balansegang, mellom å redusere risiko, og hvordan sikkerhetstiltak og prioriteringer påvirker produksjon eller annen måloppnåelse.

Roar Thon, fagdirektør for sikkerhetskultur i NSM, presiserer at sikkerhet i seg selv, ikke kan være organisasjonens formål. Sikkerhet handler ikke om å produsere eller å skape verdier. Det handler om å beskytte denne produksjonen eller måloppnåelsen fra uønskede ondsinnede handlinger. Å være sikker mot ondsinnede forsettlige handlinger, vil stort sett alltid være i konkurranse med organisasjonens opprinnelige formål (Ellestad et al, 2019). Det ble av flere intervjuobjekter formulert som at sikkerhet kan oppfattes som negativt, «et gnagsår»; en hemmende faktor. Sikkerhetspersonell oppfattes ifølge respondentene, ofte som «sure» eller negative som «*dukker opp en gang iblant og er bare sur*», og påpeker feil eller pålegger andre medlemmer prosedyrer eller tiltak som vanskeliggjør hverdagen deres.

Det ble i empirien henvist til at noen ledere argumenterer med at de ikke blir målt på sikkerhet, og derfor ikke prioriterer det. For hvordan skal man måle det som ikke skjer, og kan man begrunne fraværet av sikkerhetshendelser med det ene eller andre sikkerhetstiltaket som reduserer sårbarheten, eller var det forhold hos trusselaktørene som gjorde at man ikke ble angrepet? Noen benytter parametere som hvor mange som har deltatt i presentasjoner av trusselbildet, som har tatt e-læringskurs i cybersikkerhet eller antall sikkerhetsrelaterte avvik. Men respondentene var kritiske til om man da egentlig måler sikkerhetsnivået. Respondentene beskriver at sikkerhet ikke kan eller bør måles alene, men sees som en del av oppnåelsen av organisasjonenes definerte formål. Funn fra empirien knyttes til at det en leder må evne, er å ta de resultatkravene lederen måles på, og se hvor sikkerhet påvirker disse målene. Hvordan sikkerhetsarbeidet hemmer produksjonen må sees opp mot konsekvensene av mulige sikkerhetshendelser.

Dette påvirker både hvordan sikkerhetsarbeids nytteverdi forstås i en organisasjon, hvordan verdiene oppfattes og i hvilken grad man ser på trusler som relevante, og i hvilken grad man aksepterer identifisert risiko. Dette handler altså om de grunnleggende antagelsene knyttet til sikkerhetsforståelse, trusselkognisjon og risiko, men også holdninger og normer knyttet til sikkerhetspersonell og regler og prosedyrer.

Delkonklusjon:

Hva betyr så disse særskilte utfordringene ved sikkerhetsfaget, i en kulturell kontekst? Kultur påvirket alt som foregår i en organisasjon. Selv om den ikke kan vedtas eller kjøpers, vil den virke inn på både formelle og materielle strukturer, og den vil prege arbeidsprosesser og relasjoner innenfor grupper og organisasjoner, herunder også sikkerhetsarbeidet. Kultur påvirker ledelsens beslutninger, men for at påvirkningen skal gå andre veien, fra vedtak til faktiske kulturelle endringer, er en krevende vei.

Utfordringene med å beskrive sannsynlighet og usikkerheten knyttet til trusselvurderinger, handler om at grunnpremissene for sikkerhet, ikke kan baseres på kjølige, rasjonelle fakta. Det må funderes på antagelser om trusler og risiko. Disse antagelsene vil påvirke både de formelle og materielle strukturene, så vel som den praktiske utførelsen av arbeidet og etterlevelsen av sikkerhetsprosedyrer og -regler, relasjonene gjennom kulturelle mekanismer.

Sentralt blant disse mekanismene er organisasjoners sensemakingprosess. Hvordan skal disse inputene oppfattes som «cues» og fortolkes, når det er knyttet så mye usikkerhet og abstraksjon til det? Og hvordan skal dette omsettes til aktiv deltakende sensemaking

gjennom enactment-delen av prosessen? Hva man oppfatter av trusselen mot egen organisasjons verdier, og sannsynligheten for å bli utsatt for ondsinnede uønskede handlinger, vil skape grunnleggende antagelser om risikoen og om sikkerhetstiltakenes relevans og effektivitet, og hvordan man kan prioritere sikkerhet i konkurranse med effektivitet og produksjon. Siden sikkerhet er vanskelig om ikke umulig å måle, blir de grunnleggende antagelsene om relevans, hensiktsmessighet og nytteverdi knyttet til sikkerhetsarbeid, kulturelle premisser for holdninger og normer og faktisk sikkerhetsatferd som årvåkenhet, bruk av sikkerhetsutstyr og håndtering av uønskede hendelser hos medlemmene.

6.2. Fortolkende kvalitativ tilnærming til sikkerhetskultur

På samme måte som en trusselanalytiker, må kreativt og subjektivt tolke trusselaktørenes intensjoner og kapasiteter, krever organisasjoners sikkerhetskultur en fortolkende tilnærming. Der det essensialistiske perspektivet ser på kultur som noe en organisasjon har, som en stabil og målbar størrelse, vil det fortolkende perspektivet se på kultur som mer komplekst enn de synlige artefaktene i atferd og symbolikk. Det essensialistiske perspektivet er mer håndgripelig og konkret, og gir «enklere» svar for en leder å forholde seg til når han skal ta inn over seg, bruke, utvikle eller endre kulturelle aspekter ved sin organisasjon. Men det fortolkende perspektivet argumenterer for at et slikt forenklet syn på kva kultur er og gjør, skaper stereotypier og tar ikke inn over seg de individuelle forskjellene blant medlemmene innad i kulturen.

Som nevnt tidligere, finnes kommersielle produkter som hevder å kunne skåre sikkerhetskultur, ut fra beskrivelser av de synlige artefaktene som medlemmene selvrappporterer på. Det var delte oppfatninger om verdien av slike målinger hos intervjuobjektene. Dette vil kunne gi et bilde av organisasjonens kultur, men bildet vil være en forenkling og overgeneralisering av det komplekse som ligger i det kulturelle. Kritikere av essensialistisk tilnærming, ville sagt at denne type analyser er en politisk og ideologisk konstruert stereotypi, med svært begrenset bruksområde. Stereotypier blir beskrevet som «...en type sosialt effektive fordommer» (Eriksen og Sajjad 2006, s. 56), som ikke anerkjenner forskjeller mellom folk innad i ei gruppe, og er ofte basert på forutinntatte ideer. «*Problemet er at da vrir du organisasjonen mot å følge med på det, mot å oppfylle det som er enkelt å avdekke,*» uttrykte en respondent som problematiserte slik essensialistisk tilnærming på det kulturelle artefakt-nivået.

Smith (2006, s. 915) hevder at studier av kultur i forretningskontekst, må bevege seg videre fra en slik essensialistisk tenkning, mot mer kvalitative analyser og beskrivelse av organisasjonskulturer. Earley støtter denne tanken, om å se på kultur ikke som statiske verdier, men mot mer dynamisk meningsdannelse: "the meaning we attach to aspects of the world around us" (2006, s. 925). Fokus på meningsdannelse integrerer i større grad de individuelle forskjellene innenfor den same kulturelle konteksten, og tillater at man inkluderer psykologi og kognitive aspekter i den kulturelle identiteten.

En fortolkende tilnærming til sikkerhetskultur som meningsdannende systemer som kan inkludere psykologiske og sosiale parametere, vil altså kunne gi en høyere forståelse enn overforenklete og negativt ladede, forutinntatte essensialistiske beskrivelser. Det fortolkende perspektivet betyr at vi ser på hvordan mennesker benytter de kulturelle meningssystemene til å fortolke verden, og hvilke handlinger og atferd har for betydning for menneske, framfor å beskrive dette fra et distansert utenforstående perspektiv. Flere

intervjuobjektet problematiserte påliteligheten til de kvantitative essensialistiske målekriteriene, fordi de kun måler det man har besluttet å bruke som parameter.

Vi må altså gå fra å observere og beskrive, og så ta et steg videre til å fortolke. Essensialisten forsøker å benytte sine observasjoner og beskrivelser, til å utlede en lovmessig predikasjon på hvordan en representant for den observerte kulturen, vil opptre. Fortolkeren vil forsøke å finne meningen med den atferden man har observert gjennom et dypere dykk i kompleksiteten bak individet sitt kulturelle meningsunivers. Geertz' fortolkende forståelse av kultur, oppsummerer at analysen av kultur ikke kan være «an experimental science in search of law, but an interpretive one in search of meaning» (1973, s. 5).

For den fortolkende gruppen kulturteoretikere er kultur noe dypere enn den symbolske manifestasjonen gjennom historier, ritualer, symboler og språk. Disse er artefakter for å overføre kultur, men ikke selve kulturen i seg selv. Artefaktene gir bare tegn på at det finnes en mye dypere og altomfattende meningssystem i organisasjonen (Buchanan og Huczynski, 1997 s. 514-515).

Mening er en kopling mellom det som «har» mening – en handling, en uttalelse, et atferdsmønster – og det som «gir» dette mening. Hjernen vår søker å skape mening gjennom å skape et sett med kategorier av prototypiske eksempel, koblet sammen i større mønster. Man kan se på disse kategoriene som kulturelle modeller. Modellene gir en mening for individet, men er også delt blant medlemmene i ei gruppe, som artefakter og kognitive konstruksjoner.

Nye fenomen eller hendelser som det ikke er etablert holdninger til eller normer for, må sees i lys av de mentale modellene som gruppen har etablert for dette nivået. Når politietaten møtte utfordringen med at nyutdannede tjenestekvinner ønsket å bruke hijab som en del av uniformeringen, var det ikke etablerte normer for dette, og uenigheter ble uttrykt blant annet i en kronikkveksling i Aftenposten i 2022.

«For hva er i realiteten forskjellen på en synlig muslimsk kvinne og en «usynlig» muslimsk mann? Vil det faktisk at jeg går med hijab, utgjøre en reell forskjell for jobben jeg gjør?» spør Hani Hussein Ali i Aftenpostens Si ;D 23. september.

«Religiøse symboler og/eller plagg, uansett religion, vil undergrave politiets evne til å fremstå nøytrale og som en yrkesgruppe som behandler alle grupper i samfunnet likt. Ingen har rett til å bli politi. Et av politiets kjennetegn er uniformen deres. En uniform er en ensartet, lik bekledning for utføring av en spesiell virksomhet. Religiøse eller politiske symboler og/eller plagg burde da ikke tilhøre politiets uniform,» svarer Serine Aarvik i same medium 22.10.22.

I en spørreundersøkelse gjort av NRK i 2009, svarte 96 % av ca. 2000 polititjenestepersoner, at de ikke ønsket hijab tillatt som en del av uniformeringen. Et overveldende flertall, 88,6 %, svarte videre at de begrunnet dette med at «prinsippet om symbolfri uniform/nøytralt politi er så viktig at det bør stå over andre hensyn.» Denne tematikken skal ikke drøftes i denne oppgaven, men tjener som et eksempel på hvordan et synlig artefakt og diskursen rundt denne, blir vurdert, basert på mentale modeller for kulturell verdisetting. Daværende leder i Politiets Fellesforbund, Arne Johannesen formulerte at «Dette er et tydelig prinsipielt syn om at politiet er likt, ett politikorps for alle er signalet» (Skille & Strand, 2009). Nøytralitet, likhet og symbolfrihet blir da mentale modeller for hvordan dette vektet mot f.eks. retten til å uttrykke seg religiøst eller som en del av en «annen» kultur enn politietatens.

Men under disse verdiene, holdningene og normene, som et fundament for den meningen de gir for kulturens medlemmer, ligger det Schein betegner som grunnleggende antagelser. For å spille videre på det foregående eksempelet, så vil verdiene om nøytralitet og likhet, måtte basere seg på en grunnleggende antagelse om hva hijab representerer, hva politiuniformen betyr i møte med publikum, og ikke minst, hvilke konsekvenser dette har for tillitten til politiet i møte med norske borgere. Disse mentale modellene er ikke like lette å formulere og argumentere for eller mot. Fordi dette er «bare sånn det er».

«Uansett hvordan man snur og vender på det, så er og blir hijaben et underkastelsesmerke under den muslimske guddommen. Det er et unaturlig symbol å bli møtt av foran i en rettssal eller når man har med politiet å gjøre», skriver Vebjørn Selbekk, sjefredaktør i Dagen i en kronikk (Selbekk, 2020). Hans ytringsfrihetskommisjons-kollega Sarah Zahid svarer kontant at «muslimer ikke betegner hijab som et «underkastelsesmerke» (Zahid, 2020). Nok en gang er dette ikke en drøfting av saken, men et eksempel på hvordan representanter for forskjellige kulturer, har vidt forskjellige og motstridende grunnleggende antagelser om hva hijab er. Dette danner fundamentet for at det utvikles forskjellige holdninger til plagget som i sin tur blir grunnlaget for de ytre artefaktene, i dette tilfellet diskursen rundt tematikken.

Det en essensialistisk tilnærming vil fokusere på, er i all hovedsak de observerbare artefaktene, og de eksplisitte verdiene og normene som man klarer å sette ord på. Men dette blir da en deskriptiv fremstilling. Men det inkluderer ikke sensemaking-prosessen man får tilgang til gjennom fortolkningens dypdykk ned til de grunnleggende antagelsene, som Holliday kaller «thick slicing», eller «tykke beskrivelser». Fortolkende tykke beskrivelse søker å finne de underliggende kulturelle delte mentale modellene som ikke er umiddelbart tilgjengelige.

Å vurdere de tidligere nevnte uttalelsene om hijab i politiet, som beskrivelse av kulturen Arne Johannesen, Vidar Selbekk eller Sarah Zahid representerer, er det motsatte av «tykke beskrivelser». Ved en slik tilnærming vil man dermed gå glipp av det fundamentale i kulturen; de kulturelle delte mentale modellene på det grunnleggende antagelses-nivået. Først når man «gjør det kjente ukjent» og setter til side «enkle svar», ved å åpne opp for kompleksitet, kan man beskrive hele det kulturelle og ikke bare hva som kommer til eksplisitt uttrykk.

En fortolkende tilnærming vil kunne forklare Johannesens utsagn, kan fortolkes som basert på et politikulturelt verdisyn om at alle borgere skal møtes på en lik og rettferdig måte av politiet. Videre kan dette verdisynet tolkes dit at det baserer på den grunnleggende antagelsen om at alle mennesker er likeverdige og at lik behandling fører til rettferdighet. Zahids kulturelle verdier kan tolkes som at lik behandling av ulike individer, ikke er rettferdig. At det ligger en grunnleggende antagelse om at mennesker må møtes med respekt for deres ulike identiteter, basert på en antagelse om at positiv forskjellsbehandling er mer rettferdig enn distansert likebehandling.

Som nevnt og beskrevet gjennom teorien og empirien i denne oppgaven, finnes det metoder og produkter som hevder å måle en organisasjons sikkerhetskultur. Digital penetrasjonstesting, kontrollerte phishing-tester på mail, spørreundersøkelser og øvelser er blant disse. Jeg har gjennom oppgavens teoridel, redegjort for kulturens tre nivåer. Og det er min påstand at disse metodene i all hovedsak måler de synlige artefaktene, og eventuelt tar med selvrapporing på verdier, holdninger og normer.

I medisinsk terminologi kaller man det å identifisere og klassifisere en sykdom eller tilstand, for diagnostikk. Det er, spesielt innen allmennpraksis, vanlig med det som kalles symptomdiagnose. Det betyr å omtale symptom, som f.eks. ryggsmertor selv om man ikke kan finne objektive tegn til sykdom. Undersøkelser av sykdomshistorie og kliniske enklere undersøkelser ved bruk av blodtrykksapparat, stetoskop og ultralyd, vil gi en ytterligere forståelse. En fullstendig diagnose krever derimot ytterligere metoder som blodprøveanalyse, røntgen, CT, MR, PET, EKG osv. Korrekt diagnose er en forutsetning for fullgod behandling og for vurdering av utvikling og prognose for sykdommen (Bruusgaard, 2022).

På samme måte vil måling av sikkerhetsatferd gi en symptomdiagnose, eller beskrivelse av hvordan de synlige artefaktene gir seg utslag i sikkerhetsatferd – de mentale modellene som styrer medlemmenes bruk av sikkerhetssystem og etterlevelse av sikkerhetsregler. Men for å forstå hvorfor «pasienten» - her forstått som en gitt organisasjon – har disse symptomene, må man undersøke både hvilke verdier, holdninger og normer som styrer atferden – de mentale modellene for å verdivurdere handlinger og atferd. Og disse er igjen basert på medlemmenes mentale ubevisste modeller for hvordan verden henger sammen – de grunnleggende antagelsene.

Det er denne fundamentale forståelsen jeg argumenterer for at en organisasjon trenger for å bevisst kunne påvirke kulturen i ønsket retning. Det er dermed ikke feil å identifisere symptomer eller formulere de verdier, holdninger og normer som ligger til grunn for atferden. Men gjennom fortolkende «tykke beskrivelser» som inkluderer de grunnleggende antagelsene, finner man ut hva som i bunn og grunn hemmer og fremmer hensiktsmessig sikkerhetskultur.

Forskjellen mellom Hofstede (1980) sine kulturelle dimensjoner maktdistanse, usikkerhetsunnvikelse, individualisme-kollektivism, maskulinitetsorientering og langtidsoverorientering og den siste tillagte dimensjonen «indulgence vs restrained», er hvordan man forholder seg til vurderingene og plasseringene på en skala. McSweeney (2002) oppsummerer kritikken av Hofstede. Denne kritikken dreier seg om at Hofstedes dimensjoner påberoper seg å beskrive alle medlemmer i en nasjonalkultur, ut fra de identifiserte gjennomsnittlige tendensene. De kulturelle forskjellene eller mangfoldet innenfor en kultur, blir ikke beskrevet. Og Hofstede tar utgangspunkt i at funn fra gitte arbeidsplasser, kan overføres til en hel nasjonalkultur. Det vises videre til at Hofstede bruker anekdotisk bevisføring, ved å vise til synlige artefakter som historier om atferd, som bekrefter dimensjonenes validitet.

De sikkerhetskulturelle dimensjonene jeg har presentert og skal drøfte videre, har ikke som formål å fange en statisk og fundamental «essens» i en organisasjon, for å vurdere denne som god eller dårlig. Det er heller ikke formålet å skape et resultat som skal brukes til å predikere fremtidig atferd. Dimensjonene jeg har valgt ut skal fungere som et sett begreper som man kan benytte i tykke beskrivelser av kulturelle trekk, som er relevante innenfor sikkerhetsaspektet ved en gitt organisasjon. De er tenkt som overskrifter når en leder, en arbeidsgruppe eller en ekstern konsulent skal skape tykke beskrivelser av de kulturelle trekkene som påvirker hvordan en medlemme i en organisasjon forstår og forholder seg til sikkerhet. Ved å ta utgangspunkt i kultur som delte mentale modeller, som eksisterer både som individuelle og kollektive meningssystemer, kan man ta innover seg hvordan dette vil gi forskjellige utslag hos de enkelte medlemmene. Og ved å forstå etableringen og den kontinuerlige utviklingen av

disse modellene, gjennom en aktiv og kollektiv sensemaking-prosess, vil man ikke låse seg til en statisk forståelse av sikkerhetskulturen i en gruppe.

Askehave (2006), argumenterer for at det ikke er nødvendig å tenke «enten/eller», i arbeidet med å forstå og jobbe aktivt med organisasjonskultur. En essensialistisk «måling» av sikkerhetskulturelle artefakter som hvordan sikkerhetstiltak faktisk benyttes, hvordan prosedyrer etterleves, i hvilken grad svikt i egen sikkerhet rapporteres, gir en «symptomdiagnose»; et utgangspunkt for å undersøke sikkerhetskulturen dypere. Ved å observere disse ytre artefaktene, kan man bruke dette «øyeblikksbildet» til å mer kvalitativt fortolke hva som faktisk er forklaringer til at sikkerhetskulturen kommer til syne på denne måten.

Men for å kunne aktivt arbeide for å utvikle sikkerhetskulturen i ønsket retning, må man forstå den i hele dybden. En slik forutsetning krever at man ikke bare beskriver, men streber mot å forstå hele det kulturelle meningssystemet, helt ned til de grunnleggende antagelsene, og ikke bare beskrive og måle eller vekte ytre artefakter. På samme måte som man gjennom tykke beskrivelser, kan etablere en forståelse for hvorfor noen grupper iverer for eller motarbeider bruk av hijab som en del av polituniformen, kan man slik skape en forståelse for hvorfor det i noen organisasjoner utøves sikkerhetsatferd som bidrar til redusert risiko, men i andre er det greit å «lure» sikkerhetssystemet, ved å dele brukernavn og passord eller tar med seg telefonen inn i mobilfrie soner osv.

6.3. Hensiktsmessig sikkerhetskultur

Gjennom det foregående avsnittet, har jeg argumentert for en fortolkende tilnærming til sikkerhetskultur. Det normative kontra det deskriptive ved slike vurderinger av kultur er også relevant å drøfte mer inngående. En fortolkende tilnærming handler om å forstå meningssystemet i de kulturelle modellene, og er således nært beslektet med kulturrelativismen. Kulturrelativisme er et perspektiv som går ut på å forstå alle kulturer eller kulturmønstre som likeverdige, noe som innebærer at alle samfunn må forstås ut fra sine egne premisser, at man tar det for gitt at det ikke kan etableres noen felles verdiskala som ulike samfunn og kulturer kan vurderes eller rangeres i forhold til. På denne måten kan kulturrelativisme forstås som motsatsen til etnosentrisme (Siverts og Fagernes, 2021).

Formålet med de dimensjonene jeg presenterer, er heller ikke å skåre en organisasjon på en «god til dårlig» kulturell skala. Dette har vært en del av kritikken mot Hofstede og essensialistenes tilnærming til kultur. Den kvalitative analysen gjennom bruk av sikkerhetskulturelle dimensjoner, kan likevel benyttes til kritisk å vurdere sikkerhetskultur. Her er det viktig å ta med seg formåls-premisset i organisasjoner: «En organisasjon er et sosialt system som er bevisst konstruert for å løse spesielle oppgaver og realisere bestemte mål» (Kaufmann og Kaufmann, 2015, s. 57). En virksomhet skal tjene penger, lønne sine ansatte, etablere eller posisjonere seg i et marked. En ideell organisasjon skal fremme medlemmenes felles syn eller interesser. En avdeling skal oppnå resultater innen det ansvarsområdet de er tillagt.

Dette formålet vil skape en standard der kulturen enten bidrar positivt og fremmer mulighetene til å oppnå målet eller målene, eller den kan virke negativt og hemme måloppnåelse. Slik vil også sikkerhetskulturen kunne virke fremmende eller hemmende – hensiktsmessig eller ikke hensiktsmessig. Hensikt handler om bevisst streben etter å oppnå det man ønsker. Hensiktsmessig sikkerhetskultur vil altså fremme sikkerheten.

Men samtidig skal ikke sikkerheten gå på bekostning av organisasjonens formål, slik empirien problematiserer og jeg drøftet ovenfor. Hensiktsmessighet vurderes derfor ut fra om det er et formålstjenlig middel for å fjerne hindringer for at organisasjonens målsetninger oppnås, uten samtidig å hindre denne måloppnåelsen.

En deskriptiv fortolkning av sikkerhetskulturen, vil dermed kunne holdes opp mot en ønsket tilstand, og man kan identifisere uønskede sider ved organisasjonens sikkerhetskultur. Dersom kulturen preges av frykt for å rapportere svikt i sikkerhetstiltak eller brudd på sikkerhetsprosedyrer, vil man kunne beskrive det som en negativ side ved kulturen. Men kontra å rangere dette på en verdiskala fra god til dårlig, vil en fortolkende tilnærming søke å forklare hvilke grunnleggende antagelser som gir seg uttrykk i holdninger og normer, som igjen påvirker til denne uønskede sikkerhetsatferden. Målet er å forstå meningssystemet som ligger bak den uønskede atferden.

For å kunne vurdere hva som bidrar til organisasjonens måloppnåelse, må man ha en norm å måle seg mot. Er man en aktiv skiløper, er man sannsynligvis bedre enn gjennomsnittet og kan måle seg mot andre og se hvilken plassering man får i et skirenn. Men alle virksomheter skal og kan ikke gå i «samme løypa». De har ulike rammebetingelser i form av ulikt trusselbilde og forskjellige verdier og sårbarheter. Deres sikkerhetskulturer vil ikke være sammenlignbare (Sandbakken, 2017). Slik det er forskjellige behov fysisk og medisinsk hos en toppidrettsutøver og en hobbymosjonist, er det ulike sikkerhetskulturelle behov i ulike organisasjoner. Verdi-, sårbarhets- og risikovurderinger kan gi gode inngangsverdier for hva som er hensiktsmessig i hvert enkelt tilfelle. Risikoen vil diktere i hvor stor grad sikkerhet er en viktig bestanddel i organisasjonens kulturelle modeller, og hvilke mentale modeller som omfatter sikring som er relevante.

Et offentlig bibliotek vil i en normalsituasjon ha få eller ingen sikkerhetstrusler rettet mot seg. Likevel kan man vurdere at de forvalter verdier som personopplysninger om de som er registrert som brukere, fysiske verdier i form av datamaskiner og kanskje noen verdifulle bøker, og kan ha en symbolverdi når det brukes som forsamlingslokale for interesseorganisasjoner eller som arrangementssted for møter med politisk agenda. Sårbarheter kan være manglende fysisk eller digital sikkerhet, eller fravær av prosedyrer ved sikkerheshendelser.

I den andre enden av skalaen kan man tenke seg et gassanlegg langs norskekysten, som vil være et mål for fremmede staters etterretning eller sabotasje, miljøaktivister og sivil ulydighet, digitale trusselaktører som bruker løsepengevirus osv. Anlegget forvalter enorme verdier i form av sin gassforedling, prosessanlegg, distribusjonssystem, teknologi, symbolverdi og digitale infrastruktur, bare for å nevne noen. Sårbarheter vil kunne ligge i både den fysiske sikringen, men også i personellsikkerheten eller i den digitale informasjonssikkerheten.

Det vil ikke være fornuftig å måle hverken sikkerhetssystemet eller sikkerhetskulturen ut fra de samme standardene i to slike ulike organisasjoner. Som et av intervjuobjektene formulerte det, handler det om å «operere innenfor en intensjon om å opprettholde det «Level of Security» som vi søker å oppnå.» Selv om begge eksemplene krever at medlemmene er bevisste sine verdier, og at det dannes delte mentale modeller som skaper mening rundt sikringen av disse, vil parameterne være i hver sin ende av en tenkt skala.

Denne oppgaven vil derfor ta som utgangspunkt at sikkerhetskultur ikke kan måles ut fra en universell normativ skala fra «bra» til «dårlig». Det er likevel et normativt aspekt som knytter seg til hvorvidt den eksisterende sikkerhetskulturen er hensiktsmessig eller ikke, vurdert ut fra den risikovurderingen som ligger til grunn.

Gjennom bruk av de dimensjonene jeg i det videre vil drøfte, vil man kunne beskrive en slik kulturell «ønsketilstand» og sette en standard som best bidrar til å oppnå organisasjons formål. Dimensjonene skal bidra som et begrepsapparat for både å beskrive hvor man ønsker å være, men også for å fortolkende beskrive hvor man er pr i dag. Slik vil man kunne se hvor det er avvik og begynne å jobbe aktivt i et forsøk på å påvirke sikkerhetskulturen i ønsket retning.

Jeg har flere steder i oppgaven referert til teorien om høypålitelighetsorganisasjoner eller HRO'er. Flere av intervjuobjektene trekker også frem denne type organisasjoner som f.eks. militære spesialstyrker. Denne teorien har kvalitetsvurdert disse organisasjoner som særlig resiliente mot uønskede hendelser, ut fra gitte verdier. Og en stor del av forskningen tillegger kulturelle trekk eller kvaliteter, stor vekt når det gjelder å forklare hva som gjør at de begår færre feil, håndterer hendelser på en bedre måte, og evaluerer og lærer på en mer effektiv og formålstjenlig måte.

Jeg mener at det derfor ikke er å bryte med en fortolkende tilnærming til kultur, å beskrive sikkerhetskulturer som mer eller mindre hensiktsmessige for den gitte organisasjonen. Det vil ikke være universelle, essensialistiske målekriterier som gir en «god» eller «dårlig» skår. Men en forståelse for hva den enkelte organisasjon trenger for å best mulig ivareta sikkerheten, og sikre forståelse, engasjement og etterlevelse tilpasset den risikoen organisasjonen står i.

Empirien innhentet i dette prosjektet, styrker vurderingen om at det finnes kvalitetsforskjell på sikkerhetskultur. Intervjuobjektene henviste flere ganger til «god» og «dårlig» når de forsøkte å beskrive bruken av begrepet, og i sine refleksjoner rundt hvorvidt det er mulig å måle sikkerhetskultur.

Alle respondentene henviste til at organisasjonskultur må tilpasses den enkelte virksomhet. I særdeleshet ble dette tydeliggjort når intervjuobjektet fra etterretningstjenesten forklarte seg rundt viktigheten av sikkerhet for sin organisasjon som en av de mest «sentrale rammefaktorene» for alt de gjorde:

«Og hvis da en villet handling gjør at den informasjonen blir lekket, eller deler av informasjonen, eller kunnskap om noe av det her blir lekket, så påvirker det ikke bare organisasjonen vår, men også evnen til å levere det vi skal levere til AS Norge. Som jo er unik informasjon.»

Et annet intervjuobjekt formulerte «god sikkerhetskultur» på følgende måte:

«At virksomheten bevisst eller ubevisst har en kontinuerlig utvikling og diskusjon og prosesser knyttet til trusler, sårbarhet eller risiko, etter hvert som virksomheten utvikler seg. At de har en helt klar tanke om at den nye kunden som vi akkurat har fått kontrakt med nå, den endrer trussel og risikobildet vårt i betydelig grad. Og at det noe som nærmest skjer neste automatisk, er illustrasjonen på en god kultur.»

Intervjuobjektene trakk også frem behovet for å danne seg et inntrykk, forstå nå-tilstanden, for å kunne jobbe for å utvikle mer hensiktsmessige sikkerhetskulturer. Det var stort sprik i hvordan respondentene vurderte både mulighetene og metodene for å

«måle» eller gjøre en slik analyse. Det er denne oppgavens formål å bidra til en forståelse og et begrepsapparat, som kan bistå i nettopp dette arbeidet.

Delkonklusjon:

Sikkerhetskulturens synlige artefakter, kan måles og vurderes. Men denne oppgaven konkluderer med at det gir begrenset verdi ut over en «symptombeskrivelse». For å skape bevissthet og forståelse, kreves det en fortolkende tilnærming, der man søker å forstå meningsstrukturene fra de synlige artefaktene, via verdi- og holdningsnivået, helt ned til de grunnleggende antagelsene delt av gruppen som mentale modeller for hvordan verden henger sammen og fungerer, samt den sosial sensemaking-prosessen som skaper de mentalemodellene.

Dette vil gi en beskrivelse, som kan vurderes normativt. Ikke ut fra en universell skala fra «god» til «dårlig», men ut fra hva som er hensiktsmessig for at den enkelte organisasjon skal kunne nå sine mål, uten hindringer forårsaket av bevisste ondsinnede trusler. Et av oppgavens delmål er å undersøke hvorvidt en leder gjennom kvalitative analyser og bevisst tilnærming og med riktige rammer, kan jobbe kontinuerlig med på å påvirke sikkerhetskulturen i sin organisasjon. Dette krever en beskrivelse og en vurdering av nå-tilstanden, som utgangspunkt for dette arbeidet.

6.4. Bruk av felles begrepsapparat med inndeling i dimensjoner

Så hvordan kan man tilnærme seg sikkerhetskultur på en fortolkende kvalitativ måte, som gir en forståelse og et verktøy for ledere og organisasjoner som vil bevisstgjøre seg og aktivt forsøke å utvikle hensiktsmessig sikkerhetskultur? Jeg har i oppgavens teoridel, identifisert dimensjoner innenfor det grunnleggende antagelsesnivået for sikkerhetskultur i organisasjoner. Jeg vil i det videre drøfte disse dimensjonene med utgangspunkt i det teoretiske grunnlaget og basert på empirien jeg har presentert over.

6.4.1. Sikkerhetsforståelse

Den første dimensjonen har jeg valgt å kalle sikkerhetsforståelse. Dette skal innbefatte den grunnleggende forståelsen av konseptet sikkerhet. Er det noe man gjør forebyggende, for å hindre uønskede sikkerhetshendelser. Eller er det noe reaktivt der funksjonen er å respondere på sikkerhetshendelser ut fra beredskapsplanverk og prosedyrer? Sikkerhetsforståelsesdimensjonen innenfor det kulturelle, inneholder altså mentale modellene som deles i organisasjonen, som sier noe hva som oppfattes som sikkerhetsarbeid; fra forebyggende barrierer til operativ hendelseshåndtering.

Som empirien fremhever, og ut fra faglitteraturen, så ekskluderer ikke det ene det andre, og det er fullt mulig å jobbe helhetlig med prosesser og tiltak i begge ender av et slikt spekter. Men jeg vil eksemplifisere hvordan slike grunnleggende mentale modeller kan gi seg utslag i forskjellige typer organisasjoner.

En politipatrulje må fokusere på å kunne håndtere tilsiktede uønskede hendelser, fremfor å beskytte seg fra å møte dem, ganske enkelt fordi de må eksponere seg for risiko for å gjøre jobben sin. Det ligger mye proaktiv tenkning i politiets operative taktikk og handlingsmønster. Men sikkerheten baserer seg i hovedsak på å bruke de reaktive virkemidlene man har til rådighet, kontra å proaktivt unngå risikoen. Sikkerhet forstås dermed som et reaktivt fenomen og verktøy for å håndtere trusler fremfor å unngå dem.

Difi sin rapport fra 2017, om kultur, holdninger og ledelse i politiet, beskriver at forskningen på politikultur, peker på noen nokså stabile kulturtrekk. Her beskrives et kriminalitetsbekjempende tenkesett og at politiet tradisjonelt ikke har vært så opptatt av

forebygging. Mange søker seg inn i politiet for å oppleve spenning, og politiet er handlingsorientert, og fokuset på innsats er større enn fokuset på strategisk arbeid (Difi, 2017). Dette vil kunne skape en kultur for handlekraft og initiativ der man ser på forebyggende sikkerhet som noe hemmende, men fremdyrke et fokus og en prioritering av reaktive sikkerhetstiltak.

På den andre siden vil en høyteknologisk virksomhet som forvalter sensitiv informasjon som gir dem et konkurransefortrinn, fokusere på å forebygge alle tenkelige trusler som kan kompromittere disse verdiene til konkurrenter. Hvis dette først skjer, er det ingen måte å reversere skaden på. Da er konkurransefortrinnet borte, og må bygges på nytt. Et slikt perspektiv vil bidra til å utvikle seg en sikkerhetskultur med et sterkt proaktivt fokus. Denne grunnleggende antagelsen vil altså danne seg i samspillet mellom hvordan man identifiserer rollen sin og organisasjonens formål, og hvordan man oppfatter og forstår hvilke verdier man skal beskytte.

Ut fra empirien innhentet i dette prosjektet, ble det fremholdt at denne dimensjonen er vanskelig å bevisstgjøre seg for medlemmene i en organisasjon, som er en del av definisjonen for de grunnleggende antagelsene. Disse utvikler seg gjennom overføring av taus kunnskap og etableres som en kulturell forståelse som det ikke stilles spørsmål ved. Intervjuobjekter i denne oppgaven refererte til «kulturelle sannheter» eller taus, implisitt kunnskap om hvordan man tenker sikkerhet; altså grunnleggende antagelser. Disse grunnleggende antagelsene trenger ikke ha oppheng i organisasjonens reelle behov, men kan være etablert over tid uten bevisst styring. Aktive valg ut fra risikoanalyser og trusselvurderinger, og kommunikasjon rundt dette til alle involverte, vil kunne omforme implisitt taus kunnskap til eksplisitt bevisst bevissthet og bidra til å endre disse grunnleggende antagelsene.

Det kan f.eks. være hensiktsmessig for en politiorganisasjon å ha større fokus på det forebyggende sikkerhetsarbeidet. Men den grunnleggende forankringen om at risiko er en del av hverdagen, vil motvirke en slik endring i tankegangen. Elisabeth Myhre Lie beskriver i sin avhandling om forebyggende politiarbeid, at det er et stabilt kulturtrekk i politiorganisasjoner, at de ser ut til å være mer orientert mot kriminalitetsbekjempelse enn service og hjelpeoppgaver. De ansatte er spenningsøkende og hedrer maskuline egenskaper og er villige til å bruke tvangsmakt når de mener det er nødvendig. Politi er et handlingsorientert yrke der målet er jakten på «de kriminelle» (Lie, 2022). Dette handlingsfokuset vil da kunne prege hvordan politiorganisasjoner danner og viderefører mentale modeller knyttet til hva sikkerhetsarbeid er. Ønsker man en kulturell utvikling, kreves altså en aktiv bevisstgjøring på risiko, og hva som menes sikkerhet i betydningen å redusere denne risikoen.

Det ble i datainnsamlingen presisert at det kan eksistere subkulturer i hver sin ende av spekteret innenfor samme organisasjon, der en avdeling har en utpreget proaktiv forståelse av sikkerhetsfaget, mens en annen kanskje kun tenker operativ hendelseshåndtering. En IKT-avdeling eller et arkiv, kan ha en type mentale modeller, mens de som jobber operativt ute har andre. Dette kan være hensiktsmessig siden de som avdelinger er utsatt for forskjellige trusselaktører. Men det er likevel viktig at begge sider får en forståelse for hvorfor det finnes forskjeller og hvilke utfordringer og potensielle synergieffekter man kan ha i dialogen mellom slike subkulturer. Digitale angrepsvektorer kan finnes ute hos operativt beredskapspersonell, og en voldelig trusselaktør kan komme seg inn på IKT-avdelingen.

De grunnleggende antagelsene om hva sikkerhetsarbeid er, vil påvirke hvilke holdninger organisasjonen har til hensikten med sikkerheten; om den skal aktivt forebygges eller om man aksepterer en viss risiko og forbereder seg på håndtering. Et av intervjuobjektene beskrev det som en dimensjonerende faktor som henger sammen med organisasjonens formål og verdier.

Dette er fortolkningsdelen av sensemaking-prosessen, der man vurderer inputene som handler om risiko og sikkerhetshendelser. Det inkluderer også holdninger og normer; hvor lojal man er til sikringssystemer som gjør hverdagen tungvint og som det kanskje er vanskelig å se verdien av. Derfor har intervjuobjektene understreket at man må bevisstgjøre medlemmer på hvorfor man fokuserer på den ene eller andre typen tiltak. Bevisstgjøring skaper fortolkningsrammer og vil kunne medføre høyere forståelse og motivasjon for etterlevelse av policyer og regler. Verdier som forsiktighet og «føre var»-prinsipper, kontra handlekraft og initiativ, vil bidra til en draging mot i hver sin ende av spekteret.

Synlige artefakter i enactment-delen av sensemaking-prosessen, innenfor denne dimensjonen, handler blant annet om diskurs. Hvordan snakkes det om risiko og sikkerhetsarbeid i organisasjonen? En organisasjon i den proaktive enden av spekteret vil f.eks. snakke negativt om alle uønskede hendelser. Dette er noe man vil og/eller må unngå. Risikoatferd vil omtales i negative ordelag, og det vil være sterke sosialiserende krefter som virker for at medlemmene skal etterleve de forebyggende sikkerhetstiltakene. En organisasjon i den andre enden av spekteret, vil fokusere sine heltehistorier på de som klarte å håndtere en uønsket hendelse på en effektiv, kreativ eller eksemplarisk måte. I typiske operative hendelseshåndterings-organisasjoner, som politi, vektere eller militære, vil man kunne se synlig utstyr for hendelseshåndtering, med en særlig symbolverdi. Våpen, utstyrsbelter, verneutstyr som skuddsikre vester, stikksikre hansker, hjelm osv. vil her ha en kulturell symbolverdi i tillegg til den operative nytteverdien.

Hva som er hensiktsmessig for en gitt organisasjon må baseres på en aktiv og bevisst vurdering. For en organisasjon vil forebygging være det viktigste mens for andre vil man oppleve så mange sikkerhetshendelser man ikke klarer å forebygge, at man må ha mest fokus på hvordan man skal håndtere disse gjennom beredskap og operativ håndtering. For de fleste vil likevel ytterpunktene på spekteret, medføre at man mangler noe. Selv en innovativ bedrift som lever av konfidensialiteten til sine forretningshemmeligheter, bør ha en viss beredskap for å håndtere tap av disse, selv om fokuset i hovedsak legges på å beskytte disse proaktivt. Og en politipatrulje må, selv om fokuset er på å håndtere en uønsket hendelse, kunne kombinere dette proaktivt egensikkerhet slik at man unngår unødig risiko.

Ved å bruke dette spekteret, vil en organisasjon både kunne bevisstgjøre seg hvor de bør prioritere sikkerhetsarbeidet sitt, utfordre den tause kunnskapen og gjøre den eksplisitt, og forstå og beskrive den eksisterende kulturelle modellen som kan hemme eller fremme den ønskede plasseringen man har innenfor spekteret.

6.4.2. Trusselbevissthet/trusselkognisjon

Kystverket eksemplifiserer i sin publikasjon ISPS-nytt 2-22, forskjeller i trusselkognisjon på følgende måte:

«Lukk øynene og tenk på en kake. Ikke les videre før du ser for deg kaken. Hva slags kake så du for deg? Var det en bløtkake med krem og bær, eller var det kanskje en sjokoladecake? Vi mennesker tenker i bilder, men tankebildene våre er ikke like. Kaken du så for deg var ikke den samme som jeg så for meg. Slik er det med risiko også. Vi oppfatter den ulikt. Skal vi bake den samme kaken gjelder det å unngå en tilfeldig røre av ingredienser. Når man skal vurdere risiko er det viktig å beskrive hva man ønsker å beskytte. Da gjelder det å se for seg det samme risikobildet» (Kystverket, 2022).

Kognisjon handler om erkjennelse, oppfatning og tenkning. I filosofi og psykologi opptrer ofte uttrykket «kognisjon» som motsetning til det følelsesmessige og intuitive. I store norske leksikon, beskrives kognitive system som system som kan behandle en viss type informasjon som sanseintrykk, minner, tanker eller språk. Kognisjon står for det som har med fornuftsbestemt og erfaringsbasert erkjennelse å gjøre (Kjøll et al, Store norske leksikon).

Denne dimensjonen må sees i sammenheng med avsnittet som drøfter sikkerhetsfagets kulturelle utfordringer knyttet til sannsynlighet og trusselvurderinger. Dimensjonen handler om de grunnleggende antakelsene om hva som er sant og hvordan man kommer fram til sannhet i organisasjonen, og den påvirker hvordan medlemmene i organisasjonen håndterer informasjon. Aksepterer organisasjonen informasjon om trusler utenfra fra eksperter og trusselvurderinger, eller krever den intern kunnskapsoverføring om hva som er relevant, eller må medlemmene bli enige i fellesskap om hvilke trusler som kan ramme organisasjonen? Som drøftet ovenfor, er sikkerhetstrusler mer uforutsigbare, har større usikkerhet knyttet til sannsynlighetsberegning, og har lavere frekvens enn de fleste sikkerhetshendelser. Hvordan organisasjonen klarer å forholde seg til denne mindre konkrete og mer abstrakte risikoen, og hvordan man forholder seg tilgjengelige kilder som PSTs og Etterretningstjenestens trusselvurderinger, faller inn under denne dimensjonen. I empirien fremkom det at det er lettere og mer akseptabelt å forholde seg til trusselinformasjon, jo mer lokal og relevant den er.

Det som ofte er fokusområder for essensialistiske sikkerhetskulturmålinger, er graden av bevissthet eller «awareness» som er det engelske faguttrykket. Trusselkognisjonsdimensjonen forstås av intervjuobjektene som noe som går dypere ned på de grunnleggende antagelsene, og må ikke sammenblandes med «awareness», her forstått kunnskapsnivået om trusselfenomener. Carpenter og Roer (2022) hevder at slik kunnskap eller bevissthet, ikke har direkte påvirkning på atferd. På samme måte som man vet hvilken mat som er sunn og usunn, og at vi vet at fysisk aktivitet er bra for helsen, men likevel velger potetgull og sofaen, vil vi også utvise risikoatferd, selv om vi kjenner til trusselbildet. Denne dimensjonen vil dermed ikke automatisk kunne observeres gjennom sikringsatferden til medlemmene i form av etterlevelse av policy og retningslinjer.

Bevissthet eller «awareness» er også en individuell kvalitet. Det er noe enkeltmedlemmet i en organisasjon tilegner seg eller mangler. Trenden i empirien er at en kollektiv delt forståelse rundt trusselbildet, er mest hensiktsmessig. Det dimensjonen trusselkognisjon handler om, er hvordan informasjon omdannes til mening etablert i delte mentale modeller, gjennom sensemaking-prosessen og organisatorisk læring.

Tilegning av kunnskap om potensielle trusler er bare den første delen i denne prosessen, også benevnt som creation. Interpretation eller tolkingen av innhentede inntrykk, og enactment – å handle etter de innspill man har fått og de fortolkninger som er gjort, må også inkluderes i denne dimensjonen. Det er den kollektive prosessen i gruppen, der trusselbildet sanses gjennom formidling av f.eks. trussel eller risikovurderinger, men også hvordan medlemmene oppfatter dette og aktivt skaper meningsfellesskapet om trusler og risiko, som inngår i denne dimensjonen. Igjen handler det om å etablere delte mentale modeller for hvordan man tar til seg informasjon som er relevant for sikkerheten. Empirien peker i klar retning av behovet for å involvere og informere bredt for å skape felles delte mentale modeller for vurdering og erkjennelse av trusler.

Derfor kan ikke den grunnleggende dimensjonen for trusselkognisjon, måles ut fra kunnskapsnivået til de enkelte medlemmene, men hvordan organisasjonen bruker denne informasjonen til å danne meningsfellesskap gjennom delte mentale modeller. Sensemaking-prosessen er det som danner grunnlaget for trusselkognisjonen og resultatet i form av de delte mentale modellene.

Rossnes beskriver hvordan HRO'er har en "mindfulness" – bevissthet og åpenhet knyttet til det å akseptere fakta ved svikt eller feil, og uten å forestille seg perfektjon som 0-visjoner for uønskede hendelser. Hvis sikkerhetshendelser er uunngåelige, må organisasjonen utvikle ferdigheter til å detektere svikt og begrense konsekvensene. Man må være villig til å revidere og oppdatere egne forventninger, både knyttet til egne sårbarheter, men også trusselaktører og modus.

«The idea of mindfulness is the equivalent of continuous surveillance of the existing situation based on expectations, updating these expectations based on new experiences and willingness and capability to invent new expectations» (Rosness et al 2010, s. 60-61).

Hvordan formidles trusselvurderinger i organisasjonen, kan være dimensjonerende i denne sammenhengen. Blir det sendt ut som en kvartalsvise e-poster, fremlagt som et foredrag på en fellesparole, inkludert i driller eller øvelser eller drøftet på avdelingsvis møter? Hva medfører dette av engasjement og involvering av medlemmene? I hvilken grad kan medlemmene bruke denne forståelsen til å påvirke egen og andres bruk av sikkerhetsprosedyrer og -tiltak? Integrasjon av trusselinformasjon svekkes når man unngår å dele informasjon på tvers av nivå og avdelinger, fordi det kan svekke enhetens makt og tilgang på ressurser i form av informasjon. Dette ble trukket frem av et av intervjuobjektene som hemmende for sikkerhetskulturen. Nye tolkinger og forslag kan også møte aktiv motstand fra andre enheter, både på grunn av det velkjente «not-invented here» syndromet eller fordi innovasjonen utfordrer andre aktørers maktposisjon (Rossnes et al 2013, s. 25). De interne maktforholdene i en organisasjon, påvirker med andre ord hvordan informasjon deles og formidles, noe som igjen kan påvirke trusselbevisstheten og -kognisjonen. Et intervjuobjekt fremhevet viktigheten av at medlemmene forstår og aksepterer slik informasjon, og understreket at det krever opplæring

Dimensjonen handler med andre ord om den røde tråden fra informasjonen presenteres, via medlemmenes kollektive tolkning, og deretter gjennom den aktive bruken av informasjonen for å skape mening. Dersom trusselinformasjonen mottas passivt og ikke brukes gjennom en aktiv sensemaking-prosess, vil den dermed ha liten eller ingen kulturell påvirkning.

Samtidig handler ikke sensemaking om rasjonelt å finne sannhet og oppnå korrekt forståelse, men heller om å kontinuerlig skrive om en pågående historie, og drives av troverdighet heller enn nøyaktighet. Som beskrevet tidligere er trusselvurderinger og sannsynlig innenfor sikkerhet, preget av abstraksjon, kvalitative vurderinger og semantiske beskrivelser. Det er ikke gitt at budskapet oppfattes enhetlig i en organisasjon eller gruppe. I alle fall ikke der det er aktivt engasjement og deltakelse i sensemaking-prosessen. Det vil si at dersom denne prosessen får leve sitt helt eget liv, kan den miste forankringen i det opprinnelige budskapet; de faglige analysene og vurderingene. Aktuelle trusler kan tolkes og omskrives som irrelevante, og mindre sannsynlige trusler kan ilegges for stor vekt.

Trusselkognisjon må derfor beskrives ut fra hvordan den kollektive meningsdannelsesprosessen i en organisasjon utøves. Kan man beskrive den som ledelsesstyrt der informasjonen som gis aksepteres som sannhet, eller er den mer styrt av uformelle autoriteter eller gruppeprosesser blant medlemmene? I en organisasjon med hierarkisk organisering, der ledere har stor autoritet, kan dette redusere hvor mye medlemmene selv deltar i denne meningsdannelsen. Er det derimot aktiv involvering av alle medlemmer, flat struktur og rom for personlige initiativ, vil man ha større sjanse for at medlemmene danner en alternativ kollektiv konstruksjon av trusselbildet.

En stor kompleks organisasjon som f.eks. Equinor, vil ha et system for distribusjon av trussel- og risikovurderinger. Størrelsen på organisasjonen og plattformen informasjonen deles på, skaper derfor lite rom for en felles kollektiv meningsdanning. Resultatet blir enten at informasjonen ikke blir inkludert i organisasjonens kollektive meningsdanning, fordi det skaper for lite involvering og engasjement, eller så kan det dannes flere ulike meningsfellesskap på de forskjellige arbeidsstedene. Men med lavere engasjement og aktiv deltakelse i sensemaking-prosessen, vil det opprinnelige budskapet i trusselvurderingen bevares. Dette vil bety en passivt mottakende trusselkognisjon.

En liten bedrift der man samles for å drøfte de årlige trusselvurderingene, vil på sin side gi rom for en aktiv involvering og et engasjement som skaper en enhetlig trusselkognisjon. Dette vil imidlertid kunne medføre at den sosiale konstruksjonen blir noe helt annet enn det som faktisk var det opprinnelige budskapet. Dette kan beskrives som en aktiv konstruerende trusselkognisjon.

Den delte meningsskapende trusselkognisjonen, vil i sin tur påvirke hvilke holdninger en organisasjon har til trusselbildet. En respondent understreket at slik kognisjon er en ferdighet som må trenes. I en gruppe med aktiv sensemaking, vil kunne skape et eierskap til det oppfattede trusselbildet. Gruppen vil danne seg en oppfatning og forståelse av trusselen og den risikoen organisasjonen opererer med. Man vil kunne observere meninger og diskusjoner om trusler, og aktivt engasjement i trusselbrifer eller andre fellesforum.

Grunnleggende antagelser på den aktivt konstruerende enden av spekteret, handler om at trusselbildet er alles ansvar å sette seg inn i. Kulturelle verdier handler om engasjement og interesse for potensielle trusselfenomener. Dette kommer til uttrykk i hvordan, hvor ofte og hvor engasjerte medlemmene er når det snakkes om trusselbildet.

I den andre enden har man en grunnleggende antagelse om at dette er et ansvar som ledelsen eller sikkerhetsavdelingen må ha. Det er en akseptert holdning at man aksepterer den informasjonen som man blir gitt, og normene krever ikke at man skal engasjere seg. Det blir heller sett på som «å se spøkelser på høylys dag» om det snakkes

høyt eller mye om trusler. Og de ser på organisasjoner eller individer i den andre enden av spekteret som «paranoide» eller «konspirasjonsteoretikere».

Jeg har definert spekteret for denne dimensjonen fra aktiv konstruerende, til passiv mottakende. Igjen så er ikke dette et spekter med normering på en skal fra dårlig til bra, men hensiktsmessighet. Denne dimensjonen vil måtte sees opp mot det som er det faktiske trusselbildet, og hvordan organisasjonen omsetter input til sine interne meningsdannende modeller. For noen organisasjoner vil aktiv deltakelse være formålstjenlig, men andre er avhengig av å etablere upåvirkede beskrivelser av trusselen og hva denne innebærer for organisasjonen. Ytterpunktene vil sjeldnere være hensiktsmessige, men hver organisasjon bør definere hvor på spekteret man ønsker å være.

6.4.3. Risikoaksept

Denne dimensjonen ser på hva som er den grunnleggende antagelsen om risiko i organisasjonen. Ser man på risiko som noe naturlig og akseptabelt, eller unngår man den ved alle korsveier, og søker å eliminere all risiko? Gitt sikkerhetens særegne utfordringer i forhold til å måle effekt av tiltakene, og den negative effekten sikringstiltak kan ha på drift og inntjening, vil noen organisasjoner utvikle en aksept for å leve med risiko. En organisasjon uten sikkerhetsrelaterte hendelser over lang tid, vil også kunne utvikle en følelse av å være «usårbare». Høy tiltro til egen hendelseshåndtering vil også gi ytterligere aksept for å leve med risiko. Da blir sårbarheter og risiko noe man anerkjenner, men samtidig aksepterer som et nødvendig onde. Slik er det med bruk av privatbil. Vi kjenner alle risikoen, blant annet ved at vi eksponeres for nyheter om bilulykker i media. Men vi velger likevel å bruke bil, og aksepterer risikoen uten å bruke mye kapasitet til å tenke på den.

Intervjuobjektene understreket at bevisst risikoaksept igjen krever et bevisst forhold til risikobegrepet. Intervjuobjektene i oppgavene understreker at man alltid forholder seg til risiko i alt man gjør, bevisst eller ubevisst. Å bare la det skure og gå, og overse risikoen er ikke det samme som å rasjonelt akseptere den. Nok en gang handler ikke de kulturelle dimensjonene om faktabasert rasjonell tenkning. Dette er snakk om sensmaking-prosessen, der medlemmene aktivt delta i prosessen om å skape mening. Derfor handler denne kulturelle risikoaksept-dimensjonen, ikke om hvorvidt det er gjort en risikovurdering og saklig ledelsesstyrt vurdering av restrisiko. Det handler om hva de mentale modellene hos medlemmene sier om risiko – som noe negativt, «farlig» og uønsket, eller som noe positivt som inkluderer spennende muligheter. De mentale modellene har ikke alltid oppheng i det reelle trusselbildet.

Som en del av den meningsdannende fortolkningsprosessen, vil tidligere erfaringer spille inn her. Organisasjoner som har opplevd negative konsekvenser som skader på fysiske verdier eller medlemmer liv og helse, økonomisk tap eller skade på omdømme, vil kunne utvikle en sterkere og mer bevisst aversjon mot risiko. Organisasjoner med sterk bevissthet på sine verdier og sårbarheter, vil også kunne trekke i denne retningen. Intervjuobjektene trekker her også frem eierskap til verdiene. I organisasjoner der medlemmene ikke forvalter egne verdier, er det en tendens til å akseptere høyere risiko. En finansorganisasjon som forvalter andres verdier, vil ikke ha den samme følelsen av eierskap til verdiene, og kan dermed være villig til å akseptere høyere risiko i bytte mot høyere potensielt utbytte. I en hjørnesteinsbedrift der drift er viktig for så å si hele bygda sin overlevelse, vil man ikke akseptere høy risiko. Det gir mening for medlemmene å unngå risiko fordi det kan ramme dem selv på flere plan. Da blir den

grunnleggende antagelsen, at risiko er nesten like ille som de faktiske uønskede hendelsene.

Kulturelle verdier for organisasjoner med høy risikoaksept, vil være av typen «mot» og «offensivitet». Holdninger på denne siden vil vise seg når man snakker om mulig gevinst. Innovasjon og utvikling er målet, og risiko assosieres med mulighet. «Den som intet våger, intet vinner» er et kjent ordtak for organisasjoner i denne enden av spekteret. Eller som Hellen Keller formulerte em slik holdning i *The Open Door* (1957):

«Security is mostly a superstition. It does not exist in nature, nor do the children of men as a whole experience it. Avoiding danger is no safer in the long run than outright exposure. Life is either a daring adventure, or nothing.»

I den andre enden vil kulturelle verdier være «trygghet», «forutsigbarhet» eller «stabilitet». Holdninger uttrykkes f.eks. gjennom ordtakene «Man prøver ikke en elvs dybde med begge føtter» eller «Forsiktighet er visdommens mor». Normen er «å tenke før man handler».

Mytene eller heltehistoriene man forteller i risikovillige organisasjoner, handler om en modig beslutning som gav suksess eller ekspansjon. Synlige artefakter i den andre enden av spekteret, er symboler som representerer kontinuitet og stabilitet, som at organisasjonen har vært virksom lenge. Ingen eller få uønskede hendelser vil da være suksesshistoriene.

Dimensjonens synlige artefakter handler om man søker å unngå all risiko gjennom beslutninger, innføring av omfattende prosedyrer, investeringer i sikringsutstyr, og atferden blant medlemmene i situasjoner hvor man vet det finnes en trussel. Diskursen rundt risiko og sårbarheter, er en del av de synlige artefaktene innenfor denne dimensjonen; hvordan man snakker om risiko, som noe skummelt eller som mulighetsvinduer.

I ytterste instans kan man se medlemmenes sikkerhetsatferd knyttet til identifiserte risikosituasjoner. Tar man med tjenestetelefonen i utlandet på steder med høyt trusselnivå? Bruker man wifi-tilkobling hos andre bedrifter eller hoteller selv om man kjenner til risikoen ved dette? Eller benytter man egne telefoner på reiser til risikoområder og bruker kun mobildata? Deler man informasjon med eksterne partnere ukritisk eller med forsiktighet? Det er også synlig i ledelsens risikovillighet i beslutninger og styring. Er det en akseptert risiko for å gjøre forretninger med land som PST advarer mot etterretningstrusselen fra? Er det investert i materielle sikkerhetsstrukturer og er sikkerhetsledelse og risikostyring en integrert del av lederansvaret?

Dimensjonen kan sees i sammenheng med Hofstedes (1980) dimensjon *Usikkerhetsunnavikelse*, som dreier seg om medlemmenes følelse av komfort eller om de føler seg truet i usikre og ukjente situasjoner. Usikkerhetsunnavikende kulturer vil ifølge Hofstedes dimensjoner, forsøke å minimere følelse av usikkerhet gjennom valg av teknologi, vektlegging av regelverk og formalia og behov for rapportering og kontroll.

Men der Hofstede forsøker å fange «essensen» i en nasjonalkultur, skal den sikkerhetskulturelle dimensjonen risikoaksept sees som et begrepsapparat for å forklare kulturelle delte mentale modeller som eierskapsfølelse knyttet til verdier, hva som er akseptabel atferd i situasjoner med identifisert risiko, og hvordan disse skaper mening rundt den opplevde risikoen blant medlemmene i en organisasjon. Med bakgrunn i den fortolkende tilnærmingen, skal man ikke plassere en organisasjon på en skala for å

predikere fremtidig atferd, men søke å forstå gjennom tykke beskrivelser av hvordan organisasjonens sensemaking-prosess peker i den ene eller andre retningen innenfor spekteret. Skalaen man kan benytte for å beskrive denne dimensjonen vil gå mellom defensiv, forsiktig risikoaversjon, til offensiv, opp mot skjødesløs «hybris».

6.4.4. Menneskesyn

Denne dimensjonen handler om hvor kulturens grunnleggende antagelser om mennesker, plasserer seg på et spekter mellom å se på mennesket som upålitelig og en sårbarhet som må styres, eller som en ressurs som ved riktig motivasjon, er det viktigste sikringstiltaket i en organisasjon. Dimensjonen innebærer også om organisasjonen kollektivt ser på mennesket som noe som kan påvirkes og formes av omgivelser og situasjonsfaktorer. Dette påvirker i tilfelle hvordan organisasjonen ser på og vurderer ledelse og ansatte, og hvilke systemer for styring og kontroll som vurderes som nødvendige og akseptable. Denne dimensjonen handler om tillitt til menneskers vurderinger og evner og den graden av autonomi man gir medlemmene på dette grunnlaget. Dette inkluderer graden av overvåkning og kontroll som organisasjonen mener er nødvendig og som medlemmene aksepterer som en del av de felles mentale modellene.

Dimensjonen fremstår kanskje spesielt relevant i personellsikkerhets-perspektiv, der man vurderer egne medlemmer som potensielle trusler. Men dimensjonen er på ingen måte irrelevant for de øvrige delene av sikkerhetsarbeid. Denne dimensjonen er relevant for hvordan man designer både fysiske og digitale sikkerhetssystemer, for hvordan man styrer tilganger og hvilke krav til autorisasjon for de enkelte medlemmene. Den kulturelle grunnleggende antagelsen rundt i hvor stor grad man kan stole på organisasjonens medlemmer, vil i stor grad påvirke både utforming og krav til bruk av slike sikringsystemer.

Dimensjonen handler ikke bare om å mistenke egne medlemmer for ondsinnet aktivitet. Det handler også og i hvor stor grad man stoler på at medlemmer vil klare etterleve policyer bruke de teknologiske sikkerhetstiltakene; hvor mye man kan stole på medlemmenes evner og kompetanse. Skal disse designes for å håndtere menneskelig feilbarlighet, eller designes som verktøy som mennesker skal bruke ut fra egne vurderinger?

Denne dimensjonen handler om de delte grunnleggende antagelsene om mennesker. Dette vil i sin tur påvirke de mer bevisste og uttalte verdiene og holdningene organisasjonen har vedrørende sine medlemmer. Er mennesker fundamentalt late og velger snarveier, eller yter mennesker så godt de kan i alle situasjoner? Er medlemmene en verdsatt ressurs i organisasjonen, eller er de midler for å oppnå mål?

Intervjuobjektene beskriver hvordan tillitt i organisasjoner, går begge veier. Denne dimensjonen handler ikke bare om ledelsens syn på sine medarbeidere, men også den tillitten medlemmer har til å rapportere svikt og sårbarheter. Har medlemmene tillitt til systemet og ledelsen, vil de også kunne akseptere kontroll og overvåkning.

I store komplekse organisasjoner, med stor utskifting av medlemmer, eller i organisasjoner som sikkerhets- eller etterretningstjenester der en insider kan gjøre stor skade, eller der medlemmene jobber mye selvstendig, kan det være hensiktsmessig med en mer «mistenksom» kultur og sterke kontrollregimer. Grunnleggende antagelser blir da at mennesker har for mange sårbarheter og laster som kan lett føre til at de blir motivert til å skade egen organisasjon. Innenfor menneskesynsdimensjonen er den ene enden av

spekteret, det Rossnes et al kaller en «syndebukk-kultur». Her rettes oppmerksomheten mot å finne en person som kan stå til ansvar, og svekker mulighetene for en åpen utprøving av årsakssammenhenger og fordomsfri leting etter bedre løsninger. En kultur med grunnleggende antagelser i denne enden av spekteret, vil ha sterke normer knyttet til å bevare egen status og manglende åpenhet i organisasjonen vil også være hemmende for organisatorisk læring (Rossnes et al 2013, s. 24). Holdninger og normer blir at man må eller bør overvåke medlemmene, for å kunne detektere eller avsløre når de trør over grensen.

På den andre siden, kan man i en liten organisasjon med engasjerte og dedikerte medlemmer med eierskap til verdiene, utvikle en grunnleggende antagelse og tiltro til den menneskelige faktoren som kapabel til å håndtere alle typer trusler, og undervurdere menneskers eksisterende og potensielle sårbarheter. Jo lenger ut i den andre enden av spekteret, jo høyere vurderes medlemmenes individuelle evne til å vurdere situasjoner. Kulturelle verdier som blir fremelsket er «sunn fornuft» eller «godt norsk bondevett» som sikkerhetsbarrierer. Normene og holdningene går på at det er mindre behov for og aksept for overvåkning og kontroll, fordi man både forventer at medlemmene løser situasjonen, og melder fra om svikt eller uønskede situasjoner.

I tillegg vil det kunne observeres gjennom diskursen som går på medlemmene og deres pålitelighet. Organisasjoner i den enden av spekteret som ser på mennesker som sårbarhet, snakker ofte om at sikkerhetens «svakeste ledd» er den menneskelige faktoren. Organisasjoner i den andre enden, vil heller snakke mennesket som «last line of defence» og fokusere på brukervennligheten i teknologiske sikkerhetstiltak, som svakheten i systemet. Nettopp denne diskursive forskjellen, ble trukket frem av flere av intervjuobjektene.

Denne dimensjonen kan kanskje best observeres gjennom de synlige artefaktene som man i hovedsak finner i styringsmekanismene; sikkerhetsstyring, kontroll- og overvåkingsregimer, prosedyrer og sanksjons- eller belønningssystem. Viser man tillit og gir autonomi til medlemmene, eller detaljstyrer og kontrollerer alt de gjør? I den ene enden hvor man ser på mennesket først og fremst som en sårbarhet, vil det være fokus på etterlevelse eller «compliance» av det som er vedtatt av regler og policyer. Jo lenger ut i denne enden av spekteret, jo mer overvåkning og kontroll vil man se. Det kulturelle handler om de delte mentale modellene for om dette er akseptert eller til og med ønsket, eller om det blir sett på som negativt, og hvordan dette oppfattes, fortolkes og utføres i en aktiv sensemaking-prosess.

Det er ikke slik at det er normativt bedre å se på medlemmene som positive garantister for sikkerheten i en organisasjon. Å være i ytterpunktet i denne enden av spekteret, er å fraskrive seg ansvar. Dersom man ikke ser menneskenes feilbarlighet, vil man heller ikke sørge for nødvendig kompetanse og kapasitet hos medlemmene til å håndtere både uønskede hendelser og utvikling av egne sårbarheter. Et grunnleggende positivt menneskesyn, trenger ikke innebære en total naivitet for at mennesker kan gjøre både bevisste ondsinnete handlinger og ubevisste feil og tabber.

Så selv om det semantisk kan forstås slik, så er heller ikke det å se på mennesket som en sårbarhet, ubetinget negativt. Å kontrollere kan skape trygghet, og ta bort noe av ansvaret fra enkeltmedlemmet og legge det over på organisasjonen.

Derfor er det igjen viktig å se sin egen organisasjon, de på verdier og sårbarheter, kompleksiteten i egen organisasjon, om sikkerhetssystemet er håndterbart for

medlemmene osv. og finne det stedet på spekteret som fungerer hensiktsmessig for egen organisasjon. Så kan man fortolke hvordan dette fungerer i praksis, og søke å tette gapet mellom ønsket og reell kulturell plassering på spekteret.

6.4.5. Relasjoner/konfliktaksept

Denne dimensjonen ser på hvordan relasjoner betraktes i en organisasjon. Det innebærer nærhet i de interne relasjonene i en organisasjon, men også hvorvidt man betrakter konflikter som noe utelukkende negativt, eller om det finnes positive sider ved konflikt. For lavt eller for høyt konfliktnivå, basert på hva som er hensiktsmessig i den enkelte organisasjon, vil dermed være av negativ betydning (Rossnes et al 2013, s. 25). Oppfattes det sosiale som en viktig del av organisasjonen? Eller er formålet, produksjonen eller resultatene det altoppslukende for organisasjonens medlemmer? Nye grupper eller organisasjoner, vil kanskje ikke ha etablert trygge, forutsigbare sosiale relasjoner, noe som kan påvirke hvor man plasseres på spekteret i denne dimensjonen.

Flere intervjuobjekter nevner spesialavdelinger i Forsvaret eller politiet som HRO'er med nære relasjoner og stor aksept for konflikt og/eller direkte tilbakemeldinger. «Å ta opp feil med enkeltmann er uproblematisk- Det er vi vant til. Vi evaluerer alle oppdrag. Vi korrigerer hverandre systematisk under trening,» siterer Malin Stensønes i sin bok basert på samtaler med politiets beredskapstropp (2017, s. 53). Forsvarssjef Eirik Kristoffersen beskriver tilbakemeldingskulturen i Forsvarets Spesialkommando som «nådeløst ærlig, men ikke ydmykende» (2020, s. 138). Disse HRO'ene, er kanskje ikke målestokken alle organisasjoner bør sammenligne seg med. Men som det ene intervjuobjektet forklarte handler det om «å gi hverandre tilbakemeldinger, korrigere hverandre, men implisitt hjelpe hverandre». Tonen slike avdelinger har, ville sannsynlig ikke fungert på enhver arbeidsplass. Men det skjer ut fra en totalforståelse at man er avhengig av direkte og tydelige tilbakemeldinger med en felles forståelse av at dette gjøres for alles beste, kan skape positive ringvirkninger. HRO'er kjennetegnes blant annet av at de ser på feil som muligheter for læring. Rosness beskriver disse som «error friendly learning culture». De fremelsker atferd som tilbakemelding, informasjonsdeling, rom for å be om hjelp og åpenhet rundt svikt og feil, og skape rom for å uttrykke skepsis. Dette skaper initiativ hos medlemmene til å identifisere og utbedre feil og mangler, og man øker intern kontroll mellom medlemmene, uten å samtidig miste trygghet, autonomi og tillitt (Rosness et al 2010, s. 58-61).

Psykologisk trygghet handler om i hvilken grad medarbeidere føler seg trygge på at de kan si hva de mener uten å frykte negative konsekvenser, slik som tap av jobb eller forfremmelsesmuligheter, og at man ikke vil ydmyke, avvise eller straffe hverandre for å uttrykke sine meninger eller tanker (Edmondson, 1999). Schein (1965) fremhever opplæring, involvering, inkludering av alle, få frem gode forbilder, og å støtte hverandre som sentrale elementer for å fremme psykologisk trygghet. Clark (2020) trekker også frem inkludering og læring, forstått som det å tørre å bidra og å utfordre tilstanden i en endringsprosess.

Samtidig vil et altfor høyt konfliktnivå, der man ikke tar hensyn til situasjon og andres individuelle emosjonelle tilstand, skape negative effekter. I grupper hvor det er sterke konflikter mellom ulike interesser, skjulte agendaer og vikarierende motiver vil betingelsene for gode læringsprosesser ikke være til stede. Men et visst konfliktnivå av forskjellige mentale modeller kan være et gode, særlig når organisasjonen kjennetegnes av åpenhet og høy takhøyde (Rossnes et al 2013, s. 25).

De grunnleggende antagelsene vil variere mellom hvorvidt man ser på konflikt som noe utelukkende negativt, eller som muligheter for utvikling og forbedring. Blant annet gjelder dette holdninger til konflikter; om det er greit å si ifra om man er uenig, om det er takhøyde for å komme med nye forslag, og man kan komme med tilbakemeldinger, om holdningen til avviksrapportering er at det er en kilde til forbedring eller en måte å fordele skyld på. Selv om det er en grunnleggende antagelse, at tilbakemeldinger skal gis direkte og saklig, vil man måtte balansere dette opp mot andre hensyn. Menneskers sosiale omgang er ikke basert på rene fakta, men også på et hierarki og sosiale mekanismer som preger trivsel og opplevd trygghet. Et trygt arbeidsmiljø ble trukket frem av intervjuobjektene som er «godt sikkerhetstiltak». Holdninger og verdier innen denne dimensjonen inkluderer hvor stor vekt man legger på det psykososiale arbeidsmiljøet og den psykologiske tryggheten i organisasjonen. «Takhøyde» benyttes som en positiv skildring i den enden av spekteret, mens det i den andre beskrives som «stormfullt» eller «fiendtlig».

Synlige artefakter ved denne relasjonen, kan være de planlagt sosiale arrangementene; fra julebord, sommerfest eller vinlotteriet på fredager. Skaper disse arenaene positivt engasjement, og anses de som viktige for trivsel og motivasjon?

De synlige artefaktene inkluderer i tillegg avviksrapporteringens form og mengde; kan man si ifra om kritikkverdige forhold, feil, mangler, svikt i egen eller andre bruk av sikkerhetssystemet osv.? Eller vil de negative sosiale konsekvensene hindre slik rapportering? Men også om man kan observere tilbakemeldingsklimaet slik det eksempelvis er beskrevet i elitestyrkene til politiet og Forsvaret. Intervjuobjektene beskrev at avviksrapportering er med på å forme hvordan man tenker og identifiserer seg som enhet. Det handler om deltakelse og engasjement i felles jobbmøter. Sier man ifra når man er uenig, eller «hilser man til lua» og følger konvensjoner og flertallet? Preges organisasjonen av konfronterende eller unnvikende konfliktatferd? Kan man være uenige, eller undertrykkes konflikter og «feies under teppet»?

Flere av disse artefaktene, og et element i hele dimensjonen, korrelerer med hva som er akseptert distanse mellom ledd i organisasjonshierarkiet og grunnleggende antagelser og holdninger til makt. Aksepterer kulturen stor maktdistanse, og maktbruk av ledere, eller er egalitet og likhet og flat struktur en organisatorisk grunnverdi? Er organisasjonen preget av stor maktdistanse og/eller sosial distanse mellom medlemmer «på gulvet», mellomledere og toppledelsen? Eller er det sosiale relasjoner mellom og møtepunkter for direktøren og operatøren? Kan korporalen sette seg ned i lunsjen og snakke med obersten, og kan mellomlederen lufte sine personlige standpunkt i allmøtet?

Igjen kan vi se elementer fra Hofstedes dimensjoner (1980), denne gangen dimensjonen *maktdistanse*. Men igjen skal ikke organisasjonen tildeles en skår på en skala. Den fortolkende tilnærmingen skal utlede tykke beskrivelser av sosial atferd, rapportering og kommunikasjonsklima, forankret i holdninger, verdier og normer, som igjen er fundert på grunnleggende antagelser.

Relevansen for sikkerhet bunner i hvorvidt kulturen skaper et klima for å melde fra om avvik som forringer sikkerheten; om de som jobber i førstelinje kan melde fra om forbedringspunkter eller påpeke mangler ved de sikkerhetstiltakene de forvalter. Og om det er rom for det et intervjuobjekt kalte «konstruktiv uenighet» som basis for å utvikle kulturen i mer hensiktsmessig retning.

Sterke sosiale relasjoner kan skape trygghet til å si ifra, men kan også hemme avviksrapporing fordi man ikke vil utlevere kollegaer. Hvor vidt organisasjonskulturen aksepterer at man sier ifra, og tåler å stå i konfliktsituasjoner, er en viktig del av dette. Personellsikkerhetsmessig, er det essensielt for deteksjon av innsidere, eller personer med sårbarheter som kan utnyttes av en ondsinnet trusselaktør, at andre medlemmer vil og tør si ifra om bekymringer de måtte ha. Samtidig vil et konstant høyt konfliktnivå, kunne virke negativt for sikkerheten, ved at misfornøyde medlemmer som føler seg urettferdig behandlet, utvikler et nag som kan føre til at man ønsker å skade organisasjonen sin.

Hva som er hensiktsmessig må vurderes for hver organisasjon, og baseres på forhold som organisasjonens størrelse og kompleksitet, forum og arenaer for meningsutvekslinger, organisering og distanse mellom enheter, og selvfølgelig risikovurderinger for hele organisasjonen.

6.5. Hvordan kan ledere benytte seg av denne tilnærmingen til sikkerhetskultur?

Som det ene intervjuobjektet formulerte det: «*Det er den eneste konstanten med kultur – at den endrer seg.*» En leder som tar det organisasjonskulturelle på alvor, og ønsker å jobbe aktivt med utvikling av denne vil kunne benytte seg av de beskrevne dimensjonene for å gjøre seg opp en mening om hva som er hensiktsmessig og ønskelig, og hva som er den gjeldende kulturen i organisasjonen.

En forutsetning for å manøvrere i det vanskelig tilgjengelige landskapet som er organisasjonskultur, er å vite hvor man er. Jeg har i denne oppgaven stilt kritiske spørsmål rundt måling av sikkerhetskultur. Det hersker en oppfatning blant enkelte både ledere og sikkerhetsfaglige eksperter, at dette kan gjøres. Jeg vil trekke frem det ene intervjuobjektet, som har utviklet et kommersielt verktøy som gir en skår innenfor det han definerer som sikkerhetskultur. Intervjuobjektet uttrykte at for å kunne jobbe med sikkerhetskulturen i en organisasjon, er det essensielt at man måler hvor man er og skaper en baseline som man kan jobbe ut fra. Dette beskrives også i faglitteraturen, blant annet i boken med tittelen *The Security Culture Playbook*: «*The culture you measure doesn't live in a black box; it is greatly influenced by a host of factors you may not think to consider*» (Carpenter og Roer, 2022, s. 119).

Refleksjonene hos intervjuobjektene rundt om og hvordan man kan måle eller kartlegge sikkerhetskulturen, var på samme måte som all kulturell forskning og kommersiell virksomhet, delte. Jeg har i denne oppgaven drøftet meg frem til noen parametere, som vil kunne benyttes av ledere for å starte denne tilnærmingen.

Den første delen er forståelsen av sikkerhet som begrep. Her har jeg understreket kompleksiteten mellom det teoretiske og det praktiske, og den iboende usikkerheten når man skal vurdere risiko. Videre har jeg understreket at sikkerhet er en kontinuerlig prosess og ikke et prosjekt med en start- og sluttdato.

Deretter har jeg drøftet kulturbegrepet, og kommet frem til en tilnærming til det kulturelle som delte mentale modeller. I dette ligger det at det ikke er snakk om individuell kunnskap og atferd, men hvordan medlemmene fortolker og skaper mening ut av verden rundt seg.

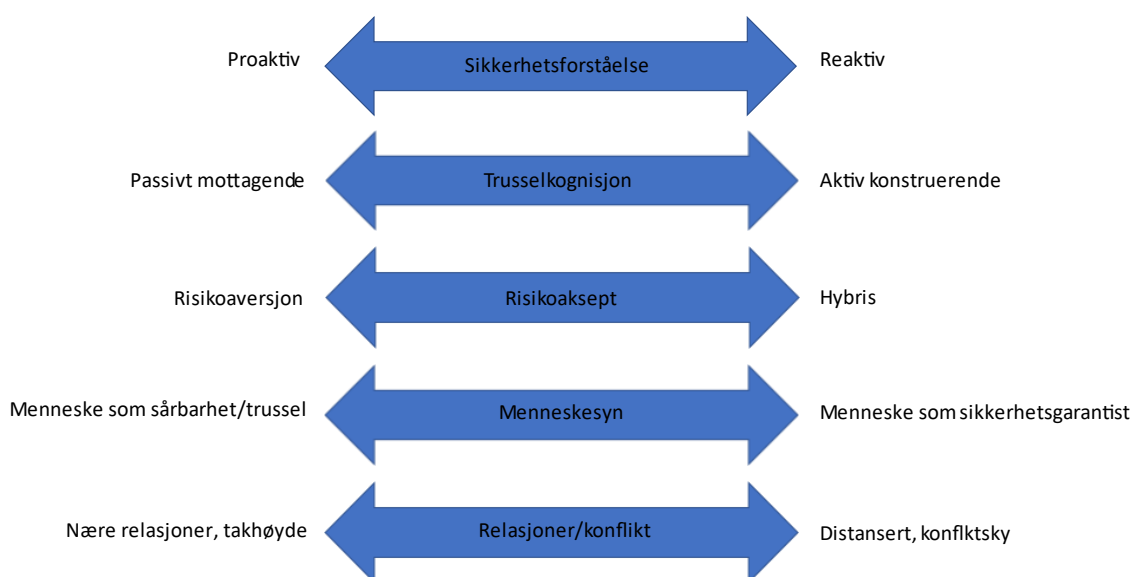
Bruken av mentale modeller som illustrasjon, skaper forståelse av at dette handler om hvordan vi oppfatter og fortolker verden rundt oss. Sensemaking-prosessen som skaper og utvikler de delte mentale modellene, understreker det kollektive og kontinuerlig

utviklende aspektet ved kultur. Elementet med felles meningsystemer bygger under at dette er sosiale prosesser som skapes i fellesskap i en gruppe eller organisasjon. Sikkerhetskulturen er den delen av dette som kan påvirke den kontinuerlige sikkerhetsprosessen.

En slik forståelse vil ikke forenkle jobben til en leder, men den vil skape et mer realistisk utgangspunkt for bevisst ledelse for å oppnå et mål. Måling av de synlige artefaktene, f.eks. sikkerhetsatferd som etterlevelse av retningslinjer eller bruk av sikkerhetssystemer, vil fungere som symptomer; på linje med tett nese og rennende øyne. Men vil man diagnostisere hvorfor det er slik, må man søke forklaringen gjennom tykke beskrivelser ned på de grunnleggende antagelsene.

Bevissthet og aktive valg er ikke en garanti for ønsket kulturendring. Kai Roer beskriver at organisasjonskultur oppstår blant annet gjennom felles erfaringer og forståing som man får gjennom regelmessig samvær, som på jobben. Han hevder at endring er mulig gitt kulturen sin «plastiske» dynamiske egenskap (Roer 2015, s. 12). Dette er hovedpoenget i teorien om sensemaking som en kontinuerlig sosialiserende prosess. Men som hovedregel er kulturendring i organisasjoner, en svært langsiktig, gjerne årelang prosess (Kaufmann & Kaufmann 2015, s. 372-376). At det er mulig, men likevel vanskelig uten å kunne garantere ønsket resultat, støttes av denne oppgavens informanter.

Poenget er å skape forståelse for hva en leder beskriver som sikkerhetskulturen i egen organisasjon. Kontra målinger av antall sikkerhetsavvik eller prosentandelen som åpnet en phishingtest-epost, eller hvor mange som gjennomføre e-læringskurset i oktober, for å beskrive sikkerhetskulturen, foreslår jeg fem dimensjoner på det grunnleggende antagelses-nivået: Sikkerhetsforståelse, Trusselkognisjon, Risikoaksept, menneskesyn og relasjon/konfliktdimensjonen. Disse dimensjonene tar utgangspunkt i tidligere kulturmodeller, men er gjennom denne oppgaven utarbeidet spesifikt for sikkerhetskultur. Jeg har drøftet hver dimensjon inngående i forrige avsnitt, basert på teori og refleksjoner fra intervjuobjektene.



Figur 4: Sikkerhetskulturelle dimensjoner

Formålet er å skape et begrepsapparat for organisasjoner og ledere som ønsker å bevisstgjøre seg egen sikkerhetskultur, og i neste rekke jobbe aktivt med å utvikle den. Det gjentas at disse dimensjonene, selv om de beskrives på spektre, ikke er normative vurderingsskalaer, som har en idealskår alle må strebe etter. Poenget med modellen er at ledere kan definere hvor man mener at egen organisasjon skal ligge på disse spektrene, for at kulturen skal bidra til å oppnå et hensiktsmessig sikkerhetsnivå.

Når dette nivået er beskrevet, kreves det en fortolkende tilnærming til egen organisasjonskultur. Det anerkjennes at dette er en vanskelig prosess, og at man ikke får en klinisk diagnose med to streker under svaret. Man får en fortolkning med tykke beskrivelser av egen organisasjonskultur. Og ved å bruke dette begrepsapparatet, kan man forklare funn i medarbeiderundersøkelser, revisjoner, penetrasjonstester eller avvik.

Det er i oppgavens drøfting, konkludert med at kultur som mentale modeller, er i konstant endring gjennom aktive sensemaking-prosesser mellom medlemmene. Det naturlige neste spørsmålet er hvorvidt en leder eller ledelse, aktivt kan påvirke og utvikle sikkerhetskulturen i egen organisasjon. Alle intervjuobjektene i denne oppgaven, var enige om at det var en mulig, men samtidig vanskelig og tidkrevende oppgave. Å jobbe med kulturutvikling er en kontinuerlig prosess som inkluderer det man sier og gjør i det daglige. «Utvikling av kultur er ikke vanskelig,» uttrykte et av intervjuobjektene med begrunnelse i at sosialisering og mellommenneskelig konstant påvirker og videreutvikler kultur.

Ledelse blir av et av intervjuobjektene presisert som:

«å påvirke en gruppe mennesker mot å oppnå organisasjonens mål, der sikkerhet handler om mulige hindringer mot å nå disse målene.»

En annen formulerte det som at:

«Tenker man på kultur som delte mentale modeller, så er ledelse en av forutsetningen for å skape eller sikre et slik sosialt fellesskap».

Sikkerhetskultur påvirker organisasjonens evne til å nå sine mål. Å aktivt jobbe med å utvikle kulturen mot det som er mest formålstjenlig, her med fokus på en hensiktsmessig sikkerhetskultur, er derfor å anse som et lederansvar. I ledelsesteorien er dette lederansvaret eksempelvis formulert av Northouse:

«Leadership is a process whereby an individual influences a group of individuals to achieve a common goal» (Northouse 2019, s. 5).

Med forutsetningen om at det er en leders pliktet å jobbe med utvikling av sikkerhetskultur, må vi ta innover oss leders maktposisjon og hvordan man kan benytte sin makt til denne type endringsarbeid. Jeg har i teoridelen beskrevet hvordan ledelse innebærer et maktspekt, og at dette av Rossnes et al (2013), beskrives som underkommunisert. Styring, kontroll og tilsyn, og organisatorisk læring forutsetter en eller form for bruk av makt i en eller annen form (Rossnes 2013 et al, s. 27).

Eksempelvis kan en leder søke å bevisst påvirke sikkerhetsforståelsens kulturelle element i en organisasjon. Mennesker og organisasjoner vil alltid lære av operasjoner som blir sett på som suksessfulle (Rossnes 2016, s. 2). Dette skjer i det daglige, men kan også styres gjennom ledelse etablerte mekanismer; rapportering, debrief, evaluering, simulering og øvelser (Rossnes 2016, s. 13). Hva en leder vektlegger i sin

definisjon av suksess, og hvordan dette formidles, vil kunne påvirke de grunnleggende antagelsene om hva sikkerhetsarbeid betyr. Legger leder vekt på hvordan beredskapen mobiliserte og håndterte hendelser, og klarte å avbryte et angrep og minimere konsekvensene, drar det i den reaktive retningen. Legger leder i stedet vekt på 0-visjoner for sikkerhetshendelser, og de erfaringene der barrierene har stanset angrep, vil det kunne påvirke kulturen i den proaktive retningen. Krav om etterlevelse av proaktive sikkerhetstiltak, skaper en rutinisering som etterfølges av normalisering – en grunnleggende antagelse om at «slik skal det være».

Ønsker en leder å oppnå aktivt engasjement rundt trusselbildet, vil det være mest hensiktsmessig å bruke innflytelsesmakt, kontra de mer tvangs- og styrkepregede makttypene. Prinsippene i transformasjonsledelse, herunder idealisert påvirkning og intellektuell stimulering, vil også kunne bidra til å skape engasjement om å beskytte organisasjonens verdier mot identifiserte trusler. Å gi trusselpresentasjoner prioritet i arbeidshverdagen, vise at ledelsen fokuserer på slik bevissthet, og benytte mer inkluderende og aktiviserende plattformer for deling av informasjon, kan en leder påvirke denne dimensjonen.

Innenfor risikoakseptdimensjonen, vil en leders oppgave blir å skape minst mulig avstand med det som er vedtatt som akseptabelt risikonivå, og det som er den kulturelle mentale modellen i organisasjonen. Et klart og tydelig budskap, og en maktutøvelse rettet mot de daglige praksisene i form av dominans og disiplin, vil kunne gi ønsket effekt. Her er det viktig å knytte tydelige insentiver til hvordan man forholder seg til risiko, og således kan transaksjonsledelsesstil, fungere bedre innenfor denne dimensjonen. Leder kan altså påvirke de mentale modellene gjennom å markere tydelige formelle strukturen som medlemmene tvinges til å forholde seg til.

Dimensjonen som omhandler menneskesyn, kan f.eks. påvirkes av en leder, ved å fokusere på den gjensidige tillitten i organisasjonen. Å bygge tillitt gjennom inkluderende lederstil, og bruke både eksplisitte og implisitte rammer for sosialt akseptabel atferd, kan benyttes for å bygge under de verdiene eller dydene man ønsker å utvikle (Rossnes et al 2013, s. 24).

En leder som vil påvirke relasjons- og konfliktdimensjonen, kan f.eks. gjøres gjennom konkret styrt erfaringslæring. Her kan en leder dyrke og fremheve verdien av avviksrapportering som noe positivt og utviklende, og slik skape en «error friendly learning culture». Dette vil kunne påvirke de grunnleggende antagelsene om dette, og holdningene til å rapportere avvik. Systemisk styring bør også inkludere uformelle arenaer der man søker å skape et kommunikasjonsklima, men også uformelle interne relasjoner i den retningen man har vurdert som hensiktsmessig.

Denne oppgaven har ikke som ambisjon å lage en «bruksanvisning» for ledere, som man punktvis kan følge for å komme fra a til å. Dette er et så komplekst tema, at det vil kreve både ytterligere forskning og praktisk utprøving for å finne «best practice». Men det vil likevel være spesifikke utfordringer, prosesser og sammensetninger innenfor de sikkerhetskulturelle dimensjonene, i hver enkelt organisasjon. Og en leder må ta utgangspunkt i egen situasjon og finne den veien og de metodene som man tror vil kunne fungere best.

7. Konklusjon/oppsummering

Gjennom denne oppgaven har jeg ønsket å knytte sammen sikkerhetsfaget med kulturfaglige teorier, for å skape en forståelse og et felles begrepsapparat som kan tjene som verktøy for ledere som ønsker å utvikle egen sikkerhetskultur. Det er et enormt komplekst tema, og det er veldig mange undertema uten klare definisjoner eller samstemthet, hverken innenfor det praktiske sikkerhetsfaget eller det teoretiske kulturfaget. Bare å begrepsavklare «sikkerhet» og «kultur» hver for seg, har vært en utfordring. Gjennom drøfting har jeg kommet frem til en forståelse og begrepsbruk som denne studien baserer seg på. Det var aldri ambisjonen for denne oppgaven, å etablere universelt aksepterte definisjoner for hverken kultur-, sikkerhets- eller sikkerhetskulturbegrepet. Men mine delkonklusjoner vil fungere både i et teoretisk og praktisk videre arbeid med sikkerhetskultur.

Gjennom en redegjørelse for sikkerhetsfagets praksis, fra risikovurdering, gjennom tiltakssetting og beredskap, til styring og ledelse, har jeg kommet frem til følgende definisjon av sikkerhetsbegrepet:

Proessen, inkludert det teoretisk-analytiske og det praktisk-operative arbeidet med formål å redusere og håndtere risikoen for uønskede tilskete hendelser utført av ondsinnede bevisste trusselaktører.

Opgavens teoridel er todelt. Den første delen av teorikapittelet handler om tilnærming og forståelse av kulturbegrepet. Jeg har argumentert for en forståelse av kultur som delte mentale modeller som skapes gjennom uformelle, kollektive, konstruksjonistiske sensemaking-prosesser. Teorikapittelet synliggjør videre hvordan teorier knyttet til sikkerhetsfaget som teorier om høypålitelighetsorganisasjoner og organisatorisk læring, beviser relevansen til det kulturelle innenfor fagområdet sikkerhet.

Opgaven argumenterer for at sikkerhetskultur skal forstås som en del av organisasjonskulturen, og foreslår følgende definisjon av sikkerhetskulturbegrepet:

De delte mentale modellene innenfor en organisasjon, som danner felles meningssystemer for medlemmene innenfor rammene av sosialt samspill og prosessene som påvirker forståelsen for og utførelse av sikkerhet i organisasjonen.

Jeg har drøftet hvordan man kan beskrive og bedømme sikkerhetskultur. Gjennom dette har jeg konkludert med at det ikke finnes en objektiv standard for god eller dårlig sikkerhetskultur, men hensiktsmessige kulturer for hver enkelt organisasjon, vurdert ut fra hva som bidrar positivt til å beskytte organisasjonens verdier og samtidig ikke hindrer organisasjonens måloppnåelse. For å kunne vurdere sikkerhetskultur har jeg derfor presentert en modell med fem dimensjoner som kan brukes for å kvalitativt fortolke de grunnleggende kulturelle mentale modellene som påvirker sikkerhetskulturen: Sikkerhetsforståelse, trusselbevissthet/-kognisjon, risikoaksept, menneskesyn og relasjoner/konflikter.

Gjennom empiri, der sikkerhetsfaglige eksperter har reflektert rundt sikkerhetsfaget, sikkerhetskulturbegrepet, de nevnte dimensjonene og hvordan sikkerhetskultur kan måles og utvikles, fremkommer det klart at det mangler et felles begrepsapparat. Empirien viser tydelig at det er ulik forståelse av sikkerhetskultur som begrep og hva dette inkluderer. Studiens funn viser at det er særlige utfordringer knyttet til sikkerhetsfaget, som gjør det kulturelle aspektet ved sikkerhet, relevant. Funnene viser

en trend i oppfatningen blant sikkerhetsekspertene, om at sikkerhetskultur kan kartlegges og bevisst styres, men det er ulike oppfatninger rundt hvordan dette kan gjøres og hvor vanskelig det er.

Intervjuobjektene reflekterer rundt de sikkerhetskulturelle dimensjonene jeg har identifisert i teorikapittelet, deres forståelse av disse, og vurderinger av relevans og nytteverdi, styrker antagelsen om behovet for et felles begrepsapparat – her forstått som de sikkerhetskulturelle dimensjonene – for å kvalitativt analysere og beskrive, og formulere hva som er hensiktsmessig sikkerhetskultur for den enkelte organisasjon.

Opgavens drøftingsdel styrker vurderingen av fortolkende kvalitativ tilnærming til sikkerhetskultur som mer hensiktsmessig og nyttig. Jeg har argumentert for at en essensialistisk tilnærming vil kunne avdekke «symptomer» tilgjengelige gjennom kulturens synlige artefakter, men at for å «diagnostisere» eller forstå hvorfor kulturen får disse utslagene, må man fortolke seg ned til de grunnleggende antagelsene. Dette betyr at måling av synlige artefakter som atferd, etterlevelse av policyer og avviksrapportering, kan være nyttige inngangsverdier for å bevisstgjøre seg egen organisasjons sikkerhetskultur, men ikke fyllestgjørende for en leder som aktivt ønsker å bevisstgjøre seg og jobbe for å utvikle eller endre egen organisasjons sikkerhetskultur.

Opgaven drøfter videre i hvilken grad det er mulig for en leder å bruke denne bevisstheten og aktivt påvirke sikkerhetskulturen i ønsket retning. Det er denne oppgavens konklusjon at det er ikke bare mulig, men et lederansvar å søke å utvikle organisasjonskultur på en bevisst måte. Ledelse handler om å påvirke en gruppe mennesker mot å oppnå organisasjonens mål. Og sikkerhet handler om å motvirke mulige hindringer mot å nå disse målene, og faller derfor innunder leders ansvar.

Gitt at forskjellige organisasjoner har et vidt spekter av forutsetninger og premisser, er det ikke denne oppgavens mål å lage en oppskrift for hvordan den enkelte leder kan drive slikt utviklings- og endringsarbeid. Kultur kan ikke vedtas på et styremøte, eller kjøpes av en leverandør. Men ved å bruke de sikkerhetskulturelle dimensjonene kan man utvikle «tykke beskrivelser» og kvalitative vurderinger av hvor man står og hvor man ønsker å utvikle seg. Ansvar og utviklingsarbeidet fordrer både denne bevisstheten som dimensjonene kan bidra til, og aktivt arbeid der ledere må bruke de verktøy man har til rådighet, inkludert forskjellige lederstiler og makttyper, valgt på bakgrunn av den identifiserte veien fra standpunkt til mål.

Sikkerhetskultur kan ikke besluttes, men må utvikles i det sosiale samspillet innad i organisasjonen. Alle organisasjoner har en sikkerhetskultur som er i konstant utvikling, påvirket av eksterne faktorer som trusselbildet, og av interne formelle og uformelle prosesser. Bevisst og aktivt lederstyrt arbeid er ikke en garanti for endring til en optimal kulturell tilstand. Den beskrevne sensemaking-prosessen som danner de mentale modellene, påvirkes av alle organisasjonens medlemmer gjennom uformelle og konstante sosiale prosesser. Men det står som en konklusjon etter det omfattende arbeidet som ligger til grunn for denne oppgaven, at det både er et ufravikelig ansvar og faktiske muligheter å drive et formålsstyrt utviklings- og endringsarbeid for å utvikle en hensiktsmessig sikkerhetskultur. Sikkerhet er et lederansvar, og det må være en leders mindset å bevisst kontinuerlig jobbe med og ikke mot sin organisasjons medlemmer, for hele tiden å styre kulturen mot en hensiktsmessig og formålstjenlig kulturell tilstand.

7.1. Studiens begrensninger og forslag til videre arbeid med tematikken

Denne oppgavens funn og konklusjoner, setter opp et teoretisk rammeverk og foreslår et begrepsapparat som kan benyttes av ledere for å kartlegge, fortolke og beskrive sikkerhetskultur i egen organisasjon. Men det innrømmes at dette er et tidlig steg i en utvikling av et relativt nytt fagområde. Som tidligere nevnt er sikkerhetskultur slik denne oppgaven definerer det opp mot *Security*, et begrep som kun har vært i bruk i drøye 10 år.

Resultatet kan beskrives som en forståelsesmåte utviklet i brytningen mellom praksis fra sikkerhetsfaget innhentet i empirien gjennom intervjuer med fageksperter, og det teoretiske grunnlaget som er presentert i denne oppgaven. Selv om oppgaven bygger på ekspertenes erfaringer og refleksjoner, er oppgavens konklusjoner ikke utprøvd som praktisk verktøy. Kulturstudier og teoriutvikling kan ikke valideres gjennom eksperimenter, og en forståelsesmodell har kun nytteverdi dersom den aksepteres av de som det er tenkt skal bruke den.

Det vil kreve aktiv innsats å tydeliggjøre resultatene, herunder å argumentere for deres troverdighet og bruksverdi. Å lage presentasjoner som tar hensyn til den eksisterende diskursen rundt temaet sikkerhetskultur, vil øke sjansen for at denne forståelsesmodellen treffer aktuelle mottakere, at de oppleves som relevante og kan generaliseres og tas i bruk (Andenæs, 2001).

Opgaven har ikke testet denne tilnærmingen og metodikken på reelle organisasjoner. Hvordan dette utviklings- og endringsarbeidet i praksis kan operasjonaliseres, og den praktiske nytteverdien er dermed ikke validert gjennom faktisk bruk. Hvordan en leder i praksis vil benytte dette begrepsapparatet, og hvordan han vil operasjonalisere dimensjonsmodellen, vil kreve et ytterligere arbeid. Videre anvendelse av modellen vil måtte evalueres både teoretisk, og opp mot den nytteverdien sikkerhetspraktikere og ledere ser i resultatet.

Videre arbeid med å skape et felles begrepsapparat, og å teste og utvikle denne oppgavens sikkerhetskulturelle forståelsesmodeller, vil måtte gjøres i samspill med sikkerhetspraktikere og ledere med sikkerhetsansvar. Konkrete erfaringer og evalueringer av disse, kan skape «best practises», og et grunnlag for å videreutvikle analysemetodikk av det sikkerhetskulturelle, og ledelsesteori for sikkerhetsledere.

Litteraturliste:

- Abelson, R. P. (1976). *Script Processing in Attitude Formation and Decision Making*. J. S. Carroll & J. Payne, (eds) Cognition and Social Behavior. Hillsdale, NJ: Erlbaum
- Albrechtsen, E. (2003). *Security vs Safety*. NTNU- Norwegian University of Science and Technology. Department of Industrial Economics and Technology Management.
- Ali, H. H. (12.09.2022). En ung muslimsk jente. Er det virkelig ingen håp for politidrømmen. Aftenposten, si ;D. Tilgjengelig fra: <https://www.aftenposten.no/meninger/sid/i/APIzpn/en-ung-muslimsk-jente-er-det-virkelig-ingen-haap-for-politidroemmen>
- Allaire, Y. & Firsirotu, M. E. (1984). *Theories of Organizational Culture*. Tilgjengelig fra: <https://journals.sagepub.com/doi/abs/10.1177/017084068400500301?journalCode=ossa>
- Andenæs, A. (2001). *Generalisering: Om ringvirkninger og gjenbruk av resultater fra en kvalitativ undersøkelse*. I H. Haavind. (red). *Kjønn og fortolkende metode. Metodiske muligheter i kvalitativ forskning*. Gjøvik: Gyldendal Akademisk
- Askehave, I. (2006) *Communication: Transmitting messages or fusing horizons*. Academica, Århus
- Aven, T. (2007). *Risikostyring*. Universitetsforlaget
- Axelrod, R. (1976) *Structure of Decision: The Cognitive Maps of Political Elites*. Princeton, NJ: Princeton University.
- Balakrishnan, V. & Humaidi, Norshima (2015). *Leadership Styles and Information Security Compliance Behaviour: The Mediator Effect of Information Security Awareness*. International Journal of Information and Education Technology, Vol. 5, No. 4, April.
- Bang, H. (1988). *Organisasjonskultur*. Tano Aschehoug
- Becker, H. S. & Geer, B. (1960). *Participant Observation: The Analysis of Qualitative Field Data*. R. Adams and J. Preiss, Eds., Human Organization Research, The Dorsey Press, Homewood
- Befring, E. (2007): *Forskningsmetode med etikk og statistikk*. Samlaget
- Berger, S. (2021). *Morgendagens beredskap et lederansvar*. Tilgjengelig fra <https://openarchive.usn.no/usn-xmlui/bitstream/handle/11250/2771247/no.usn%3awiseflow%3a2498278%3a43261501.pdf?sequence=1&isAllowed=y>
- Bjerkøy, V. (2013). *Hva er norsk kultur?* Aftenposten. Tilgjengelig fra: <https://www.aftenposten.no/meninger/debatt/i/oRjr0/hva-er-norsk-kultur>
- Bjørklund, R. A. (1997). *Politipsykologi*. Vett & Viten
- Borgerud, I. M., Finstad, L., Nylund, M. H., Christensen, E., Kassman, A., Fredriksen, S. & Lynum, C. (2021): *Politikorrupsjon. Lederskap, risikokerkjennelse og læring*. Oslo: Politidirektoratet
- Bremer Mærli, M. (2012). *Risikobasert sikring (Security) og risikoreduksjon*. Notat 8/12. Det Norske Veritas
- Brodt, S. E. & Dietz, L. E. (1999). *Shared Information and Information-Sharing: Understanding Negotiation as Collective Construal*, R. J. Bies & R. J. Lewicki (eds) Research in Negotiation in Organizations, Vol. 7. Stamford, CT: JAI, 263–83
- Bruusgaard, D. 11.01.2022: *diagnose*. Store medisinske leksikon. Tilgjengelig fra: <https://sml.snl.no/diagnose>

- Buchanan, D. A. & Huczynski, A. (1997). *Organizational behaviour: an introductory text*. Prentice Hall, London.
- Busmundrud, O. (08.01.2019) *Sannsynligheter og usikkerheter - begrepsavklaring i forbindelse med risikovurderinger*. Forsvarets Forskningsinstitutt (FFI-rapport 18/02058).
- Cameron, K. S., & Quinn, R. E. (2013). *Identifisering og endring av organisasjonskultur: De konkurrerende verdier*. Oslo: Cappelen Damm.
- Carpenter, P. & Roer, K. (2022). *Security Culture – Playbook*. Wiley
- Clark, T. R. (2020). *The 4 stages of psychological Safety: Defining the path to inclusion and innovation*. Berrett-Koehler Publishers.
- Conway, A.R., Cowan, N.A. & Bunting, M.F. (2001). *The cocktail party phenomenon revisited: The importance of working memory capacity*. Bulletin and Review, 8, 331-335
- Cox, S. & Flin, R. (1998). *Safety culture: Philosopher`s stone or man of straw*. Work and Stress, 12 (3), ss. 189-201
- Croll, M. (2023). *THE RISE OF SECURITY and Why We Always Want More*. Universal Publishers, Inc, Boca Raton.
- Daft, R. L. & Weick, K. E. (1984). *Toward a Model of Organizations as Interpretation Systems*, Academy of Management Review, 9, 284–95.
- Deal, T.E. & Kennedy, A.A. (1982). *Corporate Cultures: The Rites and Rituals of Corporate Life*. Addison Wesley Publishing Company, Reading, 126.
- Denis G. (2022): *Minute Tools Content Team, Edgar Schein`s Organizational Culture Model*. Tilgjengelig fra: <https://expertprogrammanagement.com/2022/09/edgar-schein-culture-model/>
- Deter, J., Schroeder, R. & Mauriel, J. A. (2000). *Framework for linking culture and improvement initiatives in organisations*. The Academy of Management Review 2000;25(4):850–63.
- Difi (2017) *Evaluering av nærpoltireformen. Underveisrapportering om kultur, holdninger og ledelse i politiet*. Direktoratet for forvaltning og ikt 2017:9. Tilgjengelig fra: https://kudos.dfo.no/files/fb2/fb2023713352985deaa351e310b9ea703fe103abfda0e541b7f5a205c6bd5354/Kultur_holdninger_ledelse.pdf
- Dillon, R. L. & Liebe, R. M. (2009). *Risk-Based Decision Making for Terrorism Applications*. Risk Analysis 29 (3) 321–335
- DNV GL. (2019). *Håndtering av innsiderisiko*. Petroleumstilsynet. Tilgjengelig fra: <https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/prosjektrapporter2019/hvordan-handtere-innsiderisiko/>
- Earley, P. C. (2006). *Leading Cultural Research in the Future: A Matter of Paradigms and Taste*. Journal of International Business Studies, 37, 922–31.
- Edmondson, A. (1999). *Psychological Safety and Learning Behavior in Work Teams*. Administrative Science Quarterly, 44(2), 350–383.
- Ekstedt, M. & Flores, W.R, (2014). *Shaping intention to resist social engineering through transformational leadership, information Security culture and awareness*. Tilgjengelig fra: https://www.sciencedirect.com/science/article/pii/S0167404816000067?casa_tok=en=kdLEVvRmooMAAAAA:SQOliUco_I0Vv7QC2TG_acphhkmaLTNFCC-qumEPVpwIwIYuDZKAUjZQf6a9TBgKImuamYzbQw
- Ellestad, J., Skuggestad, E., Gustad, A. & Lija, M (2019) *Sikkerhetskultur ved NTNU*.

- Engen, O.A., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E. & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet*. Oslo: Cappelen Damm.
- Equinor (ukjent dato). *Helse, sikkerhet og sikring*. Tilgjengelig fra: <https://www.equinor.com/no/baerekraft/helse-sikkerhet-og-sikring>
- Eriksen, T. H. og Sajjad, T. A. (2006). *Kulturforskjeller i praksis* (4. utg.). Gyldendal.
- Evalueringsutvalget etter Borgarting lagmannsretts dom av 19. juni 2020 (26.05.2021). *Politikorrupsjon Lederskap, risikoerkjennelse og læring*. Hentet fra: <https://www.politiet.no/globalassets/dokumenter/pod/rapporter/rapport-fra-evalueringsutvalget.pdfgsutvalget.pdf>
- Fiske, S. T. & Taylor, S. E. (1991). *Social Cognition*, 2nd edn. New York, NY: McGraw-Hill.
- Fuglseth, K. (2007). *Vitskapsteori og hermeneutikk*. I: Fuglseth, K og Skogen, K (red). Masteroppgaven i pedagogikk og spesialpedagogikk. Design og metoder. 2. utgave. Cappelen Akademisk Forlag, Oslo.
- Geertz, C. (1973). *The interpretation of cultures*. Basic Books, Inc., Publishers.
- Glendon, A. I., & Stanton, N. A. (2000). *Perspectives on Safety culture*. *Safety Science*, 34(1-3), 193–214.
- Glomseth, R. (2019). *Hva er organisasjonskultur, og hvorfor bry seg med den?* MAGMA 2/2019. Hentet fra: <https://old.magma.no/hva-er-organisasjonskultur-og-hvorfor-bry-seg-med-den?tid=213203>
- Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City, NJ: Doubleday.
- Goffman, E. (1974). *Frame Analysis: An Essay on the Organization of Experience*. Cambridge, MA: Harvard.
- Gundersen, D. (04.05.2018). *prosess*. Store norske leksikon. Tilgjengelig fra: <https://snl.no/prosess>
- Hatlebrekke, K. A. (2021). *The Problem of Secret Intelligence*. Edinburgh University Press
- Hatlebrekke, K. A. & Smith, M. L. R. (05.07.2010): *Towards a new Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure*. I *Intelligence and national Security*, vol. 25, 2010 – Issue 2, s. 147-182.
- Hofstede, G. (1980). *Culture's Consequences, International Differences in WorkRelated Values*. Beverly Hills, CA: Sage
- Holliday, A. (2019). *Understanding Intercultural Communication*. CRC Press Inc
- Hong, Y. Y. & Chiu, C. Y. (2001). *Toward a Paradigm Shift: From Cross-Cultural Differences in Social Cognition to Social-Cognitive Mediation of Cultural Differences*. *Social Cognition*, 19, 181–96
- International Organization for Standardization (2018). *Risikostyring – Retningslinjer (ISO Standard nr. 31000:2018)*
- International Organization for Standardization (2005). *Ledelsessystemer for kvalitet - Krav (ISO Standard nr. 9001:2015)*
- Jacobsen, Dag I. & Torsvik, J. (2019). *Hvordan organisasjoner fungerer* (5. utg.). Fagbokforlaget
- Justis- og beredskapsdepartementet (01.11.2022) *Hovedprinsipper i beredskapsarbeidet*. Tilgjengelig fra: <https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/hovedprinsipper-i-beredskapsarbeidet/id2339996/>
- Justis og Beredskapsdepartementet (16.10.2020). *Stortingsmelding 5, 2020-2021*

- Kaufman, A. & Kaufman, G. (2015). *Psykologi i organisasjon og ledelse* (5. utg.). Fagbokforlaget
- Kessler, G. C. & Shepard, S. D. (2022). *Maritime CyberSecurity. 2. edition*. ISBN: 9798412526034
- Kjøll, E. & Trandøy, K. E. (ukjent dato). *kognitiv*. Store norske leksikon. Hentet fra <https://snl.no/kognitiv>
- Kleven, T. A. & Hjordemaal, F. R. (2002). *Innføring i pedagogisk forskningsmetode - en hjelp til kritisk tolking og vurdering* (3. utg.) Fagbokforlaget
- KnowBe4 (2021). *The Security Culture Report 2021 – A Global Security Culture Perspective During a Pandemic*. Tilgjengelig fra: <https://blog.knowbe4.com/security-culture-report-2021-a-global-security-culture-perspective-during-a-pandemic>
- Kristoffersen, E. (2020). *Jegerånden*. Gyldendal Norsk Forlag AS
- Kroeber, A. L., & Kluckhohn, C. (1952). *Culture: a critical review of concepts and definitions. Papers. Peabody Museum of Archaeology & Ethnology, Harvard University, 47(1), viii, 223.*
- Kvale S & Brinkmann S. (2015). *Det kvalitative forskningsintervju*. 3. utg. Gyldendal, Oslo.
- Kystverket (2022). *ISPS-nytt 2-22*
- Lau, I. Y. M., Chiu, C. Y., & Lee, S. L. (2001). *Communication and Shared Reality: Implications for the Psychological Foundations of Culture*. *Social Cognition*, 19, 350–71.
- Legge, K. (1995). *Human Resource Management: Rhetorics and Realities*. Macmillian Business
- Leseth, A. B. & Tellmann, S. M. (2019). *Hvordan lese kvalitativ forskning?* Cappelen Damm Akademisk
- Lie, E. M. (2022). *Annerledespolitiet – Idealer og dilemmaer i politiets forbyggende dialogarbeid*. Det juridiske fakultet Universitetet i Oslo. Tilgjengelig fra: <https://www.duo.uio.no/bitstream/handle/10852/98476/PhD-Lie-2022.pdf?sequence=1&isAllowed=y>
- Liu, L. A. og Dale, C. (2009). *Using Mental Models to Study Cross-Cultural Interactions*. Tilgjengelig fra: https://www.researchgate.net/publication/304609034_Using_Mental_Models_to_Study_Cross-Cultural_Interactions
- Martin, P. (2019). *The Rules of Security. Staying Safe in a Risky World*. Oxford University Press.
- Moe, S. (29.12.2021) *Flere alvorlige dataangrep: – Tror det er den nye normalen*. E-24. Hentet fra: <https://e24.no/teknologi/i/KzegzM/flere-alvorlige-dataangrep-tror-det-er-den-nye-normalen>
- Myrset, O. (12.03.2021). *Dataangrep kostet Akva Group opptil 50 millioner kroner*. E-24. Hentet fra: <https://e24.no/naeringsliv/i/Vqj7Pr/dataangrep-kostet-akva-group-opptil-50-millioner-kroner>
- Nasjonal Sikkerhetsmyndighet (2014). *Økt risiko – styrket beredskap*.
- Nasjonal Sikkerhetsmyndighet (2015). *Risiko 2015*
- Nasjonal Sikkerhetsmyndighet (2019). *Risiko 2019*
- Nasjonal Sikkerhetsmyndighet (31.08.2020a) *Grunnprinsipper for sikkerhetsstyring*
- Nasjonal Sikkerhetsmyndighet (31.08.2020b). *Grunnprinsipper for fysisk sikkerhet*

- Nasjonal Sikkerhetsmyndighet (2020c). *Temarapport om innsidere*.
- Nasjonal Sikkerhetsmyndighet (2020d). *Risiko 2020*
- Nasjonal Sikkerhetsmyndighet (2021). *Risiko 2021*
- Nasjonal Sikkerhetsmyndighet (2023). *Risiko 2023*
- Nasjonal Sikkerhetsmyndighet (ukjent dato). *Risikovurdering av IKT-systemer*. Tilgjengelig fra: <https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf>
- Nasjonal Sikkerhetsmyndighet (ukjent dato). *Sikkerhetskultur*. Tilgjengelig fra: <https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/>
- Nasjonal Sikkerhetsmyndighet (ukjent dato). *Veileder i sikkerhetsstyring*. Tilgjengelig fra: <https://nsm.no/getfile.php/132933-1591350417/NSM/Filer/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf>
- Neisser, U. (1976). *Cognition and Reality: Principles and Implications of Cognitive Psychology*. San Francisco, CA: W. H. Freeman.
- Northouse, P.G. (2019). *Leadership – Theory and Practice* (8. utg.). Sage publishing
- Nosworthy J. (2000). *Implementing information Security in the 21st Century – do you have the balancing factors?* Computers and Security 2000;19(4):337–47.
- NOU 2000: 24. *Et sårbart samfunn – Utdfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Justis- og politidepartementet.
- NOU 2006: 6. *Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Justis- og politidepartementet.
- NOU 2012: 14. *Rapport fra 22. juli-kommisjonen*. Statsministerens kontor
- NOU 2016: 19. *Samhandling for sikkerhet – beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. Forsvarsdepartementet
- Næringslivets sikkerhetsråd (2019). *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2019*. Tilgjengelig fra: <https://www.nsr-org.no/aktuelt/innlegg-ma-handtere-risikoen-for-spioner-blant-egne-ansatte>
- Oxford Learner's Dictionaries (ukjent dato). *Safety*. Tilgjengelig fra: <https://www.oxfordlearnersdictionaries.com/definition/english/safety?q=safety>
- Oxford Learner's Dictionaries (ukjent dato). *Security*. Tilgjengelig fra: <https://www.oxfordlearnersdictionaries.com/definition/english/security?q=security>
- Perry, R. W. & Lindell, M. K. (2003). *Preparedness for Emergency Response: Guidelines for the Emergency Planning Process*. Disasters, 2003, 27(4). (336–350).
- Piètre-Cambacédès, L. & Chaudet, C. (2010). *The SEMA referential framework: Avoiding ambiguities in the terms "Security" and "Safety"*. International Journal of Critical Infrastructure Protection, Vol. 3:2. S. 55-66.
- Politiets Sikkerhetstjeneste (18.03.2022). *PST vurderer etterretningstrussel fra Russland i Norge som økt*. Tilgjengelig fra: <https://www.pst.no/alle-artikler/pressemeldinger/oppdatert-trusselvurdering-pst-ser-en-okt-etterretningstrussel-fra-russland-i-norge/>
- Politiets Sikkerhetstjeneste (2023). *Nasjonal Trusselvurdering 2023*
- Politiets Sikkerhetstjeneste (28.02.2020). *Målutvelgelse for politisk motiverte trusselaktører*. Tilgjengelig fra: <https://www.pst.no/globalassets/artikler/utgivelser/2020/malutvelgelse-hos-politisk-motiverte-trusselaktorer-1.pdf>
- Postholm, M. B. (2010). *Kvalitativ metode* (2. utg.). Universitetsforlaget

- Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate
- Reason, J. (2000). *Safety paradoxes and Safety culture*. *Injury Control & Safety Promotion*, 7(1): 3-14
- Reichers, A. E., & Schneider, B. (1990). *Climate and culture: An evolution of constructs*. B. Schneider (Ed.), *Organizational climate and culture* (pp. 5-39). San Francisco: Jossey-Bass.
- Reniers, R. L. E. P., Corcoran, R., Drake, R., Shyrane, N. M. og Völlm, B. A. (2011). *A Questionnaire of Cognitive and Affective Empathy*. *Journal of Personality Assessment*, 93: 1, 84-95.
- Richter, A., & Koch C. (2004). *Integration, differentiation and ambiguity in Safety cultures*. *Safety Science*, 42(8), 703-722.
- Roer, K. (2015). *Building a Security Culture*. IT Governance Publishing.
- Rumelhart, D. E. (1984). *Schemata and the cognitive system*. R. S. Wyer, Jr. & T. K. Srull (Eds.), *Handbook of social cognition*, Vol. 1, pp. 161-188). Lawrence Erlbaum Associates Publishers.
- Røhjell, D. (29.10.2022) *Sannsynlighetsord, kommunikasjon og etterretning*. Politforum. Tilgjengelig fra: <https://www.politforum.no/fagartikkel/sannsynlighetsord-kommunikasjon-og-etterretning/230105>
- Sandbakken, P. (09.05.2017). *Sikkerhetskultur: har vi det eller ikke?* Tilgjengelig fra: <https://www.cw.no/hva-andre-mener-sikkerhet/sikkerhetskultur-har-vi-det-eller-ikke/746596>
- Schein, E. H. (1983). *Organizational Culture: A Dynamic Model*. Alfred P Sloan School of Management Cambridge MA.
- Schein, E. H. (1987). *Organisasjonskultur og ledelse: Er kulturendring mulig?* Oslo: Mercuri Media Forlag.
- Schiefloe, P.M. (2021): *Organisasjonsanalyse*. Fagbokforlaget
- Selbekk, V. (16.06.2020). *KrF bør skrote hijab-forslaget*. Tilgjengelig fra: <https://www.dagen.no/okategoriserade/krf-bor-skrote-hijab-forslaget/>
- Shore, B. (1996) *Chapter 2: Rethinking culture as models*. I *Culture in mind*. Oxford University Press, USA, pages 42 – 71 (27 pages), (kopiert)
- Siverts, H. & Fagernes, S. (26.01.2021). *Kulturrelativisme*. Store norske leksikon. Hentet fra: <https://snl.no/kulturrelativisme>
- Skille, Ø. B. & Strand, T. (16.02.2009). *Vil ikke ha hijab i egne rekker*. NRK. Tilgjengelig fra: <https://www.nrk.no/norge/vil-ikke-ha-hijab-i-egne-rekker-1.6483603>
- Sлагnes, B. (06.03.2023): *Hva vet vi om innsiderisiko?* Forsvarets Forskningsinstitutt (FFI-rapport 23/00546)
- Smith, P. B. (2006). *When Elephants Fight, the Grass Gets Trampled: The GLOBE and Hofstede Projects*. *Journal of International Business Studies*, 37, 915-21.
- Standard Norge (2008). *Krav til risikovurderinger*. Norsk Standard (NS nr. 5814:2008)
- Standard Norge (2014). *Samfunnsikkerhet – Beskyttelse mot tilsiktede uønskede handlinger . Krav til sikringsrisikoanalyse*. Norsk Standard (NS nr. 5832:2014)
- Stensønes, M. (2017). *På vår vakt*. Aschehoug & Co
- Stolt-Nielsen, H. & Lysberg, M. (29.10.2021). *Dataangrepet kostet Hydro 800 millioner kroner. Nå er det kriminelle nettverket avdekket*. Aftenposten. Tilgjengelig fra: <https://www.aftenposten.no/norge/i/47WR3o/dataangrepet-kostet-hydro-800-millioner-kroner-naa-er-det-kriminelle-nettverket-avdekket>

- Svartdal, F. (16.06.2022). *Læring*. Store norske leksikon. Tilgjengelig fra: <https://snl.no/l%C3%A6ring#:~:text=L%C3%A6ring%20er%20definert%20som%20en,viktig%20forskningsomr%C3%A5de%20i%20moderne%20psykologi.>
- Telenor (2022). *Trusselbildet*. Tilgjengelig fra: <https://www.telenor.no/om/digital-sikkerhet/2022/trusselbildet/>
- Thaler, R. H. (2015). *Misbehaving: The making of behavioral economics*. W W Norton & Co.
- Thon, Roar (16.11.2022): *11 Tegn på god sikkerhetskultur*. Tilgjengelig fra: https://www.linkedin.com/posts/roar-thon-secdefence7429052_hva-kjennetegner-en-god-virksomhetskultur-activity-6999022563649556480-JMP2/?utm_source=share&utm_medium=member_ios
- Tjora, A. (2021). *Kvalitative forskningsmetoder i praksis*. Gyldendal Akademisk. 2021.
- Tjønndal, A. & Fylling, I. (2021). *Digitale forskningsmetoder* (1.utg.). Cappelen Damm Akademisk.
- Wegner, D. M. (1987). *Transactive Memory: A Contemporary Analysis of the Group Mind*. New York, Springer
- Weick, K. E. (1969) *Social Psychology of Organizing*. New York, NY: McGraw Hill.
- Weick, K. E. og Sutcliffe, K. M. (2007). *Managing the Unexpected Resilient Performance in an Age of Uncertainty*. Tilgjengelig fra: https://www.researchgate.net/profile/Kathleen-Sutcliffe/publication/265106124_Managing_the_Unexpected_Resilient_Performance_in_an_Age_of_Uncertainty/links/55e83a4308aeb6516262fe22/Managing-the-Unexpected-Resilient-Performance-in-an-Age-of-Uncertainty.pdf
- Weick, K. E., Sutcliffe, K. M. & Obstfeld, D. (2005): *Organizing and the Process of Sensemaking*. *Organization Science*, vol. 16, nr. 4 s. 409-421)
- Wormnæs, B. (2013). *Behandling som virker* (1. utg.). Cappelen Damm Akademisk
- Zahid, S. (15.06.2020). – *Hijabforbudet for politi og dommere truer ytringsfriheten*. *Advokatbladet*. Tilgjengelig fra: <https://www.advokatbladet.no/hijabforbudet-for-politi-og-dommere-truer-ytringsfriheten/152167>
- Žižek, S. (2006). *Philosophy, the "unknown knowns," and the public use of reason*. *Topoi*, 25(1), 137-142.
- Økokrim (2022). *Trusselvurdering*. Tilgjengelig fra: <https://www.okokrim.no/oekokrims-trusselvurdering-2022.6527255-549350.html>
- Aakre, S. (2020). *Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko?* Tilgjengelig fra: <https://old.magma.no/hvilket-trusselbilde-star-norske-virksomheter-overfor-og-hvordan-kan-apenhet-bidra-til-a-forsta-cyberrisiko>
- Aarset, M. (2017). *Håndtering av risiko*. ISBN 978-82-93459-02-6. Vitenskapelig monografi
- Aarvik, S. (10.10.2022). *Hijab i politiet. Akseptabelt?* *Aftenposten Si ;D*. Tilgjengelig fra: <https://www.aftenposten.no/meninger/sid/i/Q7yqKA/hijab-i-politiet-akseptabelt>
- Aase, T. H., Fossåskaret, E. & Fuglestad, O. L. (1997). *Metodisk feltarbeid*. Universitetsforlaget.

