Universitetet
i Stavanger

«Skyhøyt Spill – Resilient taktikk mot dronetrusler»

«Hvordan har operatørene operasjonalisert prinsippene fra resilience engineering i forbindelse med håndtering av dronetrusselen høsten 2022?»

Masteroppgave i risikostyring og sikkerhetsledelse

Tommy Bugge Hansen

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Vår 2023

FORFATTER: Tommy Bugge Hansen

VEILEDER: Kristin Sørung Scharffscher

TITTEL PÅ MASTEROPPGAVE: «Skyhøyt Spill - Resilient taktikk mot dronetrusler»

EMNEORD/STIKKORD: Sikring, resilience, hybride trusler, droner, økt trussel, krig, Ukraina-krigen, security, resilience engineering

SIDETALL: 104 (inkludert innholdsfortegnelse, referanser og vedlegg)

STAVANGER ……13.Oktober 2023 ……

DATO/ÅR

Framsidebilde: Bilde uten flammer er brukt med tillatelse av Nordic Unmanned. De to andre er egenprodusert med AI.

Forord

Hver gang jeg begir meg ut på en ny studie for å øke egen kunnskap blir jeg like oppgitt og samtidig ydmyk for hvor lite jeg egentlig kan. For snart 30 år siden tok jeg eksamen i Examen Philosophicum. Derfra har jeg båret med meg to sitater. Descartes sin læresetning «Cognito ergo sum» - jeg tenker, altså er jeg, har vært en fattig trøst når frustrasjonen har vært som verst. Sokrates sin erkjennelse av at «det eneste jeg vet er at jeg intet vet», er noe jeg til stadig har blitt påminnet om. Jeg lar meg imponere over de som skriver en slik studie uten veiledning. Uten gode innspill, kritiske spørsmål og observasjoner av min veileder Kristin hadde jeg trolig neppe kommet meg helskinnet gjennom denne studien.

Takk til Riana Steen som har bidratt med gode innspill og diskusjoner i innspurten av studien. Din entusiasme og konstruktive kommentarer dro meg ut av et mørkt hull.

Takk til min gode kollega Ivar Kvadsheim som har tatt seg tid til å lese og korrigere mine mange språklige feil. Takk til min nåværende og tidligere arbeidsgiver som har støtte dette prosjektet.

De fleste som har vært gjennom en slik studie med familie og jobb, vet at dette koster. Takk til ektefelle og barn som til stadig har godtatt en far og ektemann som «bare skal gjennomføre et lite studie til».

Sammendrag

Formålet med denne studien, utover å undersøke operatørenes håndtering av dronetrussel høsten 2022, er å lukke et kunnskapsgap innen studie av perspektivet «resilience engineering» (RE-perspektivet). Det er få studier som har undersøkt hvordan RE perspektivet har blitt operasjonalisert i håndtering av sikringshendelser. I denne studien ønsker jeg å undersøke:

> *Hvordan har operatørene operasjonalisert prinsippene fra «resilience engineering» i forbindelse med håndtering av dronetrusselen høsten 2022?*

Studien har tatt utgangspunkt i Erik Hollnagel sin definisjon av «resilience», og hans fire egenskaper som bidrar til å bygge «resilience». Det er lagt til grunn en kvalitativ metode, hvor det er gjennomført semistrukturerte intervju av seks personer som jobber i petroleumsnæringen, og som har vært aktivt involvert i håndtering av droneobservasjonene høsten 2022. Det er gjennomført en tematisk analyse av data. Det er også anvendt en deltakende observasjon ettersom jeg selv har vært deltakende i håndtering av droneobservasjonene.

Operasjonaliseringen av prinsippene fra «resilience engineering» (RE) i håndtering av dronetrusselen høsten 2022 har vært en kompleks prosess for operatørene. De sentrale funn i studien er:

Operatørene har lagt betydelig vekt på overvåking ved bruk av trussel- og sikringsrisikovurderinger. Selv om disse metroenene er verdifulle for overvåking, er de mindre velegnet for å forutse fremtidige scenarioer. Overvåkningens avhengighet av eksterne kilder fremhever et kritisk område for forbedring. Funn tyder på at operatørene har hatt en reaktiv respons, men til tross for dette har de vist en proaktiv tilnærming til iverksettelse av tiltak.

Operatørene har operasjonalisert evnen til å lære i håndtering av dronetrussel ved å dra nytte av lærdommer fra tidligere hendelser, legge vekt på trening og øvelse, samt forsterke tverrfaglig samarbeid og nettverksbygging. Funnene indikerer en blandet tilnærming til RE-prinsippene. Mens det er klare styrker i operatørenes evne til å reagere på og lære fra trusler, er det også rom for forbedring i deres evne til å forutse og overvåke slike trusler. En forståelse av disse styrkene og svakhetene kan bidra til å informere fremtidig håndtering ved å forbedre praksis i forbindelse med dronetrusler og andre komplekse utfordringer.

Denne studien understreker viktigheten av en kontinuerlig evaluering og tilpasning av praksis for å håndtere komplekse trusler i en verden i stadig endring.

Summary

The purpose of this study, beyond examining the petroleum operators' handling of the drone threat during autumn 2022, is to close a knowledge gap within the study of the resilience engineering (RE) perspective. Few studies have examined how the RE perspective has been operationalized in the handling of security incidents. What I want to research in this study is:

> *How have the operators operationalized the principles of resilience engineering in addressing the drone threat in the fall of 2022?*

The study is based on Erik Hollnagel's definition of resilience and his four characteristics that help build resilience. A qualitative method has been used, where semi-structured interviews have been conducted of six people who work in the petroleum industry and have been actively involved in handling the drone observations in the autumn of 2022. A thematic analysis of the data has been carried out. A participatory observation has also been used, as I myself have been involved in handling the drone observations.

The operationalization of resilience engineering (RE) principles in dealing with the drone threat in autumn 2022 has been a complex process for the operators. The key findings of the study are:

Operators have placed considerable emphasis on surveillance using threat- and security risk assessment. While these methods are valuable for monitoring, they are less suitable for predicting future scenarios. Monitoring's reliance on external sources highlights a critical area for improvement. Findings suggest a reactive response, but despite this, they have shown a proactive approach to implementing measures.

The operators have operationalized the ability to learn in dealing with drone threats by drawing on lessons learned from previous incidents, emphasizing training and exercise, as well as reinforcing interdisciplinary cooperation and networking. The findings indicate a mixed approach to the RE principles. While there are clear strengths in operators' ability to respond to and learn from threats, there is also room for improvement in their ability to anticipate and monitor such threats. An understanding of these strengths and weaknesses can help inform future management of incidents by improving practices related to drone threats and other complex challenges.

This study underscores the importance of a continuous evaluation and adaptation of practices to deal with complex threats in an ever-changing world.

Innholdsfortegnelse

1.1. Figurliste

1.2. Tabell

1.3. Forkortelser og begrep

Forkortelser

HRO	High Reliability Organizations
NHO	Næringslivets hovedorganisasjon
NSM	Nasjonal Sikkerhetsmyndighet
OED	Olje og Energidepartement
PST	Politiets Sikkerhetstjeneste
PTIL	Petroleumstilsynet
RE	Resilience Engineering

Begrep

Begrep	**Forklaring**
Resiliens	Den iboende evnen i et system til å justere sine funksjoner i forkant av, under, eller etter endringer og forstyrrelser, slik at det kan opprettholde nødvendige funksjoner under både forventede og uforventede forhold (Hollnagel, 2011a, s. 275).
Risiko	Usikkerhet knyttet til om en uønsket hendelse vil inntreffe og hvilke konsekvenser den vil få (Standard Norge, 2021).
Sabotasje	Å skade eiendom, produksjonsmidler eller tekniske systemer med hensikt (Engen, 2023).
Sikringskontekst	Forstås her som at en virksomhet har en verdi, en trussel som ønsker å påføre skade eller ta verdien, og at det er et ønske om å beskytte verdien (tiltak/barrierer) (Busmundrud et al., 2016, s. 51).
Sikringsnivå	Forstås her som en klassifisering basert på vurdert sikkerhetsrisiko eller trussel. Disse nivåene hjelper organisasjoner å iverksette passende sikkerhetstiltak. Nivåene kan variere fra "lavt" til "kritisk", avhengig av trusselens alvorlighetsgrad.
Sikringsrisiko-vurdering /analyse	Systematisk framgangsmøte for å beskrive risiko (Standard Norge, 2021).
Situasjonsforståelse	Situasjonsforståelse kan i denne studien forstås som hvordan vi rammer inn, fortolker og forstår verden rundt oss, og forutser hva som kan skje i eget miljø/scenario.
Trussel	Tilsiktet handling som kan føre til en uønsket hendelse (hendelse som kan medføre tap av verdier) (Standard Norge, 2021).
Verdi	Ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen (Standard Norge, 2012).

Introduksjon

1.1. Oppgavens bakgrunn

Da Russland innledet angrepet på Ukraina den 24. februar 2022, forandret det geopolitiske landskapet seg betydelig. Vestens sanksjoner har skapt et presset Russland, og som en konsekvens har landets innsats innen hybrid krigføring intensivert (PST, 2023).

115 droneobservasjoner ble høsten 2022 meldt inn til politiet (Stormark, 2023b). Dette, kombinert med tidligere hendelser, som arrestasjonen av ansatt i Det Norske Veritas (DNV) i 2020 for påstått samarbeid med russiske spioner og økningen i cyberangrep, sprenging av rørledning mellom Europa og Russland («Nord Stream»), peker på et eskalerende og mer komplekst trusselbilde (VG.no, 2020; Åklagarmyndigheten, 2022).

Jens Stoltenberg uttalte nylig at næringslivets sikkerhet er av nasjonal interesse, og at det ikke kan overlates til virksomhetene alene (Aftenposten, 2023). Samtidig har petroleumsindustriens rolle som Europas energileverandør blitt stadig mer kritisk, noe som også understrekes av norske myndigheter.

Denne masteroppgaven konsentrerer seg om petroleumsindustriens respons på trusselbildet fra høsten 2022, spesielt relatert til droneobservasjonene. Til tross for at industrien har håndtert sikkerhetstrusler tidligere, er omfanget og typen av utfordringer i 2022 noe nytt. I løpet av høsten 2022 så vi stor oppmerksomhet og interesse internasjonalt for hvordan Norge håndterte dronetrusselen og den generelle økte trusselen om sabotasje fra Russland. Tilstedeværelsen av militære fartøy rundt petroleumsinnretninger og besøk fra EU-kommisjonens president og NATOs generalsekretær på Troll A plattformen vitnet om interessen og myndighetenes involvering (VG.no, 2023).

Figur 1 Militær tilstedeværelse offshore (Forsvaret, 2022)

Operatørene har et ansvar for å forebygge, håndtere og virke etter hendelser. «Resilience engineering» gir et perspektiv på hvordan organisasjoner kan forberede seg på og håndtere uforutsette situasjoner (Thoma et al., 2016, s. 1). Likevel er det mangel på konkrete studier som

omhandler dette i organisasjonssammenheng, spesielt når det kommer til sikkerhetsutfordringer (Engen et al., 2016, s. 154). Denne studien vil søke å fylle dette kunnskapsgapet ved å utforske «resilience» innenfor rammen av dronetruslene i 2022.

1.2. Tidligere forskning

Selv om det er en fremvoksende interesse rundt «Resilience engineering» (RE) perspektivet og sikring/«security» , er det få studier som har anvendt RE-perspektivet på konkrete hendelser drevet av tilsiktede handlinger. Videre er mye av forskningen orientert mot makroperspektiver som sikkerhetspolitikk og samfunnssikkerhet.

Berling & Petersen (2020) utforsket operasjonaliseringen av «resilience» i de nordiske landene. De påpeker at den nordiske tilliten til staten og viljen til å dele informasjon legger til rette for en overordnet «resilience», men denne studien er begrenset til makroperspektivet (Berling & Petersen, 2020).

Sissel Jore har kastet lys over bruken av «resilience»-begrepet i terrorismeforskning (Jore, 2023), mens Marquez-Tejon et al. har gjennomgått litteraturen for å forstå forholdet mellom Enterprise Security Risk Management og organisatorisk «resilience», og avslører et fortsatt umodent forskningslandskap (Marquez-Tejon et al., 2022).

Steen har hatt søkelys på sammenhengen mellom «Safety-II»-konseptet og sikringsrisiko, og har utforsket hvordan sikringsrisikovurdering (SRA) kan komplettere REs kjerneegenskaper (Steen, 2019). På mastergradsnivå har Vivoll diskutert RE-perspektivet i forhold til sikringskultur, mens Skare har analysert RE-perspektivets relevans for å gjøre noe med hybridtrusler. Shukla og Solbakken har undersøkt hvordan «resilience» kan styrke cyber-beredskap i virksomheten (Hollnagel & Nemeth, 2016, s. 77–93; Woods, 2016) (Shukla & Solbakken, 2022; Skare, 2022; Vivoll, 2015).

Det ligger et kunnskapsgap i mangel på forskning som undersøker bruk av RE i reelle situasjoner. Teoretisk forståelse er utvilsomt verdifull, men den får ytterligere vekt og relevans når den suppleres med praktiske case-studier. Dette er spesielt tydelig når man ser på RE i konteksten av tilsiktede hendelser, et område hvor det synes å være en mangel på dybdeforskning. Mens tidligere studier har utforsket teoretiske aspekter av RE, mangler det empiriske undersøkelser som vier oppmerksomhet mot hvordan RE er operasjonalisert av organisasjoner som står overfor konkrete trusler.

Denne studien tar sikte på å gjøre noe med disse gapene. Forskningen vil undersøke hvordan RE kan operasjonaliseres i virkelige organisasjoner, spesielt med tanke på tilsiktede

hendelser. Gjennom denne tilnærmingen bidrar jeg med innsikt som på den ene siden kan styrke organisasjoners evne til å bygge og opprettholde «resilience» i møte med moderne og komplekse sikringsutfordringer, dette omtales også som sikringskontekst. På den andre siden bidrar studien med utvikling og bedre forståelse av teoriens anvendelse med utgangspunkt i en reel hendelse.

1.3. Oppgavens problemstilling og avgrensing

Formålet med denne studien er å undersøke hvordan operatører innen petroleumsindustrien har håndtert dronetrussel/observasjonene 2022 i lys av RE-perspektivet.

Problemstillingen for min studie er:

> *Hvordan har operatørene operasjonalisert prinsippene fra «resilience engineering» i forbindelse med håndtering av dronetrusselen høsten 2022.*

Med prinsipper i denne sammenheng legger jeg til grunn Erik Hollnagels fire potensielle evner til «resilience»: forutse, overvåke, respondere og lære. Disse blir utførlig beskrevet senere. Operatører henviser til virksomheter i petroleumsindustrien som «drifter» en innretning offshore. Med å operasjonalisere viser jeg til hvordan RE som teoretisk konsept er blitt omsatt til for eksempel praktiske tiltak, verktøy og prosedyrer.

For å besvare dette spørsmålet vil jeg først utforske de teoretiske fundamentene av RE for å identifisere de kjerneprinsippene som er mest relevante for dronetrussel-scenarioer. Med en klar forståelse av teorien vil jeg deretter dykke ned i de faktiske tiltakene og strategiene som ble gjennomført av operatørene. Gjennom intervju vil jeg kartlegge hvordan teori er omsatt i praksis. Videre vil jeg foreta en sammenligning mellom teoretiske forventninger og praktisk implementering for å identifisere eventuelt samsvar med teorien.

Dette trinnet vil ikke bare belyse hvor effektivt prinsippene ble anvendt, men også gi innsikt i hovedutfordringene og driverne operatørene har identifisert i møte med dronetruslene.

Denne tilnærmingen vil gi en forståelse av hvordan prinsippene fra RE ble operasjonalisert, samt deres effektivitet og mulige begrensninger i møte med en moderne teknologisk trussel.

Ved å kombinere teoretisk innsikt med praktiske observasjoner, søker denne studien å belyse ikke bare "hva" operatørene gjorde, men også "hvorfor" og "hvordan", og slik bidra til en rikere forståelse av «resilience» i praksis i møte med et hybrid trusselbilde som droneobservasjonene kan forstå som.

1.4. Avgrensning

Petroleumsnæringen er en omfattende industri med landbasert industri, som igjen består av leverandører, underleverandører, virksomheter som er operatører og har ansvar for drift av installasjoner. Videre virksomheter som kun er medeiere i lisenser der de ikke selv har ansvar for drift av installasjoner, samt myndighetene. Jeg har i denne oppgaven valgt å konsentrere meg om et utvalg av operatørene som har håndtert drone observasjonene for å begrense oppgavens scope og fokus. Det kunne f.eks. vært interessant å også vurdert håndteringen fra myndighetenes side, men dette ville utvidet omfanget av oppgaven betydelig.

I tillegg er det rekke ulike aktører i de operatørselskapene som kunne vært aktuelt å inkludere som beredskap, personell som håndtere flytrafikk (aviation), og operativt personell på innretningene. Disse ville gitt et annet perspektiv på håndteringen, men for å spisse oppgaven mot sikring har jeg valgt å begrense til personell som har sikring som fag.

I utgangspunktet ønsket jeg å undersøke hvordan operatørene hadde håndtert den økte trusselen fra Russland. Hybridkrigføring er et begrep som ofte brukes når man omtaler trussel fra Russland. Dette er alle typer angrep og forstyrrende operasjoner. Dette kan være cyberangrep, innsidetrussel, «jamming» av GPS signaler i Barentshavet og sabotasje. Trusselbildet er så omfattende og komplekst at jeg måtte begrense det til en konkret trussel. Dronetrusselen fikk omfattende oppmerksomhet, og hadde store konsekvenser. Jeg valgte derfor å ta å begrense studien til denne situasjonen og i perioden høsten (juni-desember) 2022. Det var i hovedsak denne perioden dronene ble observert.

1.5. Struktur

Kapittel	Oppsummering
1. Innledning	Her gis bakgrunn for studien og studiens problemstilling, samt avgrensninger som er gjort.
2. Kontekst	Her forklares konteksten som studiens problemstilling omhandler. Ukraina-krigen, trussel fra droner, samt sentrale aktører som påvirker operatørenes håndtering av dronetrusselen.
3. Teori	Her presenteres relevant teori, begrep som risiko, sikring og det teoretiske perspektiv «resilience engineering», samt Hollnagels fire egenskaper som bidrar til «resilience».
4. Metode	I dette kapittel beskrives hvordan studien har blitt gjennomført, de metodiske valg, gjennomføring av intervju og temaanalyse.
5. Empiri	I dette kapittel presenteres sentrale funn fra intervju. Dette er organisert etter Hollnagel sine fire egenskaper.
6. Diskusjon	Oppgavens problemstilling vil her bli diskutert. Empiriske funn vil bli diskutert mot teori.
7. Konklusjon	I konklusjon vil svar på studiens problemstilling presenteres.
8. Referanser, vedlegg	Her presenteres litteratur som ligger til grunn for studien, intervjuskjema og informasjon som er sendt til informantene.

2. Kontekst

2.1. Ukraina-krigen, hybride trusler, og dronetrussel

24. februar 2022 gjennomførte Russland et storskala angrep på Ukraina. Vesten svarte med å innføre strenge sanksjoner mot Russland (FN-Sambandet, 2023). Som en konsekvens har Norge blitt en viktigere energileverandør til Europa. Russland bruker en "hybrid krig"-strategi, som kombinerer tradisjonell krigføring med metoder som cyberangrep og påvirkningsoperasjoner. En utfordring med hybride trusler kan være at det er vanskelig for virksomhetene å se hvor og når den oppstår, og eventuelt når den slutter (Malerud et al., 2021; Reichborn-Kjennerud & Cullen, 2016). Et eksempel er dronetrusler mot oljeinstallasjoner i 2022 (NRK, 2022). Selv om dronene ikke forårsaket direkte skade, skapte de frykt og krevde ressurser å håndtere. Figur 2 viser ulike virkemidler i en hybrid krigføring og illustrerer kompleksiteten og utfordringen en virksomhet kan møte. Bruk av drone kan forstås både som bruk av irregulære virkemiddel og som del av en informasjonskampanje. Drone kan også brukes som et konvensjonelt virkemiddel for å angripe en installasjon.

Figur 2 Hybrid krigføring (Illustrasjon: (Savin, 2021)

I «resilience»-litteraturen refereres det ofte til enkelthendelser, som flyulykken med «US Airways flight 1549», som landet i Hudsonelven i 2009 (Hollnagel, 2011a, s. 50). Dronetruslene skiller seg fra dette ved at de varte over tid, bestod av en rekke hendelser [observasjoner] og skilte seg fra typiske sikkerhetshendelser ved at de var tilsiktet. I denne studien brukes begrepene «dronetrussel» om den generelle trusselen som de observerte dronene utgjør, og «droneobservasjon» om de spesifikke observasjonene høsten 2022.

Denne studien handler om dronetrusselen høsten 2022, hvor det antas at Russland står bak, herunder de ulike «hendelsene/observasjonene».

Selv om politiet betraktet dronetruslene som mindre alvorlige (Stormark, 2023a), har droner potensial til å bære farlige laster som for eksempel eksplosiver (*Peace Research Institute Oslo*, 2020). De kan også forstyrre helikoptertrafikk til offshoreinstallasjoner. En konsekvens av dronetrussel i kombinasjon med frykt for ytterligere sabotasje offshore var tilstedeværelse av militære fartøy (Gjerstad & Kibar, 2022).

Utfordringene knyttet til hybride trusler som har oppstått i forbindelse med krigen, sammen med usikkerheten om fremtidige hendelser og nødvendigheten av å håndtere oppståtte situasjoner, understreker nytten av å anvende et «resilience engineering»-perspektiv i håndteringen. Perspektivet kan bidra til å forstå hvordan operatørselskapene har håndtert en kompleks og utfordrende situasjon, og samtidig gi svar på hvilke egenskaper som kan underbygge systemets evne til å yte som forventet.

Når jeg i denne studien bruker begrepet respons, refererer jeg til responsen på ulike nivåer i organisasjonen. I offshore-terminologi omtales ofte organisasjonen på installasjonen som førstelinje, organisasjonen på land andrelinje, og ledelsen i virksomheten som tredjelinje. Respons omhandler også hvordan operatørene samarbeider med andre operatører og myndighetene, og de konkrete tiltak og aktiviteter operatørene iverksetter.

2.2. Petroleumsnæringen, sikringsnettverket og myndighetsorganer

Petroleumsnæringen består av operatørselskap/oljeselskaper som utvinner olje og gass på norsk sokkel. Det er operatørselskapene som er ansvarlige for å drifte installasjonene (oljeplattformene). I tillegg har man leverandørindustrien, undervannsentreprenører, forpleiningsbedrifter, forsyningsbaser og en rekke andre selskap som bidrar til denne industrien. I denne studien vil jeg ta utgangspunkt i et lite utvalg av operatørselskapene. I årsskiftet 2022/2023 var det ca. 93 felt som produserte olje og gass på norsk sokkel, og

næringen sysselsetter mer enn 200 000 personer. Norge dekker 20-25% av Europas gassbehov (Norsk Petroleum, 2023). Dette er med andre ord en omfattende industri.

Offshore Norge er en arbeidsgiver- og interesseorganisasjon for selskaper som driver på norsk sokkel. I Offshore Norge er det ulike komiteer, forum og nettverk (Offshore Norge, 2023). Et av utvalgene i Offshore Norge er sikringsnettverket, der alle operatørene er medlem og hvor også myndighetene inviteres inn. Dette er et etablert samarbeidsforum hvor operatørene samarbeider om sikring (Larsen & Østensjø, 2015; Stornes Stålesen, 2011; Vivoll, 2015).

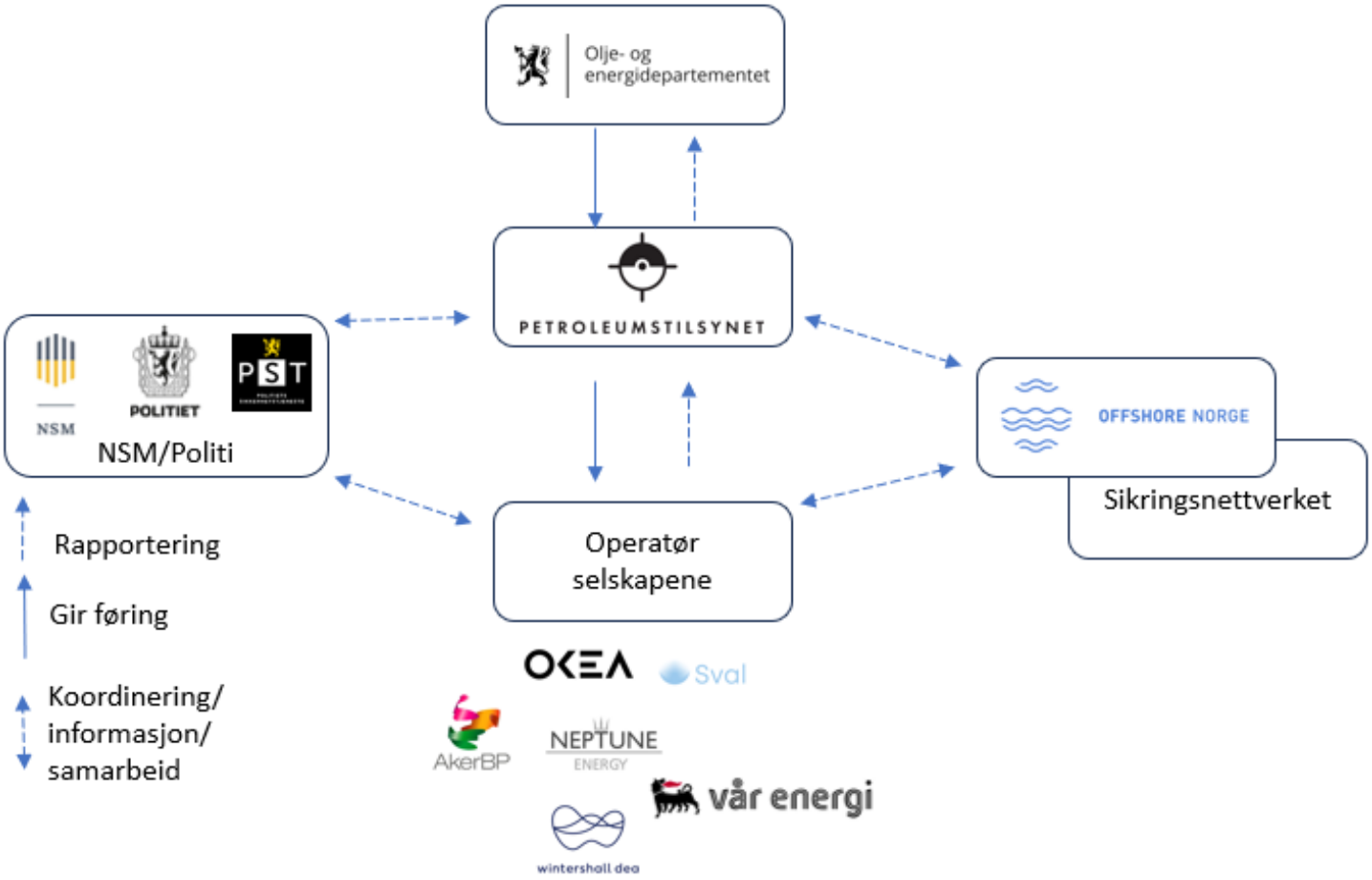
Petroleumstilsynet (Ptil) er et statlig tilsyns- og forvaltningsorgan med ansvar for tilsyn og regelverksutvikling for sikkerhet, arbeidsmiljø, beredskap og sikring i petroleumsnæringen. Ptil har delegert myndighet til å fastsette utdypende forskrifter for sikkerhet og arbeidsmiljø, og fatte enkeltvedtak i form av samtykker, pålegg med mer. Ved en beredskaps- eller sikringshendelse i petroleumsnæringen er det blant annet Ptils ansvar å føre tilsyn med operatørene, samt vurdere de tiltak som iverksettes for å få kontroll på situasjonen (Ptil, 2023e).

I 2013 fikk Ptil delegert myndighet til å føre tilsyn etter Petroleumsloven § 9.3, og har siden gjennomført en rekke tilsyn som har bidratt til å heve nivået på sikring i petroleumsindustrien (Botnan & Lausund, 2016, s. 29). Ptil er underlagt Olje og Energidepartement (ble overført fra Arbeids- og inkluderingsdepartement mai 2023) (Ptil, 2023d).

Ptil har i løpet av det siste året økt sin kommunikasjon om myndighetenes forventninger og krav til operatørene, herunder forventing om at sikringstiltak opprettholdes og styrkes for å møte den økte trusselen. Dette har fremkommet i møter med næringen, fagdag om sikring, Ptil´s nettsider med mer (Ptil, 2022a, 2022b, 2023i, 2023h, 2023b, 2023g).

I tillegg til Ptil har også Nasjonal Sikkerhetsmyndighet (NSM) og Politiet/Politiets Sikkerhetstjeneste (NSM) en sentral rolle. NSM er direktorat for nasjonal forebyggende sikkerhet og bidrar med råd, og håndtering ved cyberhendelser. NSM er underlagt Justis- og beredskapsdepartement (NSM, 2020). Politiet ivaretar den «daglige» kontakten med operatørene, og håndtering av hendelser offshore (etterforskning av droneobservasjonene). PST har ansvar for etterretning og kontraetterretning knyttet til nasjonale trusler som statlige aktører (spionasje), (overtok etter hvert etterforskning av dronehendelsene fra politidistriktene).

Figur 3 under viser en forenklet oversikt over aktørene og sammenhengen mellom dem. Ptil etablerer rammevilkår for næringen, og får oppdrag fra, og rapporterer til Olje og Energi Departementet (OED). Det er opprettet et samarbeid på alle nivå og mellom alle aktørene. Det er etablert formelle nettverk og uformell kontakt for direkte dialog mellom de ulike aktørene. Figuren er forenklet, i realiteten er det også dialog mellom departement, NSM, politi og Offshore Norge.



Figur 3 Sammenheng aktørene i petroleumsnæringen

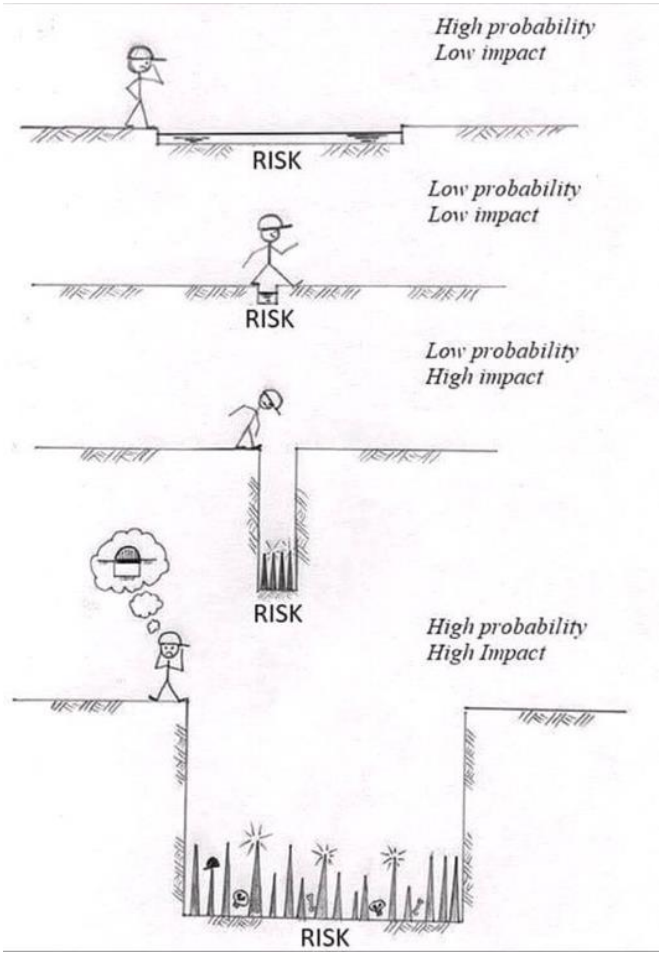
3. Teori

I denne studien skal jeg undersøke hvilke egenskaper ved operatørenes håndtering av dronetrussel høsten 2022 som har bidratt til «resilience». I tillegg til «resilience engineering» (RE) perspektivet, er begrepene risiko og sikring («security») to sentrale begrep. I dette kapittel vil jeg derfor gjennomgå disse begrepene og perspektivene. Avslutningsvis vil jeg gjennomgå kritikk av RE-perspektivet.

3.1. Risiko

Risiko er et velkjent begrep for mange av oss, vi bruker det i ulike sammenhenger, og vi blir utsatt for det daglig. I nyhetene brukes risiko om ulike temaer som helserisiko, finansiell risiko og klimarisiko. Russlands krig mot Ukraina har økt bevissthet om sikringsrisiko. Risiko for fysisk sabotasje på kritisk infrastruktur, risiko for cyberangrep og risiko for innsidere er noen av de sikringsrisikoene som nevnes av myndigheter og media (PST, 2023; Ptil, 2023a; VG.no, 2020).

Risiko kan defineres på ulike måter. Felles for de fleste definisjoner er at de sier noe om fremtiden. En definisjon av risiko som mange nasjonale og internasjonale virksomheter forholder seg til er fra standarden ISO 31000:2018 *«the effect of uncertainty on objectives»* (ISO, 2018). Sannsynlighet og konsekvens er ofte brukt i beskrivelse av risiko. Figur 4 illustrerer ulike risikobeskrivelser i sammenheng med sannsynlighet og konsekvens[1].



Figur 4 Risiko

[1] Bilde hentet fra: https://keenancdm.com/risk-probability-visualk-example-cdm-regulations/ Ukjent forfatter av bilde.

Ifølge Terje Aven vil risikoperspektivet som legges til grunn for risikostyringen påvirke hvordan risiko forstås og håndteres. Det er derfor viktig å forholde seg bevisst til dette (Aven, 2007). Risikostyring kan forklares å være alle tiltak og aktiviteter som utføres for å håndtere risiko. Formålet med risikostyring er å sikre riktig balanse mellom det å skape verdier på den ene siden, og på den andre siden å forhindre ulykker, tap og skader. En organisasjon er utsatt for ulike typer risiko, noen av disse stammer fra trusselaktører som har en intensjon og kapasitet til å utnytte en organisasjons sårbarhet for å få tilgang til organisasjonens eiendeler. Sikringsrisiko er dermed en av mange ulike risikoer en bedrift må håndtere (Marquez-Tejon et al., 2022, s. 601). Det skal jeg se nærmere på i neste kapittel.

3.2. Sikringsrisiko

«Security» eller sikring er på samme måte som risiko noe som for de fleste av oss alltid er til stede, og som vi er vant til å forholde oss til. Vi låser dører på hus og bil, og installerer alarmer for å hindre at trusselaktører stjeler det som er viktig for oss. Når det gjelder sikring som fag innen akademia er dette relativt umodent, og har fått liten oppmerksomhet fra det vitenskapelige miljøet. Når man har forsøkt å forklare hva sikring er, har man ofte sett dette begrepet opp mot sikkerhet («security» vs «safety») (Amundrud et al., 2017; Jore, 2019, 2020; Smith & Brooks, 2013). Figuren under viser skillet mellom sikring og sikkerhet, hvor skillet går mellom ondsinnet og tilsiktet og ikke ondsinnet og ikke tilsiktet. Det modellen ikke viser er at det også er en gråsone, hvor noe kan være tilsiktet, men ikke ondsinnet. Et eksempel på dette er en uteligger som legger seg til å sove i en trappeoppgang.

Figur 5 Sikring vs Sikkerhet (Jore, 2019)

Selv om sikring er et ungt fag innen akademia betyr det ikke at begrepet har vært uten definisjon og forskning, men de siste tiårene har vi sett en økning i akademisk interesse og forskning (Smith & Brooks, 2013). Begrepet sikring kan ha forskjellige betydninger avhengig av kontekst. Det kan referere til nasjonal sikkerhet, til en prosess eller en tilstand av å være fri

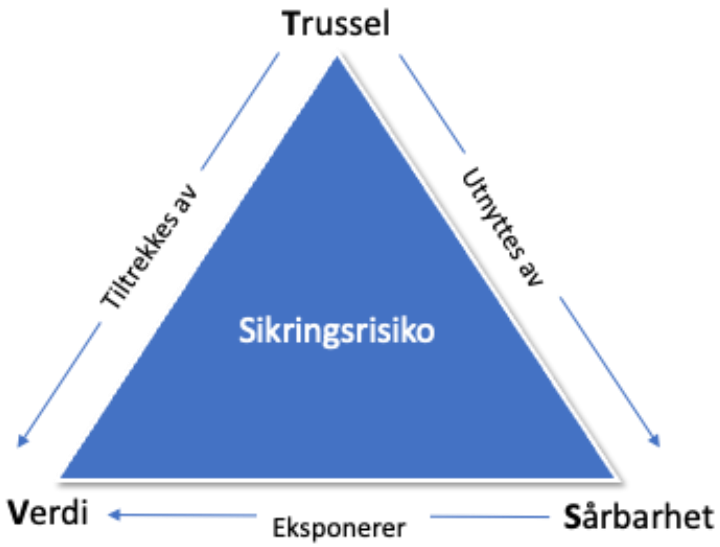
for trusler (Brooks, 2010). Likevel, med sikring i denne sammenhengen betyr det en trussel forårsaket av en ondsinnet aktør. I denne studien kan sikring defineres som:

> *[…]the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking (Jore, 2019).*

I denne definisjonen kobles sikring til «resilience». Det pekes i definisjonen på en evne eller egenskaper som kan bidra til å forberede for, motstå, tilpasse seg og gjenopprette etter en hendelse, dette er viktige komponenter som bidrar til «resilience».

Et sentralt element i styring av sikringsrisiko er identifisering og beskrivelse av risiko, dette er avgjørende for å ta risikoinformerte beslutninger, vurdere tiltak og vurdere hvordan hendelser skal håndteres. En sikringsrisikoanalyse vil ifølge Steen og Aven kunne bidra til å øke en virksomhets «resilience» for eksempel ved å identifisere scenario man ikke har tenkt på, og dermed øke evnen til å forutse (Steen & Aven, 2011).

Publisering av ny metodikk-standard for sikringsrisikoanalyse i 2014 og tilnærming til identifisering og beskrivelse av sikringsrisiko er noe av det som har skapt mest debatt innen sikringsfaget, og var på mange måter startskuddet for den akademiske interessen for sikring i Norge (Busmundrud et al., 2016). I denne standarden var sannsynlighet tatt ut og sikringsrisiko beskrevet som forholdet mellom en verdi, trussel og sårbarhet, ofte omtalt som risikotrekanten (figur 6). Denne beskrives som en nøkkel-komponent i å identifisere sikringsrisiko (Smith & Brooks, 2013, s. 69). Bruk eller ikke bruk av begrepet sannsynlighet var også et sentralt element i debatten om hvordan sikringsrisiko skulle beskrives (Busmundrud et al., 2016). I all hovedsak kan mye av debatten spores til manglende forståelse eller bevissthet om ulike perspektiv på sannsynlighet og risiko. Valg av perspektiv kan ha stor betydning for risikostyringen, og de



Figur 6 Risikotrekanten

ulike perspektiv ikke like egnet til å forstå for eksempel sikringsrisiko eller «resilience» (Aven, 2007, s. 37, 2017; Jore & Egeli, 2015; Steen & Aven, 2011).

Jore og Egeli peker på at det kan tas utgangspunkt i to perspektiver på risiko (selv om det finnes flere). Den klassisk positivistiske (tradisjonell) og det konstruktivistiske. I den klassiske tilnærmingen er risiko et produkt av sannsynlighet multiplisert med konsekvens (r=p*c), hvor sannsynlighet er basert på frekvens og historikk. Risiko kan forstås objektivt, det er med andre ord mulig å måle risiko uavhengig av følelser og mening. Det konstruktivistiske perspektivet konsentrerer seg mer om usikkerhet (r=c,u). Risiko kan her forstås subjektivt og kunnskapsstyrken som ligger til grunn for forståelsen av risikoen er sentral. Risiko blir for eksempel et utrykk for hvor usikker man er på hvorvidt en sikringshendelse skal oppstå. Det er en oppfatning i akademia at det konstruktivistiske perspektiv er bedre egnet til å beskrive sikringsrisiko (Jore & Egeli, 2015, s. 808–809). Dette underbygges også av Steen og Aven, som peker på at det som Jore og Egeli beskriver som det konstruktivistiske er det mest egnede perspektiv til å forstå og bygge «resilience» (Steen & Aven, 2011, s. 292). I 2021 ble det utgitt en revidert versjon av NS5814:21, som tar utgangspunkt i det konstruktivistiske perspektivet. Denne brukes både for «safety» og «security».

Denne gjennomgangen kan dermed tyde på at måten vi forstår sikring på har en kobling mot «resilience». Hvilket perspektiv på risiko man legger til grunn, kan være viktig for å forstå og bygge «resilience».

3.3. «Resilience»

I dette kapittel vil jeg presentere teori om «resilience» og «resilience engineering» (RE), som vil danne grunnlag for innhenting og analyse av data i senere kapittel. Jeg vil begynne med å forklare begrepene og hvorfor denne teorien er relevant for min problemstilling. Deretter vil jeg presentere RE som teori og hvordan RE-teorien kan operasjonaliseres. Til slutt vil jeg diskutere begrensninger og kritikk av RE som teori. Jeg har i studien valgt å bruke det engelske begrepet «resilience», i motsetning til å oversette til norsk – resiliens, robusthet, motstandsdyktig. Det er ikke funnet en god oversettelse av «resilience engineering» eller «resilience», og det er derfor ikke blitt oversatt. Det betyr at jeg også bruker det engelske ordet «resilient» i studien.

«Resilience engineering» er et perspektiv som kan være egnet til å undersøke studiens problemstilling. I kapittel 2.1 ble det redegjort for at den økte trusselen fra Ukraina-krigen kan forstås som en kompleks og dynamisk utfordring. Petroleumsnæringen som helhet og

virksomhetene for seg selv kan forstås som et system som skal yte og opprettholde sin funksjon før, under og etter denne situasjon. RE er et perspektiv som bidrar til å forstå hvordan organisasjoner kan håndtere komplekse og dynamiske systemer og utfordringer. Perspektivet setter søkelys på hvordan en organisasjon kan legge til rette for å kunne håndtere og operere under stor usikkerhet og kompleksitet, og kan derfor være et egnet perspektiv for å analysere og diskutere studiens problemstillingen *«hvordan har operatørene operasjonalisert prinsippene fra resilience engineering»* i forbindelse med håndtering av dronetrusselen høsten 2022» (Hollnagel et al., 2006, s. 6). Dette kapittelet vil gi leseren en forståelse av det rammeverket som blir benyttet, og det danner grunnlaget for analysen i kapittel 6.

3.4. «Resilience» og «resilience engineering»

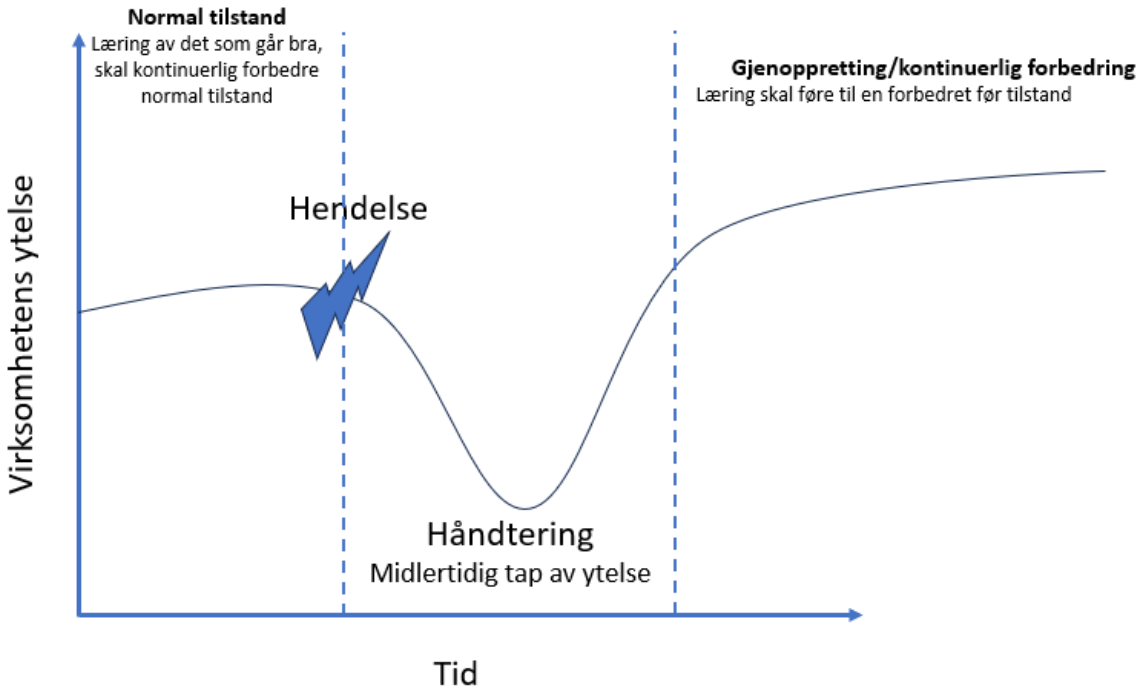
Resilience et relativt nytt perspektiv. Erik Hollnagel, som regnes som en av flere grunnleggere av perspektivet, trekker opprinnelsen tilbake til 2004 (Hollnagel, 2018, s. xiii). Begrepet «resilience» brukes innen forskjellige fagområder, og flere tolkninger har dukket opp. En litteraturgjennomgang i 2015 identifiserte mer enn 300 definisjoner av begrepet (*Darwin D1.1*, 2015). Både Aven og Stavland og Bruvoll peker på at det er mange definisjoner som brukes ulikt av de ulike akademikerne og praktikerne (Aven, 2017, s. 536; Stavland & Bruvoll, 2019, s. 33). Ifølge "Society of Risk Analysis" (SRA) (2015) er en definisjon av "resilience" *"The ability of the system to sustain or restore its basic functionality following a risk source or an event (even unknown)"* (SRA, 2015, s. 6). Klaus Thoma definerer «resilience» som:

> *[…] the ability to repel, prepare for, take into account, absorb, recover from and adapt ever more successfully to actual or potential adverse events. Those events are either catastrophes or processes of change with catastrophic outcome which can have human, technical or natural causes" (Thoma, 2014, s. 17)*

Innen "resilience engineering" har Erik Hollnagel, definert «resilience» som:

> *[...]the intrinsic ability of a system or organization to adjust its functioning prior to, during, or following changes, disturbances, and opportunities so that it can sustain required operations under both expected and unexpected conditions (Hollnagel, 2011a, s. xxxvi).*

Fellesnevneren for definisjonene er at et system har evne til å opprettholde sin funksjon, og komme styrket ut av en hendelse, til tross for at det blir satt under press. Se figur under for illustrasjon.



Figur 7 «Resilience» (basert på: Madni et al., 2020)

Definisjonen inneholder altså både et element av læring og tidsperspektiv (Stavland & Bruvoll, 2019). Figuren over viser både at man skal lære og forbedre ytelse gjennom normaltilstand, samt at læring etter hendelse skal bidra til at man kommer styrket ut av den. Ved en hendelse vil det bli et midlertidig tap av ytelse, og et mål er å redusere dette tapet fra hendelse til hendelse gjennom læring. Det er Hollnagel sitt perspektiv som legges til grunn i denne studien. Et perspektiv kan forstås som *"a particular attitude toward something; a way of thinking about something"* (Cooper, 2022, s. 2).

Noe av det som ligger til grunn for Hollnagels perspektiv er to begreper, «Safety I» og «Safety II». I «Safety-I», den tradisjonelle tilnærmingen til sikkerhet, handler mest om å forhindre feil og minimere risiko. Denne tilnærmingen forutsetter at menneskelige feil er hovedårsaken til ulykker og hendelser, og målet er å eliminere feil og avvik fra prosedyrer.

I motsetning til dette anerkjenner «Safety-II» («resilience engineering») at mennesker er en integrert del av komplekse systemer, og at deres handlinger og beslutninger kan bidra til sikkerhet på uventede måter.

«Safety-II» antar at mennesker ikke bare er kilden til problemer, men også løsningen, og at sikkerhet ikke bare er fravær av skade, men også tilstedeværelsen av positive resultater.

Målet med «Safety-II» er å utvikle og opprettholde motstandsdyktighet i systemet, slik at det kan fortsette å fungere effektivt selv i møte med uventede hendelser og forstyrrelser (Hollnagel et al., 2015).

David Woods argumenterer for at «resilience» er et verb, og viser til kapabiliteter som bygger og opprettholder potensialet for en kontinuerlig evne til å tilpasse seg («adaptability») (D. Woods, 2018, s. 5). «Resilience» er dermed ikke en statisk tilstand, men kapabiliteter i et dynamisk og tilpasningsdyktig system. Det som gjør et motstandsdyktig («resilient») system forskjellig fra andre systemer, er dets evne til å reagere dynamisk på endringene i miljøet det opererer i, og dets evne til å tilpasse seg uforutsette hendelser (Thoma et al., 2016, s. 7). Et eksempel på en uforutsett hendelse er utgangspunktet for denne studien, den pågående krigen Russland fører mot Ukraina, og de «hybride» truslene land som støtter Ukraina står overfor. Begrepet «resilience» kan forstås som noe som viser til egenskaper et system må ha eller må utvikle for å håndtere uventede og komplekse hendelser.

«Resilience engineering»-perspektivet søker å forstå hvordan de adaptive kapabilitetene et system innehar blir etablert, opprettholdt, degradert og mistet (D. Woods, 2018, s. 1). Dette underbygges også av Hollnagel som skriver at RE ser på ulike måter å forbedre evnen et system har for å lykkes under varierende situasjoner (Hollnagel, 2015, s. 1). Klaus Thoma trekker fram kritisk funksjonalitet og samtidig betydning av teknologi som skal kunne øke systemets ytelse.

> *Resilience Engineering means preserving critical functionality, ensuring graceful degradation and enabling fast recovery of complex systems with the help of engineered generic capabilities as well as customized technological solutions when the systems witness problems, unexpected disruptions or unexampled events (Thoma et al., 2016, s. 2).*

Selv om Thoma her peker på kritiske egenskaper, argumenterer Hollnagel for at RE konsentrerer seg om systemets ytelse, og ikke nødvendigvis en kvalitet eller egenskap systemet har (Hollnagel, 2015, s. 1). Ordet «engineering» antyder at «resilience» er noe som er mulig å bygge og tilpasse, og at det er basert på noen vitenskapelige prinsipper. I neste del skal jeg se nærmere på noen anerkjente egenskaper Hollnagel har etablert.

Jeg har så langt gjennomgått «resilience»-begrepet, og «resilience engineering»-perspektivet. Denne gjennomgangen har vist at RE er et relevant perspektiv som kan brukes for å analysere og diskutere problemstillingen. I neste del skal jeg se nærmere på hvordan RE kan brukes til å forstå og bygge de egenskaper som er og har vært nødvendig for operatørselskapene for å kunne håndtere den økte trussel som følge av Ukraina-krigen. Jeg skal videre konkretisere og operasjonalisere RE-perspektivet.

3.5. Potensial til «resilience»

Til tross for at det er et definisjonsmangfold, synes det i litteraturen ut til at det er en enighet om Hollnagel sine fire egenskaper for en «resilient» ytelse i en organisasjon, og at dette er en etablert tilnærming (Aven, 2022; Patriarca, Bergström, et al., 2018; Steen & Aven, 2011; D. D. Woods, 2015).

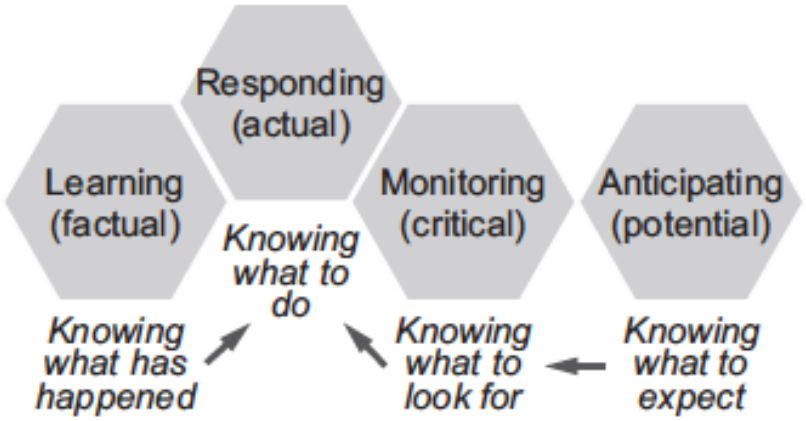
Hollnagel har pekt på fire sentrale egenskaper som et system bør inneha for at et system skal kunne inneha en evne til «resilient» ytelse.

i. **Respondere** er å vite hva man skal gjøre. Det omhandler hvordan man skal respondere på både forventede og uventede forstyrrelser eller hendelser, enten ved å iverksette etablerte og planlagte tiltak, eller å tilpasse responsen til hendelsen. Dette beskrives som å håndtere det *faktiske («actual»)*.

ii. **Overvåke** (*monitor*) er å vite hva man skal se etter. En virksomhet må overvåke både det som er, eller kan bli, en trussel. Evnen peker både på å overvåke det eksterne miljøet og ytre trusler, men også hvordan systemet yter og fungerer. Dette beskrives som å fokusere på og håndtere det *kritiske («critical»).*

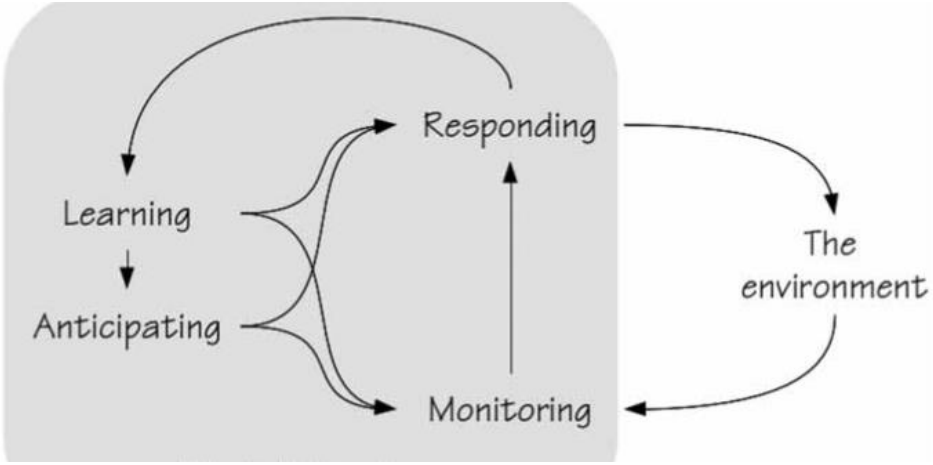
iii. Å **forutse**/**forvente** er en egenskap som peker på evnen til å kunne ha en formening om hva som skal skje, både hvilke trusler og muligheter som kan oppstå. Eksempler på dette er endring av situasjon, hendelser som kan forstyrre eller påvirke, samt konsekvenser av dette. Dette beskrives som evnen til å håndtere et *potensiale («potential»).*

iv. **Læring** er den siste av de fire essensielle egenskapene. Læring er å vite hva som har skjedd, å lære av de riktige erfaringene fra de rette hendelsene, både det som har gått galt og det som har fungert. Dette beskrives som evnen til å håndtere det *faktiske («factual»)* (Hollnagel, 2011a, s. xxxvii).



Figur 8 De fire egenskapene til et resilient system (Hollnagel, 2011a, s. xxxvii)

Figur 8 viser de fire egenskapene slik Hollnagel illustrerer dem, hvor evnen til å lære og overvåke påvirker evnen til å respondere. Å vite man skal forvente bidrar til å styrke evnen til å overvåke. Å vite hva man skal forvente vil også være avhengig av hva man lærer, det samme vil gjelde for evnen til å vite hva man skal se etter. Figur 9 viser dynamikken, og hvordan de ulike elementene påvirker hverandre, ikke i en lineær prosess, men i en iterativ og dynamisk prosess. Figuren viser også hvordan dette påvirkes av det ytre miljø f.eks. trusselbildet.



Figur 9 Avhengigheten mellom egenskapene (Hollnagel, 2014, s. 7)

Det Hollnagel påpeker som viktig er at organisasjonen må forstå hvordan disse egenskapene er avhengig av hverandre og hvordan de påvirker hverandre. Selv om Hollnagel argumenterer for at alle fire egenskapene må være til stede i et system for å kalle seg «resilient», må organisasjonen gjøre en vekting av de fire egenskapene. En slik vurdering kan være basert på kunnskap om virksomheten, aktiviteter og behov virksomheten har (Hollnagel, 2011a, s. xxxviii). Hollnagel antyder også at en virksomhet bør ha en bevissthet om dette. I praksis er

det ikke slik at en virksomhet nødvendigvis vil måle og bruke «resilience». Grad av bevissthet vil trolig kunne ha betydning for hvor målrettet organisasjonen er i å bygge resilience. Hollnagel peker også på at avhengig av kontekst og bransje, vil de ulike evnene (respondere, overvåke osv.) vektlegges ulikt (Hollnagel, 2018, s. 101). Dette kan påvirke min innsamling av data, hvor det i denne konteksten kan føre til at operatørene har vektlagt en av egenskapene mer enn en annen.

Når Hollnagel referer til de fire egenskapene i en «resilient» organisasjon så snakker han om dette som et potensial. «Resilience» er et uttrykk for en type ytelse i en organisasjon, og i beste fall kan man snakke om at en organisasjon kan ha et potensial for en «resilient» ytelse (Hollnagel, 2018, s. 26)

3.5.1. Respondere

Å reagere og respondere på en hendelse kan være avgjørende for en virksomhet eller en organisasjon. Et eksempel på manglende respons er håndteringen av terrorangrepet 22. juli 2011. I rapporten fra 22. juli-kommisjonen ble det blant annet pekt både på at angrepet kunne vært ha forhindret, og at politiets respons var for dårlig. Det ble også bemerket at flere sikrings- og beredskapstiltak burde ha vært iverksatt (Gjørv, 2012, s. 15).

En virksomhet eller individer i en virksomhet vil som oftest alltid respondere eller reagere på hendelser. Det som er avgjørende er å vite når man skal respondere, hvordan man skal respondere, og når man skal avslutte en hendelseshåndtering. Jean Pariès argumenterer:

> *At the'sharp end' of the system, 'responding to the situation' includes assessing the situation, knowing what to respond to, finding or deciding what to do, and when to do it (Hollnagel, 2011a, s. 3).*

For å oppnå dette finnes det to strategier. Den ene er en proaktiv tilnærming, hvor man er forberedt. Den andre en reaktiv tilnærming, hvor man reagerer på hendelser og tilpasser, lager eller finner løsninger. En proaktiv tilnærming vil være å foretrekke. Hollnagel beskriver at det må være noen indikatorer som trigger en reaksjon. Dette kan være både ytre og indre årsaker, som for eksempel at virksomheten endrer målsetning, eller et tilfelle hvor virksomheten angripes med vold (Hollnagel, 2018, s. 29).

Elementer i en virksomhet som kan bidra til å styrke evnen til respons kan være planer, prosedyrer, eller prosesser som tydeliggjør indikatorer for respons og når respons skal avsluttes. Planverk og prosesser kan også tydeliggjøre ansvar og roller. I henhold til

Petroleumsloven §9.2 og §9.3 er operatørene pålagt å ha beredskaps- og sikringsplaner (for utilsiktede og tilsiktede hendelser). I en sikringsplan vil det for eksempel være vanlig å ha ulike sikringsnivå som er tilpasset trusselbildet. Hollnagel argumenterer for at det er lite realistisk å ha forberedt planer ved sjeldne hendelser eller hendelser med lav frekvens. Dette er planer som må utarbeides når hendelsen oppstår, noe som kan føre til forsinket håndtering (Hollnagel, 2018, s. 30). En utfordring med dette er at sikringshendelser sjelden skjer eller aldri skjer, og legger man en slik tilnærming grunn vil det ikke være etablert mange tiltakskort. Dette må dermed forstå i lys av at teorien har sin bakgrunn i forskning om sikkerhet og ikke sikring. Samtidig kan det tyde på at Hollnagel legger til grunn det tradisjonelle risikoperspektivet som er basert på hvor ofte hendelser opptrer, og ikke perspektiv som i større grad legger til grunn kunnskap om fenomenet, og en vurdering av hendelser som kan skje, men som vi ikke har sett tidligere.

Evnen til å iverksette proaktive tiltak kan øke et systems evne til å respondere, og dermed bidra til «resilience». Hollnagel argumenterer følgende:

> *Proactive adjustment means that the system can change from a state of normal operation to a state of heightened readiness before something happens. In a state of readiness, resources are allocated to match the needs of the expected event and special functions may be activated (Hollnagel, 2015, s. 3).*

Ved å gjennomføre eller forberede tiltak før en hendelse oppstår, kan det sørge for at virksomheten øker sin «resilience». Et eksempel på dette er fra håndtering av COVID-19 hvor det ble etablert ulike tiltak som å begrense antall personer sammen og ha avstand for å hindre spredning av virus.

Det er også andre forhold som karakteriserer potensial til å respondere. Noen av disse er:

- Det må være etablert tydelige roller og ansvar, og det må være klart hvilken myndighet den enkelte har til å ta avgjørelser.
- Organisasjonen må være i istandsatt og forberedt til å reagere på og håndtere en hendelse. Dette kan innebære at man har ressurser, kompetent personell, utstyr, transport og så videre på plass, samt at man er trent.
- Ledelse og verktøy til å lede etter bør også være på plass. Dette beskriver også behov for planer og prosedyrer.

- Et siste element er å vite når man skal starte og stoppe en håndtering for å styre ressursbruken. Mobiliserer man for tidlig, kan man slite ut ressursene før hendelsen starter (Hollnagel, 2018, s. 30–31).

Denne gjennomgangen viser at det er flere elementer som kan være relevant å undersøke nærmere ved operatørselskapenes håndtering av den økte trussel som følge av Ukraina-krigen. Var operatørselskapene forberedt, hadde de identifisert denne type hendelser, var det etablert relevante planer, og var organisasjon trent på bruk av planverket?

3.5.2. Overvåke

"You can´t manage what you can´t measure" er et sitat som blir tillagt Peter Drucker, en kjent «ledelsesguru» (British Library, 2023). Lett omskrevet til denne sammenhengen kan vi si at vi heller ikke kan håndtere det vi ikke kan overvåke. Det er ikke mulig å etablere en «resilient» ytelse i en virksomhet uten at det overvåkes både for intern ytelse og eksterne påvirkninger, som for eksempel trusler. Hensikten med evnen til å overvåke er å holde et øye med hva som skjer både utenfor og innenfor virksomheten. For et operatørselskap kan dette være å overvåke trusselbildet ved å følge med på hva PST sier i sine trusselvurderinger og pressekonferanser. I tillegg er det viktig å overvåke hvordan virksomheten yter. Er for eksempel organisasjonen i tilstrekkelig beredskap, fungerer systemene slik de er tiltenkt? (Hollnagel, 2018, s. 31).

En virksomhet kan bruke ulike verktøy som sensorer og teknologi for å overvåke. Spørreundersøkelse kan være et eksempel på dette. Et kompetansesystem (oversikt over krav til kompetanse og gjennomførte kurs) kan være et annet eksempel. Det er tidligere nevnt at trusselbildet kan overvåkes. Dette kan gjøres «manuelt» ved at en person følger med i media eller leser PST sine rapporter. Dette peker også på at det kan være et element av menneskelig vurdering i å etablere eller opprettholde evnen til å overvåke (Hollnagel, 2018, s. 34).

Det å overvåke er grunnlaget for å kunne respondere, og for å kunne respondere på rett tid med rette ressurser, må organisasjonen være i stand til å vite man skal reagere på. Hollnagel argumenterer for at en effektiv respons forutsetter at virksomheten er i stand til å identifisere og kjenne igjen trender som ikke er store nok til å være en endring, men som kan få store konsekvenser (Hollnagel, 2018, s. 31–32) Et etablert «verktøy» i petroleumsnæringen er det som omtales som «risikonivået i norsk petroleumsvirksomhet – RNNP». Dette er en rekke indikatorer som er etablert på bakgrunn av en årlig undersøkelse som Petroleumstilsynet gjennomfører (Ptil, 2023f).

Bruk av indikatorer bidrar til å sikre en proaktiv overvåkning og respons, dette bidrar også til at det kan bli lettere å kjenne igjen eller identifisere trusler eller farlige situasjoner som kan oppstå. Samtidig kan det ifølge Hollnagel være at organisasjoner som endres sjelden, eller i liten grad påvirkes av ytre omgivelser, ikke har samme behov for overvåkning (Hollnagel, 2018, s. 33). En utfordring med en slik tilnærming er at virksomheten kommer i en passiv tilstand og dermed mister evnen til å være proaktiv. Hollnagel sitt argument kan derfor forstås som at virksomheten tilpasser grad av overvåkning til for eksempel situasjon. Risikoanalyse kan være relevant som grunnlag for en slik beslutning.

Hollnagel argumenterer for at indikatorer er tett knyttet opp mot overvåkning. Hensikten er å etablere et grunnlag for å vite noe om hvordan en organisasjon yter. Han peker på tre typer indikatorer:

- «Lagging indicators» - bakoverskuende indikatorer, dette kan være data som har vært samlet inn på et tidligere tidspunkt. RNNP-data er et eksempel på reaktive indikatorer, men også data som er aggregert opp over tid og dermed kan si noe om trender over tid. Disse bidrar til å skape forståelse for hendelser som har vært, og kan dermed også gi en indikasjon om årsak og virkning.
- «Current indicators» - indikatorer i nåtid. Denne type indikatorer gir en innsikt i pågående status, dette kan være varelager i en bedrift, ventetid på helpdesk, eller antall pågående dataangrep mot virksomheten. Indikatorene kan bidra til å justere ytelsen under pågående operasjoner eller aktiviteter.
- «Leading indicators» - framoverskuende indikatorer kan bidra til å si noe om en framtidig situasjon, hendelser eller for eksempel en organisatorisk tilstand. Dette er ikke indikatorer *per se,* men en tolkning av bakoverskuende og nåværende indikatorer. Indikatorene skal dermed kunne bidra til å forutse hva som kan skje. RNNP-data er igjen et eksempel på dette. Trendene fra RNNP kan brukes til å lage antagelser om fremtiden. I denne type indikatorer er det en iboende usikkerhet, og her vil for eksempel kunnskapen en har om fenomenet man skal si noe om være viktig. Et eksempel er trusselvurdering. Dette er basert på en vurdering av flere indikatorer, blant annet intensjon og kapasitet til en aktør. I tillegg kan man se på tidligere hendelser og historikk. En vurdering av hva som kan skje, basert på tidligere og nåværende intensjon og kapabilitet kan være vanskelig. Dette kan endres raskt, og virksomheten har ikke tilgang til samme kilder som sikkerhetsmyndighetene. Organisasjonen må derfor legge

noen antagelser til grunn (Hollnagel, 2018, s. 35–36). Dette kan øke usikkerheten i de framoverskuende indikatorene.

Evnen eller potensialet til å overvåke henger også sammen med evnen til å lære. Mange av de indikatorene som blir etablert, og hvilket sikrings- eller sikkerhetsnivå en virksomhet skal legge seg på, er basert læring fra tidligere hendelser. Dette er beskrevet nærmere i kap. 3.5.3.

3.5.3. Lære

Utgangspunktet for denne studien er den økte trussel som følge av Russlands krig mot Ukraina og droneobservasjoner ved norske offshoreinstallasjoner høsten 2022. Det har tidligere vært lite oppmerksomhet om sikringshendelser, til tross for at det har vært hendelser før dronetrusselen. Eksempler på dette er cyberangrepet mot petroleumsnæringen i 2014, kartlegging av «subsea» infrastruktur i 2020-2021 og den undersjøiske kabelen (overvåkningssystem) som ble kappet utenfor Vesterålen i 2020 (Dagens næringsliv, 2021; NTB, 2014, 2022). Det er ikke åpenbart at hendelsene er knyttet til den økte trusselen fra Russland som operatørselskapene står ovenfor i dag, og det er heller ingen åpenbar sammenheng mellom droneobservasjonene og Russland. Dette viser kompleksiteten i situasjonen, og det er nettopp dette som kan gjøre læring vanskelig. For å lære må man forstå hva man skal lære av og hvordan man skal kontekstualisere denne læringen, det vil si. være i stand til å forstå i hvilken sammenheng det som læres er relevant og kan brukes (Hollnagel, 2011b).

Læring er avgjørende for å etablere en evne til «resilient» ytelse i en virksomhet. En organisasjon som ikke evner å lære vil ifølge Hollnagel begrense sitt handlingsrom, og vil i stor grad overvåke de samme verdier og forhold. Læring kan forstås som hvordan en organisasjon tilpasser og tilegner seg ny kunnskap, kompetanse og ferdigheter. Evnen til å lære spiller også en viktig rolle, om ikke en forutsetning, for å kunne etablere evnen til å overvåke og reagere. Det er blant annet gjennom læring organisasjonen får innspill til hva man skal se etter og hvordan man kan forbedre sin respons. Samtidig er det vanskelig å få til læring uten at man har hendelser eller erfaring å lære fra (Hollnagel, 2018, s. 36).

Tradisjonelt har organisasjoner ofte hatt søkelys på å lære fra alvorlige hendelser. I petroleumsnæringen er det søkelys på å gjennomføre granskninger etter en alvorlig hendelse. Hollnagel trekker frem at det er viktig å skille mellom det som er enkelt å lære, og det som er viktig å lære. Hollnagel peker også på en utfordring, som er at store hendelser skjer sjelden, og det er dermed få hendelser å lære fra (Hollnagel, 2018, s. 37). For sikringshendelser er det enda

færre å lære av. Dette betyr at læring ikke bare må begrenses til det som går galt, men også det som går bra. I tillegg må virksomheten også se på andre lignende hendelser, herunder det som går bra, som kan være representative med hensyn til frekvens. I tillegg er det viktig at virksomheten har på plass systemer som sikrer en kontinuerlig læringssløyfe, og ikke bare etter hendelser (for eksempel granskning) (Hollnagel, 2018, s. 37). Dette kan dermed bety at ved å generalisere læring, fra både det som går bra og det som går dårlig, er det ikke så viktig om det skyldes en sikrings- eller sikkerhetshendelse. Et eksempel på dette er at operatørselskapene over tid har opparbeidet seg betydelig beredskapserfaring fra ulykker eller hendelser offshore. En læring kan være at stabsmetodikken som brukes i beredskapsorganisasjonen også er overførbar til sikringshendelser. Stabsmetodikk er en systematisk tilnærming som en stab eller ledelse bruker til å analysere, planlegge og håndtere en situasjon. De fleste operatørene bruker det som heter proaktiv stabsmetodikk, en metodikk som har oppmerksomheten rettet mot å dimensjonere håndteringen for potensialet i hendelsen (Lunde, 2014).

Læring krever at ulike elementer er på plass. Dette kan være en kompetent organisasjon og ledelse. Det kan også være teknologi, systemer og ressurser (penger og tid). Virksomheten må være mer bevisst på, og ha en systematisk tilnærming til læring. Læring skal føre til en endring eller korrigering av kurs (eller bekrefte at det man gjør er bra). Læring skal uansett vises igjen i det en organisasjon gjør. Hvis læring skal føre til endring, vil det kunne ta tid (Hollnagel, 2018, s. 40).

Hollnagel peker på at det er tre forhold som må ligge til grunn for at læring skal kunne finne sted.

- Det må være en mulighet for å lære. Dette betyr at det faktiske utfallet av en aktivitet er så annerledes enn det som var forventet at det er behov for å forstå hvorfor. Samtidig må virksomheten også være i stand til å forstå hvorfor det som skjer på daglig basis, og fører til et positivt resultat, går så bra.
- Det må også være en rimelig grad av likhet mellom situasjonene hvor man ser behov for å lære. Utfordringen er å dra ut fellesnevnere fra hendelsene. Ved å kun lære fra unike hendelser, vil overføringsverdien være minimal.
- Den siste forutsetningen er at det må være en mulighet for å kunne verifisere at noe har blitt lært. Dette kan være en endring i adferd, eller at kunnskap og kompetanse har økt. I praksis betyr dette at før organisasjonen har erfart en ny situasjon hvor det er mulighet for å bruke det man har lært, så har det vært begrenset mulighet for å lære (Hollnagel, 2018, s. 41).

Det er ikke vanskelig å forstå at læring har en sentral plass i operatørselskapenes styringssystem. I Styringsforskriften §23 er det et krav om at operatørselskapene kontinuerlig skal forbedre sitt sikkerhets- og sikringsarbeid, herunder læring fra både egen og andres virksomhet (Ptil, 2023c). Dette peker samtidig på at myndighetenes regelverk er en viktig driver for læring. En egenskap som det derimot kan være noe mer utfordrende å se behov for, og som kan oppfattes noe mer diffust, er potensialet til å forutse hva virksomheten kan forvente av hendelser i framtiden. Det er den siste av de fire egenskapene som bygger opp om potensialet til en «resilient» ytelse i en virksomhet.

3.5.4. Forutse

Å forvente eller forutse dreier seg samtidig i større grad om å tenke seg til noe. Dette kan kobles til det som Terje Aven beskriver som å se etter de ukjente ukjente, eller ukjente kjente. Hendelser og scenarioer vi ikke har sett for oss, eller hendelser og scenarioer som andre har sett for seg, men ikke vi (Aven, 2013, s. 45).

Hensikten med denne egenskapen er å se utover de hendelser som vi har lagt planer for. Dette kan være hypotetiske og potensielle hendelser. Hva vi tidligere har erfart og lært kan være et element som kan være en positiv eller negativ bidragsyter.

Evnen til å forutse skal ikke støtte opp om pågående aktiviteter, men skal se utover dette og for eksempel identifisere helt nye måter å gjøre aktiviteter på. Dette skal bidra til å redusere usikkerheten. To vanlige måter å redusere usikkerhet på er enten planlegging eller risikostyring, men ifølge Hollnagel så har begge disse aktivitetene iboende begrensninger som gjør at de i seg selv ikke ser utover disse. F.eks. begrenses risikovurderingen av at den må ta utgangspunkt i rammene rundt virksomhetens aktiviteter (Hollnagel, 2018, s. 44).

Hollnagel beskriver tre modeller som beskriver hvordan vi tenker om framtiden, og hvordan dette henger sammen med fortiden og det vi ser i nåtiden.

- Gjenkjenning er den enkleste form for å være forutseende. Hvis en situasjon har store likheter med noe vi har erfart tidligere, så antar vi at det vil kunne utvikle seg likt i framtiden.
- Ekstrapolasjon en annen modell som også bygger på erfaring fra fortiden, og det vi kjenner, men hvor virksomheten (eller individ) ser utover det man kan se. Hollnagel beskriver det som en «sannsynlighet» hvor framtiden er beskrevet som en kombinasjon av tidligere erfaringer og forhold.

- Den sisten modellen for å forutse er en bevisst konstruksjon av mulige framtidige situasjoner, som er basert på en forståelse av tidligere hendelser og hvordan disse har oppstått og utviklet seg. Ved å endre på ulike variabler lager man noen antagelser om hvordan kjente hendelser kan endre seg og oppstå i framtiden (Hollnagel, 2018, s. 44).

I en «resilient» virksomhet skal det være en uro og usikkerhet om den nåværende situasjonen og hva framtiden bringer. Det motsatte, en virksomhet som er tilfreds med den nåværende situasjonen og ikke vil innse at ytre forhold kan påvirke virksomhetens strategiske mål, vil ikke være «resilient». Denne uroen beskrives som en forutsetning i en «resilient» virksomhet. I tillegg vil det være viktig med tilstrekkelig ressurser, dette kan være at virksomheten har en «tenketank», eller noen som jobber aktivt med å tenke ut av boksen. Dette kan være ressurskrevende både med hensyn til tid og penger (Hollnagel, 2018, s. 46–47).

Et sentralt konsept for Hollnagel er ytelsesvariasjon. Hollnagel snakker om at uønskede hendelser i komplekse systemer kan oppstå når forskjellige deler av systemet presterer litt annerledes fra gang til gang, selv om de fungerer normalt. Disse små variasjonene kan kombineres på uventede måter og føre til problemer som ikke lett kan tilskrives en enkelt feilkilde. Hollnagel understreker at vi må forstå hvordan disse små variasjonene kan samhandle og forårsake uønskede hendelser, selv når alle delene fungerer som de skal (Hollnagel, 2017).

Dette kan overføres til håndtering av dronetrussel. På den ene siden kan det forekomme variasjoner i systemene som skal oppdage droner, inkludert radarer, bruk av overvåkningskameraer og manuelle observasjoner. Disse elementene kan for eksempel påvirkes av værforhold, vind og lysnivå. Operasjonelle variasjoner, som utskiftning av personell og variasjoner i aktivitetsnivå, kan også spille inn. Innenfor petroleumsnæringen omtales dette som ytelsespåvirkende faktorer – faktorer som kan påvirke effektiviteten til en barriere (Steen & Aven, 2011, s. 292). Dette er variasjoner som kan utnyttes av en trusselaktør. Ytelsesvariasjon kan være relevant med hensyn til å forutse fordi det viser kompleksiteten og variasjonene som kan påvirke hva som kan skje. Ytelsesvariasjon kan dermed være viktig å identifisere, dette kan også være relevant med tanke på hva som skal overvåkes.

3.5.5. Evne til å planlegge, tilpasse og kommunisere

Hollnagel foreslår at ytterligere tre elementer er relevante for å oppnå «resilience», evnene til å planlegge, kommunisere og tilpasse seg. Han beskriver dem imidlertid som elementer som muliggjør evnene til å respondere, overvåke, lære og forutse, snarere enn elementer som direkte

bidrar til «resilience». Planlegging er en nødvendig aktivitet for at enhver organisasjon skal fungere, og gjelder for enhver form for ytelse. Kommunikasjon handler om å overføre informasjon fra en del av systemet til en annen del. Hollnagel ser også dette som en nødvendig og nedarvende aktivitet i en organisasjon og kan betraktes som en tilrettelegger for evnene til å respondere, overvåke og lære. Planlegging og kommunikasjon anses likevel ikke som aktiviteter som direkte bidrar til en evne til «resilient» ytelse. Tilpasning forklares til en viss grad som sammensatt, og et resultat av kombinasjonen av funksjonene læring, respons og overvåking. Tilpasning er evnen til å justere eller modifisere seg selv, basert på erfaring (Hollnagel, 2018, s. 49–50). Selv om disse tre elementene ikke er en del av de "offisielle" fire funksjonene eller evnene i et «resilient» system, har jeg valgt å inkludere dem i min studie. Planlegging og kommunikasjon kan forstås som viktige tilretteleggere for de fire evnene og knytter dem sammen. I tillegg er de viktige elementer i risikostyring.

3.6. Kritikk av RE-perspektivet

Hollnagel sine egenskaper som er beskrevet i de foregående kapitler er essensielle komponenter for en virksomhet som skal ha en «resilient» ytelse. Denne argumentasjonen er basert på forskning fra sikkerhetsfaget, og om hvordan hendelser oppstår og kan forhindres. I følge Stavland og Bruvold representerer «resilience engineering» en måte å tenke omkring sikkerhet og sikkerhetsstyring, hvor man heller enn å styre risiko utfra kunnskap om fortiden, setter søkelys på å forbedre evnen til å være tilpasningsdyktig (Stavland & Bruvoll, 2019, s. 20).

De fire egenskapene til Hollnagel er basert på antagelsen om at folk kan oppnå «resilient» ytelse ved bygge egenskapene respondere, forutse, overvåke, og lære av uventede hendelser og forstyrrelser. Det er flere forskere som har kritisert ulike elementer ved ««Safety-II»» og RE perspektivet. En av disse er Dominic Cooper, som argumenterer for at «Safety II» er en del av flere perspektiv som beskriver RE, og omtaler disse som «new-view». Han argumenterer for at disse perspektivene representerer en samling av ikke testede og verifiserte påstander, ideer, regler og prinsipper. Han sier videre at RE sin underliggende filosofi er å kontinuerlig teste grensene til et system inntil feil oppstår, noe som fører til at nye kontrolltiltak må etableres. Dette skaper dermed et paradoks ved at konsekvensen av at RE sin underliggende tilnærming bidrar til nettopp det som perspektivet skal håndtere, nemlig begrensninger, kompleksitet og rigide systemer (Cooper, 2022, s. 2).

Cooper peker videre på at «new-view»-perspektivene mangler nye metoder for å forbedre sikkerheten, og at det heller ikke er forskning som bygger opp om de påstandene eller forutsetningene som fremmes.

> *It is very clear that none of the new-view proponents articulate a clearly defined set of practical processes, methods, tools, activities or combinations thereof, by which to improve safety per se. All appear to be solely concerned with sharing ideas and propositions based on their author's mental representations of the industrial and academic safety world. The big question, therefore, is whether or not any of new-view's ideas have merit for improving 'safety' or reducing incidents and injuries (Cooper, 2022, s. 2).*

I sin argumentasjon peker Cooper her på at akademikere som Hollnagel i stor grad er opptatt av å dele tanker og påstander, som er basert på deres teoretiske framstilling om hvordan noe henger sammen. Dette gjøres til fordel for forskning som faktisk viser en effekt av de påstander som fremlegges om hva som bidrar til sikkerhet. Hollnagel argumenterer derimot for at «Safety II» ikke er del av «new-view», han skriver at*:*

> *This is by no means the so-called 'new view' – which by the way was not new at all even when it was touted as such – but rather the realisation that humans always try to do what they think is right in the situation (Hollnagel, 2016).*

Han argumenterer her for at RE i seg selv er et tillegg til sikkerhet. Det kan allikevel tyde på at det er en oppfatning blant kritikerne om at «Safety II» er del av «new-view» som et samlebegrep for de ulike tilnærminger til RE (Cooper, 2022).

En annen kritiker er Nancy Leveson. Hun har skrevet artikler og bøker sammen med Hollnagel, og har samtidig rettet sterk kritikk mot Hollnagel sin teori og «Safety-II» (RE). Hun har blant annet rettet kritikk mot premissene for «Safety-I» og «Safety-II». Leveson peker på at Hollnagel gjennomgående karakteriserer «Safety-I» som reaktivt.

Dette er også noe som støttes av Andrew Hale, som blant annet viser til Barry Turner sin forskning om at hendelser kan ha en lang inkubasjonstid, og alle virksomheter vil i en slik periode kunne ha erfart et scenario som kan ha ført til en hendelse. Utfordringen er å vite om dette har ført til positive eller negative hendelser (Hale, 2014, s. 64). Dette peker også mot utfordringen med å frakoble seg det som har vært, og se framover. Hollnagel sin tilnærming kan dermed kritiseres for å basere seg i for stor grad på å analysere tidligere erfaringer.

Leveson skriver i sin kritikk om «Safety-II» at det finnes andre alternativer til «Safety-II» som kan bidra til å oppnå «resilience» (Leveson, 2020, s. 3–4). Hun peker videre på at dette er egenskaper som må bygges inn et system, og er ikke er resultat av menneskelig interaksjon. Samtidig peker mye av sikkerhetsforskningen på at nettopp mennesket er viktig i å oppnå sikkerhet (Grøtan et al., 2008; Hollnagel, 2014; Steen et al., 2022; van der Merwe et al., 2018)

Et av hennes hovedargumenter er at det er behov for en mer omfattende, systemorientert tilnærming til sikkerhet og motstandskraft, en som inkorporerer et bredt spekter av faktorer og tar en proaktiv tilnærming til fareforebygging og -reduksjon» (Leveson, 2020, s. 3–4). Et av poengene til Leveson er hvordan Hollnagel, og hun selv beskriver et system. Hollnagel beskriver det som alle delene i et system som henger sammen, men Leveson beskriver det som en samling komponenter som fungerer sammen for å oppnå et felles mål. En vesentlig forskjell ligger nettopp i nyansen om hva systemet skal oppnå, hvor Leveson peker mot et felles mål (Leveson, 2020, s. 40).

«Safety-II» har et entydig fokus på operatørgrensesnittet (menneskelige operatør), og har mindre oppmerksomhet på systemet som mennesket skal operere i. Leveson hevder at «Safety-II» er det motsatte av et sosioteknisk system, et system hvor det er tette koblinger og sammenhenger mellom både teknologi og menneske. I et slikt system er hovedinteressen å undersøke hvordan elementene påvirker hverandre og er integrert og koblet sammen. Kritikken er rettet mot at Hollnagel kun konsentrerer seg om mennesket og ikke det teknologiske aspektet. I følge Leveson er det ikke realistisk å legge til grunn at mennesker, eller virksomheter skal oppnå en evne til en «resilient» ytelse uten å også vurdere hvordan systemet de operer påvirker dem (Leveson, 2020, s. 104).

Et annet forhold Andrew Hale trekker fram, er basert på en doktorgradsstudie av Eve Guillaume (Guillaume, 2011) hvor hun forsøker å undersøke det som Hollnagel legger som et premiss i sin teori, hvor man skal se etter *«how and why things go right, rather than wrong»*. Når Guillaume i sin forskning skal undersøke det positive, opplever hun at dette i praksis gir virksomhetene liten effekt, og hun må falle tilbake til å undersøke nesten-ulykker. Hale argumenterer for at *«It is all very well looking at successes, but they don't seem easy to define without contrasting them with (incipient) failures*» (Hale, 2014, s. 64). Dette tyder på at det er vanskelig se på det som går bra uten å samtidige forholde seg til det som går galt.

Oppsummert er kan vi peke på noen hovedargumenter mot Hollnagel sin tilnærming til RE.

Hollnagel og RE mangler empirisk bevis som underbygger de ulike forutsetninger og påstander som perspektivet hviler på. I tillegg legger Hollnagel og RE for stor vekt på

etterpåklokskap, hvor han i for stor grad peker på å analysere tidligere hendelser. Den reaktive tilnærmingen til sikkerhet fører til at Hollnagel legger for lite vekt på design av system som har en iboende sikkerhet og «resilience».

4. Metode

Dette kapittel vil jeg gjøre rede for hvordan studien er gjennomført. I kapittelet vil de metodiske valg som er foretatt forklares og begrunnes. Styrker og svakheter ved tilnærmingen vil diskuteres. Dette for å skape en forståelse av hvordan studien har blitt gjennomført og de eventuelle utfordringer som har oppstått i gjennomføringen av studien.

Jeg har valgt en kvalitativ studie som baserer seg på semistrukturerte intervjuer med seks personer, som jobber med sikring i ulike selskap som har egenopererte installasjoner offshore. En kvalitativ metode er velegnet til å undersøke og skape en forståelse for de kontekstuelle forholdene som skal undersøkes. Metoden gir en mulighet til å fordype seg i problematikken og gir samtidig mulighet til å justere tilnærmingen og problemstilling underveis.

4.1. Valg av forskningsdesign og strategi

I denne delen vil jeg beskrive forskningsdesignet for studien min. Dette designet bestemmer hvordan den empiriske undersøkelsen er strukturert og relaterer seg til problemstillingen i studien (Jacobsen, 2022).

Studien konsentrerer seg om operatørselskapenes håndtering av dronetrusler på norsk sokkel. Valg av forskningsdesign påvirker studiens gyldighet og pålitelighet. Måten data er samlet og behandlet på, avgjør svarene jeg får og hvor etterprøvbare de er.

Valg av undersøkelsesopplegg har betydning for studiens gyldighet og pålitelighet. To viktige aspekter av gyldighet er: Intern gyldighet, om studien gir en troverdig beskrivelse og om datasettene støtter konklusjoner om årsak og virkning og ekstern gyldighet, om studiens resultater kan generaliseres (Jacobsen, 2022, s. 99).

Jeg hadde to forskningsdesign å velge mellom; intensivt og ekstensivt. Et intensivt design lar forskeren dykke dypt ned i et emne, konsentrere seg om detaljene og forstå virkeligheten. På den annen side gir et ekstensivt design en bredere tilnærming, med mulighet til å undersøke flere enheter. Et intensivt designet ble lagt til grunn for denne studien. Årsaken til dette er at det gir en dypere forståelse av temaet og hvordan forhold henger sammen (Jacobsen, 2022, s. 100). Videre, har jeg tilnærmet meg dette som en enkeltcase-studie, en tilnærming som gir en detaljert beskrivelse og mulighet for å avdekke kausale forhold (Jacobsen, 2022, s. 105–107).

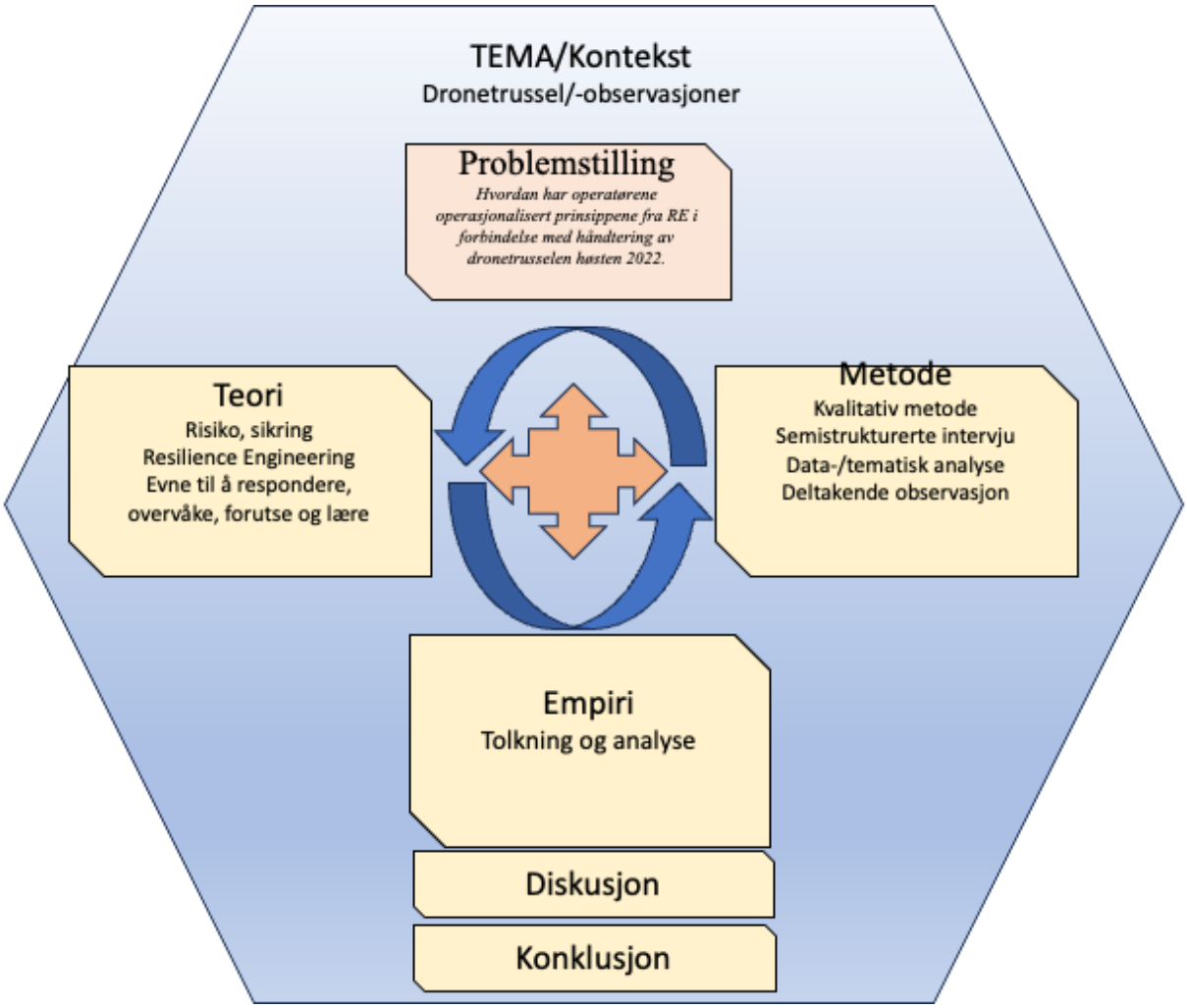
Det finnes ulike tilnærminger for å komme fra problemstilling til svar. Tjora beskriver ulike strategier som induktiv, deduktiv og abduktiv. Jeg har i min studie valgt å legge meg opp mot en abduktiv tilnærming. Denne tilnærmingen starter på samme måte som induksjon med empirien, men hvor teori og perspektiver spiller inn i forkant eller i løpet av

forskningsprosessen (Tjora, 2021, s. 40). I en slik tilnærming *«[...] leter man etter sannsynlige beskrivelser og forklaringer»* (Jacobsen, 2022, s. 38). Det er dermed en kontinuerlig samhandling mellom teori og empiri. Abduktiv tilnærming kan forstås som en iterativ prosess, hvor teori, empiri, hypotese og spørsmål påvirker hverandre i et samspill (Jacobsen, 2022, s. 38).

Ifølge Tjora *«[...]tar ofte kvalitativ forskning utgangspunkt i en eller flere teoretiske tradisjoner for å definere rammen av hva som interessante problemstillinger»* (Tjora, 2021, s. 39). Teori var sentral under utarbeidelse av problemstilling og intervjuskjema. Når empiri skulle analyseres og kategoriseres ble dette gjort med bakgrunn i Hollnagels fire egenskaper. Under intervjuene dukket det opp forhold jeg ikke hadde tenkt på. Dette bidro til at det var noe variasjon i hvilken retning de ulike intervjuene gikk. Dette igjen påvirket problemstilling og presentasjon av empiri og analysen.

Gjennom forskningsstrategi og -design har studien som mål å undersøke operatørselskapenes håndtering av dronetrussel. Ved å intervjue utvalgte personer med inngående kunnskap om studiens tema og problemstilling søker jeg gjennom informantens perspektiv og erfaring å få en inngående forståelse av problemstillingen. Det ligger dermed en ontologisk tilnærming til grunn, noe som kan forklares som en fortolkningsbasert forståelse av virkeligheten. Dette kan oppfattes som om at jeg legger vekt på hvordan virkeligheten forstås og fortolkes av informantene. Det som er viktig, er dermed ikke hva som skjer, men hvordan det fortolkes. En slik tilnærming likestilles ofte med kvalitativ metode (Jacobsen, 2022, s. 33–37).

Figuren under illustrer studiens design, hvor konteksten (dronetrussel, og økt trussel fra Russland) ligger som et bakteppe for problemstilling, teori, metode og empiri. Illustrasjonen i sentrum av figuren viser den iterative prosessen, hvor teori, problemstilling, og empiri kan påvirke hverandre. Funn fra empiri kan for eksempel føre til endring i problemstilling, og valg av teori.



Figur 10 Forskningsdesign

4.2. Innsamling av data og intervjuer

Under utarbeidelse av problemstilling ble det gjort søk etter eksisterende forskning. Det var ikke gjort forskning på tema for studien, og det var dermed nødvendig å samle inn data selv. Som allerede beskrevet ble det valgt en kvalitativ metode, og innsamling av primærdata gjennom intervju. Kvalitativ metode egner seg for å svare på studiens problemstilling, hvor man skal avklare nærmere hva som ligger i et fenomen, der vi vet lite om fenomenet som skal undersøkes, og hvor problemstilling er uklar. Det er også en sammenheng mellom intensive opplegg og kvalitativ metode. Kvalitativ metode egner seg når det er behov for nærhet og dybde i undersøkelse av problemstilling (Jacobsen, 2022, s. 143–145).

Fordelen med en slik tilnærming er at det gjennom en nærhet til informanten, gir mulighet til å oppdage forhold man ikke har tenkt på, og det gir rom for en nyanserikdom. Ulike respondenter har ulik oppfatning av samme fenomen. Tilnærmingen gir også rom for

fleksibilitet, nettopp ved at man kan endre problemstilling og hva man ser etter. Samtidig kan man stille spørsmål om hvor representativ et datasett fra et lite utvalg er. I tillegg er datasettene som ble samlet inn komplekse, det er store mengder ustrukturert data som skulle behandles. En utfordring jeg møtte på er knyttet til fleksibilitet. Ved å være åpen for ulike svar i intervjuene kunne det være vanskelig å stoppe informanten, uten å begrense videre dialog og flyt (Jacobsen, 2022, s. 141–144).

4.3. Intervjuer

Intervju

Det finnes ulike måter gjennomføre en kvalitativ undersøkelse på, for eksempel observasjon, deltakelse og intervju. For denne studien var det naturlig å velge intervju. Jeg stod også overfor ulike måter å gjennomføre intervju på. Intervju kan gjennomføres i grupper, fysisk, telefon, teams og dybdeintervju med enkeltpersoner. Intervju var egnet for denne studien, da det var få enheter som skulle intervjues, og oppmerksomheten var rettet mot den enkeltes erfaring og perspektiv (Jacobsen, 2022, s. 162–163).

Dybdeintervju/semistrukturerte intervju

Intervjuene ble gjennomført som semistrukturerte intervju eller dybdeintervju (Tjora, 2021, s. 127). Årsaken til å velge denne type intervjuform er at målet er å *«[...] skape en situasjon for en relativt fri samtale som kretser rundt noen spesifikke tema som forskeren har bestemt på forhånd»* (Tjora, 2021, s. 127). Intervjuet kan ha ulik grad av åpenhet, noe som styres av spørsmål eller for eksempel en intervjuguide. Dette betyr at intervjuet ikke er helt åpent, men styres av tema og hovedspørsmål og eventuelle oppfølgingsspørsmål. Det er dermed ikke en helt åpen samtale, noe som kan føre til stor kompleksitet i dataen (Jacobsen, 2022, s. 166). Andersen peker på at idealet med å gjennomføre intervjuer med nøkkelinformanter er en passiv lyttende rolle, hvor det stilles åpne spørsmål og informantens respons styrer samtalen. Samtidig peker han på at ved intervju av ressurssterke informanter, *«[...]kan en bevisst og aktiv forskerrolle kunne gi større uttelling – og dermed øke validitet og reliabilitet»* (Andersen, 2006, s. 279). Samtlige av informantene har betydelig erfaring og kompetanse og må anses som ressurssterke. Jeg har i min studie forsøkt å balansere mellom det å være passiv og tilstrekkelig aktiv gjennom intervjuene. I ettertid kunne enkelte intervju vært styrt enda mer, men det er ofte vanskelig å vite hvor man ender når man beveger seg noe ut av tema.

Valg av informant

Ved valg av informanter er det ifølge Tjora en hovedregel å velge ut informanter som kan uttale seg reflektert om tema (Tjora, 2021, s. 145). Ettersom det er et begrenset antall personer som jobber med sikring i de ulike selskapene er anonymitet vektlagt i presentasjon av informantene og empiri. Det gir også et begrenset rom for utvelgelse av personell. Samtidig kunne jeg valgt personer som har andre roller i selskapet, for eksempel beredskapspersonell, ledere, «aviation» med mer. Ved valg av informant var det viktig at de som ble intervjuet hadde kunnskap om både selve håndteringen og sikring. Andersen peker på at å velge velinformerte informanter som har kunnskap om det som skal belyses er viktig. Deres subjektive erfaringer er viktige bidrag til å forstå og tolke (Andersen, 2006, s. 282). Samtlige som ble intervjuet hadde en rolle som rådgiver eller leder innen sikring. Alle hadde også en aktiv rolle i håndteringen av droneobservasjonene. Enkelte hadde både en rolle i beredskap og sikring. Dette har sammenheng med størrelse på operatørselskap, hvor de mindre operatørselskapene ofte har en rolle som dekker både beredskap og sikring. Jeg har utelatt dette fra oversikten (tabell 1 lenger nede), ettersom den informasjonen sammen med annen informasjon i studien kan bidra til identifisering.

Det ble gjennomført seks intervjuer. Jeg opplevde at det mot slutten av intervjuene ble mye gjentagelser og lite ny informasjon, og valgte derfor å ikke gjennomføre flere intervjuer. Dette kan tyde på at man har oppnådd en metning. Det vil si at å gjennomføre flere intervjuer ikke vil bidra til ny kunnskap (Jacobsen, 2022, s. 203). Dette kan også være en indikasjon på at tema er relativt snevert og at gruppen er relativt lik/homogen (Tjora, 2021, s. 158). Hadde jeg for eksempel valgt personell fra ulike fagområder kunne dette bidratt til enda større nyansering av problemstilling, og ved at jeg ikke valgte dette kan dette påvirke studiens validitet. Det kan dermed påvirke i hvilken grad det er mulig å generalisere studiens funn. Tabell 1 (s.41) viser oversikt over de seks intervjuene/informantene.

Forberedelser

Med bakgrunn i tema, problemstilling og teori ble det utarbeidet en intervjuguide. Denne ble bygget opp med noen spørsmål innledningsvis som skal bidra til å etablere en trygghet hos informanten. Det var deretter fire hovedspørsmål som var relatert til evnen til å respondere, overvåke, forvente og lære. Avslutningsvis var det noen spørsmål for å avrunde intervjuet og avdekke om det evt. var noe jeg burde spurt om som jeg ikke hadde inkludert.

I tillegg til hovedspørsmålene hadde jeg inkludert en rekke tilleggsspørsmål, som kunne stilles hvis samtalen stoppet opp (Tjora, 2021, s. 160). Det var i liten grad nødvendig å bruke disse. Samtidig hadde jeg sendt ut både et samtykkeskjema og informantguiden i forkant. De hadde dermed mulighet til å forberede seg. De fleste informantene hadde forberedt seg til intervjuet, de hadde leste gjennom og reflektert over sine svar. Ulempen med å sende over så mange spørsmål er at de kunne bli påvirket. I tillegg til spørsmålene og samtykkeskjema, la jeg med et informasjonsskriv for å gi bakgrunnsinformasjon om studien og kontekst. Her ble også tema og problemstilling beskrevet.

Gjennomføring

Intervjuene ble i all hovedsak gjennomført på teams. Dette sparte både meg og informantene for tid og tilrettela for at personer på andre geografiske lokasjoner kunne intervjues (uten å måtte reise). Ulempen er at det kan være vanskeligere å etablere tillitt og åpenhet, og at den man intervjuer kan bli distrahert av andre forhold i møte. I enkelte av intervjuene oppstod slike situasjoner, enten at de ble distrahert av andre som snakket til dem, eller at de skulle vise meg noe på skjermen. Dette var allikevel ikke et stort problem. Et av intervjuene ble gjennomført fysisk. Dette ga en bedre kontroll av situasjon, tilrettela bedre for tillitt og åpenhet, og ga også bedre mulighet til å lese kroppsspråk. Jeg opplevde ikke vesentlig forskjell på teams eller fysiske møter. Min fordel er at jeg kjenner informantene, og innehar selv samme rolle som de jeg intervjuer, noe som kan bidra til åpenhet og tillitt (Jacobsen, 2022, s. 165).

Det ble gjennomført opptak av samtlige intervju, noe informantene samtykket til. Ettersom møtene ble gjennomført på teams var ikke dette noe informantene la merke til. Samtykke ble gjentatt før intervju startet og det ble presisert når opptak ble startet og stoppet. Opptak av lyd muliggjorde at jeg kunne rette full oppmerksomhet mot det som ble kommunisert, og stille oppfølgingsspørsmål uten å bli distrahert av notatskriving.

Intervjuene ble gjennomført over en periode på seks uker, hvor tilgjengelighet til informantene var avgjørende for når møtene kunne gjennomføres. Dette ga meg tid til å reflektere og forbedre gjennomføring av intervjuene.

Det var satt av en time til intervjuene, men ved enkelte intervju valgte informanten selv å fortsette diskusjon etter at møtet skulle vært avsluttet. Sett i ettertid kunne en time være litt lite tid, og jeg kunne planlagt for opp mot 90 minutter. Samtidig ville dette økt mengde og

kompleksiteten på datasettene. Et alternativ var å snevre inn problemstillingen, og styre samtalen i større grad.

I de fleste intervjuene var det en naturlig flyt, og informantene beveget seg naturlig mellom de ulike temaene som var satt. Det var dermed ikke nødvendig å «styre samtalen» fra spørsmål til spørsmål. Dette gjorde det selvsagt noe mer utfordrende når datamaterialet skulle analyseres og kategoriseres. Det var også forskjell på hvor mye tid jeg brukte på de ulike tema i de enkelte intervjuene. Hvis jeg i et intervju hadde brukt lite tid på for eksempel læring, kompenserte jeg ved å bruke mer tid på dette i et annet intervju. Samtidig var det ikke like mye data om alle temaene, noe som både gjenspeiles i empiri og diskusjon.

Informant	Gjennomføring	Varighet
1	Teams	1 time
2	Teams	1 ½ time
3	Teams	1 time
4	Teams	1 time
5	Fysisk	1 ½ time
6	Teams	1 time

Tabell 1 Oversikt over informanter

Forskerens rolle - deltakende observasjon

Mitt valg av næring og informanter kan sammenlignes med å forske i egen organisasjon. Dette en metode innen kvalitativ forskning som kalles deltakende observasjon (Jacobsen, 2022, s. 160–161). Selv om jeg ikke har gjennomført intervju og forskning når observasjonene av dronene pågikk, har jeg selv hatt en rolle i egen virksomhet med å håndtere situasjonen, jeg jobber i petroleumsnæringen og kjenner flere av de som har vært intervjuet. Dette er også personer jeg skal samarbeide med i ettertid. Fordelen er at det kan være lettere å få tilgang til informasjon ved at jeg kjenner både tema og personer, det kan være lettere å få tillitt, og jeg vil kunne være bedre i stand til å forstå konteksten. Jeg opplevde selv at kjennskap til informantene gjorde at det var en naturlig åpenhet og tillitt, og de ga selv uttrykk for at de utleverte mer informasjon enn hva de ville gjort til andre, da de hadde tillitt til hvordan informasjonen ble håndtert.

Ulempen som jeg har måttet være klar over, er utfordringen med å holde tilstrekkelig kritisk avstand og ikke være forutinntatt. Jeg har mine erfaringer og tanker om hvordan jeg ville svart. Jeg kunne komme i fare for å søke informasjon som bekreftet egne hypoteser eller fordommer,

og jeg kunne også komme i fare for å legge bånd på meg selv av hensyn til videre samarbeid med informantene (Jacobsen, 2022, s. 60).

For å unngå det såkalte 'bias' og ovenfornevnte utfordringer i min etnografiske feltforskning, var jeg nøye med å praktisere selvrefleksjon og anerkjenne egne forutinntatte holdninger. Jeg sørget for at utvalget av deltakere var representativt. Det var viktig for meg å formulere nøytrale spørsmål og tilpasse metodene basert på kontinuerlig læring i feltet. Jeg innhentet også tilbakemelding fra kolleger, og rapporterte funnene med åpenhet om begrensninger og kontekst. Etiske overveielser, som informert samtykke og konfidensialitet, ble nøye vurdert for å opprettholde integriteten av forskningen.

4.4. Etterbehandling av data

I denne delen beskriver jeg hvordan data fra intervjuene er behandlet og konvertert fra lyd til tekst, samt hvordan disse datasettene er systematisert og redusert slik at man sitter igjen med data som kan brukes til analyse.

Transkribering

Det ble gjort lydopptak av intervjuene. Opptakene ble transkribert ved bruk av et dataprogram som ikke er tilkoblet internett. Programmet bruker «OpenAI» stemmegjenkjennings-tjeneste «Whisper», og transkriberer tale til tekst. Etter at intervjuene var transkribert måtte de gjennomgås og korrigeres, og i enkelte situasjoner måtte jeg gjennomgå opptak på nytt for å korrigere teksten. Årsaken er at enkelte dialektord ikke fanges opp, og at den skriver enkelte ord slik programmet hører det (fonetisk). I tillegg måtte enkelte av de sitater som skulle brukes endres noe fra muntlig til skriftspråk, samt komprimeres uten at mening ble endret. Det som ikke fanges opp i en slik transkribering er kroppsspråk og usikkerhet hos informantene. En slik prosess er ikke mulig å gjøre helt objektiv, og peker på at jeg må være bevisst min rolle i denne prosessen (Kvale & Brinkmann, 2009). Fordelen med denne tilnærmingen er at den sikrer etterrettelighet. Sitatene er tilnærmet korrekt, og ikke basert på delvis notater eller slik jeg husker det. Der hvor jeg har vært usikker på mening, har jeg hatt mulighet til å søke tilbake i lydopptak. Kvale peker samtidig på at selv ved transkripsjon er det ikke mulig å gjengi alt hundre prosent. Det vil kunne gå tapt noe informasjon i oversettelse fra tale til tekst. Programmet som er brukt er heller ikke hundre prosent korrekt, og viser ikke punktum eller komma. Selv om bruk av kunstig intelligens er arbeidsbesparende, krever det allikevel betydelig tid i omarbeidelse og gjennomgang.

Dataanalyse: «tematisk analyse»

Dataanalyse legger til grunn at det en informant sier i et intervju kan bli redusert til mindre og mer overordnede og meningsfylte kategorier (Jacobsen, 2022, s. 215). Dette er dermed en strukturering av data, og bidrar til å identifisere vesentlig informasjon. Transkripsjonen ble gjennomgått og ulike deler ble kategorisert med utgangspunkt i Hollnagel sine fire egenskaper, samt spørsmål som ble stilt innledningsvis og avslutningsvis i intervjuet. Det ble dermed tatt utgangspunkt i intervjuguide og teori for å kategorisere intervjuene. For å kategorisere data ble det brukt Excel. I utgangspunktet laget jeg to kolonner for å kategorisere sitater. En kolonne med de fire egenskapene respondere, overvåke, lære og forutse. Dette var basert på teori og spørreskjema. Dette var hovedkategoriseringen av sitatene. Deretter en kolonne som var basert på intervjuene og tema som ble adressert. Jeg benytter her en kombinasjon av både begrepsstyrte koder, de som er fra teorien og datastyrte kategorier, de som kommer fra innsamlet data (Kvale & Brinkmann, 2009, s. 209). Hensikten var å kunne systematisere og analysere data. Denne listen ble etter hvert ganske omfattende, og i tillegg var det flere av sitatene som kunne si noe om flere temaer. Det ble derfor opprettet en ytterligere kolonne, hvor samme kategorier ble brukt i begge. Dette ga en mulighet til å sortere data på ulik måte, og gjorde det også lettere å velge ut det som kunne og ikke kunne gi verdi til studien. I tillegg hadde jeg en kolonne som viste hvilket intervju data var hentet fra. På denne måten kunne jeg identifisere felles meninger, og hva et fåtall mente og sa. Totalt ble det plukket ut 225 sitater som var vurdert som relevant. Det ble etablert ca. 80 kategorier, men dette inkluderte også ulike varianter av samme kategori, for eksempel myndigheter. Her var det også varianter som beskrev hvilken myndighet – politi, forsvar og Ptil. Det var også en rekke kategorier som kun dekket et fåtall av sitatene. Noen av de underkategoriene som ble brukt var: bevissthet, organisasjonsendring, lederforankring, hemmelighold, informasjon, situasjonsforståelse, kapasitet, kompetanse, ledelse, myndigheter, læring, mangel på informasjon, mangel på ressurser, metodens betydning, overvåke, planverk, trusselvurdering, risikoerkjennelse, rolle og ansvar, samarbeid, «task-force», tiltakskort, trening og øvelse, økt fokus. Disse kategoriene vil leseren også finne igjen i beskrivelse av empiri. Med bakgrunn i dette ble det i kapittel 6 etablert noen hovedkategorier som danner grunnlag for diskusjon av operatørenes operasjonalisering av de fire egenskapene forutse, overvåke, respondere og lære.

Denne delen kalles også koding og henviser til *«[...] analyse, undersøkelse, sammenligning, begrepsliggjøring og kategorisering av data [...]»* (Kvale & Brinkmann, 2009, s. 209). Etter at

data ble systematisert og kategorisert, ble den gjennomgått for å identifisere sammenhenger og identifisere data som bidro til å svare på problemstilling. Resultatet er presentert i kap. 5. Fullstendige sitater er inkludert i presentasjon av empiri for å underbygge funn, og gir en bedre forståelse av informantenes mening.

4.5. Etiske hensyn og vurderinger

Personvern – konfidensialitet

Personvern står helt sentralt i denne type forskning, og det innebærer en stor grad av tillitt mellom informant og den som skal gjennomføre intervju med hensyn til hvordan informasjon håndteres. Før studien ble gjennomført ble det innhentet tillatelse fra Norsk senter for forskningsdata (NSD). Denne ble godkjent 27.04.2023.

Jacobsen peker på at det ikke er mulig å garantere hundre prosent anonymitet, men at man som forsker garanterer for at informasjon, så langt som mulig, ikke skal komme på avveie (Jacobsen, 2022, s. 50).

I studien er det vektlagt at det ikke skal være mulig å koble informasjon til den enkelte informant. Informantene og virksomhetene er heller ikke identifisert. Den enkelte informant ble gitt et nummer som har blitt brukt i forbindelse med intervjuene, transkribering av intervju og ved sitatbruk. Jeg har ved flere anledninger valgt å sitere fra intervju uten å henvise til hvilken informant som har sagt hva. Dette er gjort for å redusere sannsynlighet for å «tolke» seg til hvem som har sagt hva, og dermed identifisere virksomheten.

Datasikkerhet er en utfordring og krever at man er bevisst på håndtering av elektronisk data. Data har blitt samlet inn og håndtert elektronisk, både opptak av intervju og den transkriberte informasjon har blitt lagret elektronisk. Dette har vært lagret på en kryptert PC med passordbeskyttelse. I tillegg har det vært lagret i kryptert og passordbeskyttet skylagringsløsning, for å sikre tilgjengelighet og «backup» av data. Det er brukt to ulike PCer for håndtering av data, en for innkalling og gjennomføring av intervju og en for håndtering av data. For transkribering av data er det blitt brukt et dataprogram som ikke har vært koblet til internett.

Datasikkerhet

I tillegg til personopplysninger har jeg i studien også fått tilgang til sensitiv informasjon som ikke kan brukes i studien. Dette underbygger behov for sikker oppbevaring av data. Jeg har her måttet gjøre en avveiing av hva som kan tas med i studien og hva som må utelates, da

det for eksempel kan avsløre sårbarheter eller tiltak som ikke bør gjøres kjent. Det er ikke bare enkelte informasjonsbiter som må vurderes, men den samlede informasjonen som presenteres. Jeg har derfor måttet utelate data som er relevant for studien, men som på grunn av konfidensialitet har måttet utelates.

4.6. Validitet og reliabilitet

Et viktig spørsmål ved denne studien er i hvilken grad konklusjonene er gyldige og til å stole på. Det er tre begreper som kan si noe om denne studiens kvalitet. Intern gyldighet (validitet), pålitelighet (reliabilitet), og overførbarhet (ekstern validitet) (Jacobsen, 2022, s. 240).

Intern gyldighet

Jakobsen peker på flere forhold som må vurderes når det gjelder validiteten, blant annet hvorvidt jeg har fått tilgang til de riktig kilder, og om kildene gir riktig informasjon (Jacobsen, 2022, s. 241). I delkapittel 4.3 om valg av informanter peker jeg på jeg har en begrenset mengde informanter og at det kan være en homogen masse. Disse representerer dermed ikke et tverrsnitt av operatørselskapene, men kan sies å representere et tverrsnitt av personer som jobber med sikring i operatørselskapene. Jeg kunne inkludert personer som jobber med beredskap både «onshore» og «offshore», samt annet fagpersonell enn sikringspersonell som deltok i arbeidet. Dette ville bidratt til å gi en større bredde og andre perspektiver. Ettersom jeg tilhører samme faggruppe som jeg har intervjuet, er det en fare for at jeg har vært forutinntatt, noe som kan ha preget innsamling av informasjon og intervju. Ved å ha intervjuet annet fagpersonell ville jeg kunne redusert denne faren. Samtidig er personellet som ble intervjuet eksperter og meget erfarne innen sitt område. Enkelte hadde også eksempelvis ansvar for både sikring og beredskap, og enkelte en lederrolle.

Samtlige informanter deltok aktivt og er primærkilder. De har dermed en nærhet til situasjon som ble studert. De er også alle meget erfarne innen sitt område og har dermed stor kunnskap og forståelse av faget. Ettersom dette er personer jeg kjenner og tidvis samarbeider med, kan en utfordring kan være at personellet har tilpasset sin forklaring for å fremstå på en bedre måte, eller at de utelater informasjon av samme grunn. Ettersom det er sensitiv informasjon kan også dette bidra til at informasjon utelates. For å håndtere dette er det brukt flere kilder, noe som *«[...] kan bidra til å gi en gyldig beskrivelse av fenomenet»* (Jacobsen, 2022). En styrke ved gjennomføring kan være at jeg har god kunnskap om hendelsen. I tillegg

kan det bidra til at jeg bedre forstår det som blir beskrevet av informantene, noe som kan gjøre det lettere å stille oppfølgingsspørsmål. Samtidig er det en fare ved dette ved at jeg legger egne fordommer og meninger inn i både tolkning og analyse. Før intervjuene gjorde jeg meg opp noen tanker om hva jeg ville svart, dette kan ha preget for eksempel analysen. For å ivareta dette har jeg kritisk gjennomgått resultatene, og i begrenset omfang diskutert enkelte funn med informantene. At det er i begrenset omfang skyldes utfordring med å få tilgang til informantene.

Pålitelighet

I denne delen stilles spørsmålet om det er trekk ved selve måten studien har blitt gjennomført på som har skapt de resultatene som jeg har kommet fram til (Jacobsen, 2022).

Min relasjon til de jeg har intervjuet, tidligere erfaring, både gode og dårligere, samt selve interaksjon mellom meg og informanten i intervjuet, kan ha påvirket informanten. Dette kalles intervjueffekt (Jacobsen, 2022, s. 251). Hvor og når intervju blir gjennomført kan også påvirke informanten. På grunn av COVID-19 og den utstrakte bruken av hjemmekontor og teams var samtlige fortrolig og godt kjent med bruk av teams. Dette er noe alle brukte daglig i sin arbeidssituasjon. Møtene var i tillegg planlagt i god tid slik at informantene hadde tid til å forberede seg.

Et annet forhold som kan påvirke pålitelighet er unøyaktighet ved registrering og analyse av data. Dette ble ivaretatt ved å bruke lydopptak, noe som gjør at det ha vært mulig å sjekke opptak ved usikkerhet om hva som ble sagt. I tillegg er ikke kvaliteten ved bruk av AI til transkripsjon nøyaktig, da programmet kan utelate deler av hva som ble sagt.

Overførbarhet – ekstern gyldighet

Ekstern gyldighet dreier seg om i hvilken grad funn fra studien kan generaliseres. En svakhet ved denne studien kan være at det er få personer intervjuet. Samtidig kan funn fra studien tyde på det er en viss overførbarhet, ikke bare til andre operatørselskaper, men også andre næringer. Et eksempel på dette kan være det som omhandler betydning av samarbeid. Metning i funn kan være en indikasjon på at man har valgt tilstrekkelig enheter, og at kan være en overførbarhet til andre enheter i samme kontekst. I intervjuene var det mye lik informasjon og erfaring, og etter at det siste intervjuet ble gjennomført var det lite ny informasjon. Dette kunne dermed tyde på at funn har en overføringsverdi til andre operatørselskaper og for eksempel riggselskap (Jacobsen, 2022, s. 256).

4.7. Fordeler og ulemper med valgt metode

I de foregående delkapittel er det pekt på ulike fordeler og ulemper ved metode valg. I denne delen vil jeg dermed oppsummere og belyse styrker og svakheter ved det valgte intensive forskningsdesignet, hvor semistrukturerte intervjuer ble benyttet for å forstå håndtering av dronetrusler av operatørselskapene på norsk sokkel. En umiddelbar styrke ved dette valget er muligheten for dybdeforståelse av emnet, hvor nyanser og detaljer kommer frem. Denne metoden fremhever den fortolkningsbaserte virkelighetsforståelsen som ligger til grunn for studien.

Intervjuformen tillater fleksibilitet og kan danne uforutsette innsikter. Derimot, med min bakgrunn fra samme næring, kan det potensielt føre til fordommer og bekreftelsesbias, som kan utfordre studiens interne gyldighet. Bruken av "teams» for intervjuer, selv om praktisk, kan skape en avstand til den som blir intervjuet. Det er benyttet kunstig intelligens til å transkribere. Dette kan være effektivt, men kan påvirke nøyaktigheten av teksten og må derfor etterbehandles.

Videre, med kun seks informanter, er det begrensninger på ekstern gyldighet, da funnene kan være utfordrende å generalisere bredt. Likevel har denne abduktive tilnærmingen, som en iterativ prosess mellom teori og empiri, muliggjort kontinuerlig justering av studiens fokus basert på innsamlede data.

Til tross for disse utfordringene gir det intensive designet, i sammenheng med semistrukturerte intervjuer, en rik og dyptgående forståelse av håndtering av dronetrusler i den gitte konteksten.

5. Empiriske funn

I dette kapittelet sammenstilles og presenteres mine empiriske funn. Disse er basert på intervjuer av personell med sikringsoppgaver eller ansvar i de ulike operatørselskapene og som alle har hatt en sentral rolle i å håndtere dronetrusselen mot operatørselskapene høsten 2022[2].

Av de seks informantene som er intervjuet, og som representerer seks ulike operatørselskap, er det bare ett selskap som ikke selv har rapport inn observasjon av droner. Samtlige av de andre har observasjoner. De første observasjonene ble gjort hos en av operatørene i juli, med påfølgende observasjoner i løpet av høsten hos de andre operatørene.

Intervjuene tok utgangspunkt i de fire egenskapene til Hollnagel. Basert på den informasjonen som fremkom vil jeg i dette kapittelet presentere funn som er relevant for å kunne besvare studiens problemstilling.

5.1. Forståelse av «resilience» i virksomheten

Innledningsvis i hvert intervju hadde jeg et innledende spørsmål om hvordan de forholdt seg til begrepet «resilience» og om dette var noe de jobbet for. Det var ulike forståelse og bevissthet om «resilience»-begrepet, samtidig brukes «resilience» og robusthet om hverandre. I den grad man snakket om robusthet eller «resilience» så var det enten i forhold til en robust beredskap, og i den forstand at man skal være i stand til å håndtere hendelser. En av informantene uttrykte:

> *Jeg vil jo si at i forhold til dette med robusthet, så har det vært som en del av målet og strategien vi har hatt de siste årene. Dette har vært en viktig del av å utvikle beredskapen. En robust beredskapsorganisasjon er noe som jeg har hatt som mål over lang tid. Det at du har kompetanse, at du har nok personell til å håndtere hendelser, og at du har evne til å håndtere hendelser over tid. Samtidig har vi innen sikring hatt dårlig robusthet, vi har manglet kompetanse og personell i organisasjonen.*

[2] Ved gjengivelse av sitater fra informanter er det i enkelte tilfeller ikke vist til hvilken informant som har uttalt sitatene. Årsak er at det kan være informasjon i sitatet som kan brukes til å gjenkjenne virksomheten, dette kan for eksempel være med referanse til størrelse på virksomheten eller andre forhold som sammen med andre sitater kan bidra til å identifisere vedkommende eller virksomheten vedkommende jobber for.

Informanten peker her på at elementer som tilstrekkelig personell, kompetanse, og evne til å stå i en hendelse over tid er deler i det å være robust. En annen informant beskrive «resilience» som:

> *«[...] hvor motstandsdyktig vi er overfor ulike angrep [...]».*

Informanten peker på at de har definerte fare og ulykkescenario (DFU) som beskriver ulike scenario som skal håndteres. I tillegg har de sikringsrisikoanalyser, og krav til sikring, som sier noe om hvordan de skal:

> *«[... robustgjøre seg, og hvilke håndteringsmekanismer de skal ha».*

Ifølge en annen informant er «resilience» noe man i større grad har oppmerksomhet mot innen cyberdomenet. Samtidig argumenterer hen for at:

> *[...]resilience er en del av fundamentet i både safety og security. Men man snakker mer om det innenfor cyber.*

Informanten forklarer videre at:

> *[...]ellers er det jo beredskapsorganisasjonen som skal håndtere det. Når det gjelder den reaktive fasen, håndtering, har vi innlemmet sikring i beredskapen[...].*

Sitatet viser at tilsiktede handlinger, som droner, blir håndtert som del av den ordinære beredskapen. Det kan dermed tyde på at «resilience» med hensyn til sikring ikke er noe eget, men bygges gjennom å være del av beredskap. Det informantene har til felles er at «resilience» omhandler evne til å håndtere en hendelse, og at sikring er del av beredskapen. Kommentarene fra intervjuene kan også tyde på at informantene ikke hadde et variert forhold til hvilke egenskaper eller elementer som inngår i arbeidet med å etablere «resilience» (eller jobbe mot en evne til «resilient» ytelse).

5.2. Evne til å forvente/forutse

Å kunne forutse hva som kommer til å skje opplever informantene som utfordrende. Informantene peker på at både manglende situasjonsforståelse og risikoerkjennelse, som beskrives i senere kapittel, er relevant for å forutse. I denne delen omhandles sikringsrisikovurderingen og trusselvurderingen.

Sikringsrisikovurderingene og trusselvurderingene er verktøy som kan bidra til å skape forståelse av hva man kan forvente. Det kan både bidra til å øke respons, men også evnen til å forutse. Flere av respondenten tok opp at tilnærmingen til identifikasjon av risiko var utfordrende. Den ble opplevd som statisk og greide ikke å fange opp dynamikken i det endrede risikobildet. En av informantene pekte på at flere av operatørene ser på muligheten for å etablere et bedre system for å øke situasjonsforståelsen, hvor en mer dynamisk tilnærming til risikoanalyse ble vurdert. En av utfordringene som informanten pekte på var

> *Den tradisjonelle metoden er på plass, men er ikke tilstrekkelig for å håndtere denne usikkerhet, nye fenomener oppstår nesten over natten, så dette krever en annen evne til å snu seg rundt, og denne tilnærmingen er ikke tilstrekkelig. Det viktigste er at risikoeiere skal være kjent med risiko, og hvilke verdier de sitter på. Det har de ikke i dag.*

Informantene peker her på at metoden ikke gir en tilstrekkelig oversikt over risikoelementene når de hele tiden kan endre seg.

Informant 3 pekte på utfordringen knyttet til sannsynlighetsbegrepet:

> *Jeg tror ikke vi er i mål innenfor analysebiten. Standard analyser og risikotenkning med konsekvens og sannsynlighet er ikke tilstrekkelig. Sannsynlighetsbiten i sikringssammenheng skal nærmest tas bort. For det å trekke inn sannsynlighet med det vi har erfart de siste to år, det er vanskelig. Du kan godt si at det her er så lite sannsynlig, men er konsekvensen høy nok, så må det her være med. Og i dag tror jeg nok flere og flere erkjenner at det kan skje. Og dermed så jeg tror kanskje metodikken vår, eller den historiske biten innenfor sikring, det er vanskelig å bygge videre på.*

Trusselvurdering er del av sikringsrisikovurderingen. De fleste operatørene gjennomfører en årlig trusselvurdering, og flere velger å bruke en ekstern leverandør til å gjennomføre dette. Operatørene overvåker myndighetene sine råd og trusselvurderinger og legger disse til grunn for egne vurderinger. En av operatørene beskrev at de hadde identifisert indikatorer som de skulle følge med på for å se på utviklingen av trusselbildet, men for de fleste var det innspill og endring fra myndighetene eller hendelser som medførte endringer i egen trusselvurdering.

> *Trusselvurderingen blir oppdatert minst en gang i året. Men i tillegg til det, så blir den oppdatert ved behov. Trusselvurderingen ble for eksempel oppdatert etter «Nord Stream», og vi gjorde litt endringer i forhold til innsider. Når dronene kom, medførte også dette en oppdatering.*

Informantene opplevde at det var en utfordring med måten de tilnærmer seg trusselvurderingen på. Den ble beskrevet som reaktiv og lite dynamisk, og flere så på muligheten for å forbedre denne tilnærmingen.

> *Tidligere så har vi gjort trusselvurdering en gang i året, men nå har vi et mye mer dynamisk bilde som endrer seg mye kjappere. Jeg synes at vi må ha et mer online-system og prosess for å overvåke kontinuerlig trusselbildet. For det holder ikke med en gang i året. Og det har vi jo sett, og spesielt når du har hatt en situasjon som vi har hatt nå.*

En tilnærming som flere av informantene har, er at de legger til grunn et scenario for risikovurderingen. Dette kan være basert på trusselvurderingen, eller så kan det være at man bestemmer seg for en dimensjonerende trussel som ligger til grunn for sikringen. En av informantene stilte spørsmål ved om det var nødvendig med denne type detaljerte scenario.

> *[...] Men det å være forberedt og det å forvente at det kan skje noe, trenger vi et spesifikt scenario for det? Hvor detaljert et scenario trenger vi å være forberedt på ting? Jeg tror ikke at vi trenger detaljerte scenario. Jeg tror vi har vært for detaljerte.*

Noe av årsaken til dette argumentet var at informanten opplevde at det ble for mange scenario, i tillegg var det vanskelig å være presis med stort utvalg av scenario. Det kan også bli omfattende både å vedlikeholde, samt forholde seg til. En av de andre informantene hadde valgt en annen tilnærming og valgt noen få prinsipielt forskjellige hovedscenarioer som ivaretok mange av de små detaljerte scenarioene. Fordelen var da at de kunne konsentrere seg om et mindre antall scenarier, men at de allikevel hadde ivaretatt de prinsipielt ulike mulige utfallene. Ulempen var at de for eksempel ikke hadde et detaljert tiltakskort for droner, da dette var beskrevet i et generisk tiltakskort.

5.3. Evnen til å overvåke

Når informantene ble spurt om overvåkning kunne de fortelle at dette var noe som i utstrakt grad ble utført innen «safety» faget, men at dette i liten grad ble gjennomført på samme måte innen sikringsfaget. Samtidig utføres det for eksempel en overvåkning av beredskapsorganisasjonens ytelse gjennom trening, øvelse og virksomhetens kompetansesystem.

Når det gjelder overvåkning av eksterne forhold som trussel, peker de på at de i stor grad er avhengig av myndighetene. Overvåkning består i utgangspunktet av å følge med på myndighetenes råd og trusselvurderinger, men også media med hensyn til hendelser. I den grad indikatorer ble brukt så var for eksempel hendelser i inn og utland en indikator, og media var en kilde som ble overvåket. Enkelte av operatørene brukte tredjeparts leverandører (eksterne konsulentfirma):

> *[…] selskaper som overvåker og leverer trusselvurderinger, til overvåkning av trusselbilde og media, og noen veldig få hadde en systematisk overvåkning av media ved bruk av datasystemer.*

Samtidig var dette en generell aktivitet mht. trusselbilde, og ikke bare med hensyn til dronetrussel.

Offshore er det i dag ingen som har egne systemer for overvåkning av droner, selv om dette er under utprøving. Samtlige offshoreinstallasjoner har et radarsystem, hvor de fleste er tilkoblet en felles «sentral» hos en av operatørene. Dette er et pålagt system for overvåkning av fartøy på kollisjonskurs, og brukes også til for eksempel overvåkning av oljesøl. Dette systemet er i liten grad egnet til overvåkning av droner. Ifølge informantene var det flere som vurderte denne type systemer, men det var utfordrende å finne systemer som var effektiv, og samtidig ikke for dyre.

5.3.1. Situasjonsforståelse

Når de første observasjonene ble gjort var det en utfordring å forstå hva det var, hvem som stod bak og hva som var hensikten. Denne usikkerheten gjorde at det helt i begynnelsen, da de første dronene ble oppdaget, tok noe tid før informasjon om dronene ble delt. Årsaken var et behov for å forstå hva man stod ovenfor. Informanten beskrev at de opplevde det som en uklar situasjon:

[...] I begynnelsen var det veldig uklart. De som hadde observert dronene forstod ikke helt hva de stod overfor, de visste ikke helt hva dette var, og hvorfor de var der.»

En annen informant kunne også fortelle om utfordring med å forstå risiko.

[...] Men jeg ser veldig mange organisasjoner være fryktelig usikre på hvordan man skal håndtere det, ikke minst det med å forstå risikobildet. Dette var noe de ikke var forberedt på. Og man forstod ikke hvilken risiko en drone representerte.

Under intervjuene fremkom det også at ikke alle informantene opplevde dette som en stor risiko.

[...] Altså, når du ser på hele fenomenet med dronene og observasjonene, så er det ikke noe forsøk på å påføre skade[...]. Vi så på det primært som en strategisk kommunikasjon mellom nasjonalstater der vi egentlig ikke var en part.

Informanten forklarte videre:

[...] For det første, dronetrusselen i seg selv, altså det at dronene var i nærheten av plattformen, var ikke en veldig stor trussel[...].

En slik forståelse kan selvsagt også henge sammen med at man i ettertid har fått en bedre forståelse av trusselen, men informanten gav uttrykk for at dette var deres forståelse når trusselen oppstod. En annen informant hadde en annen tilnærming, hen kunne fortelle:

[...] Dette er en betydelig risiko, uavhengig av hvor den kommer fra, hva som er hensikt - disruption eller sabotasje. Det er en overordnet risiko. [...]

Dronene var ikke bare en sikringstrussel. I intervjuene fremkom det at en enda større trussel var relatert til sikkerhet. Det var bekymring for at dronene ville krasje inn i helikoptrene som fraktet personellet til og fra innretningen. Dronene utgjorde også en potensiell tennkilde hvis de hadde landet på innretningen.

Informantene ble også spurt om hva som kunne være årsak til manglende situasjonsforståelse. Informantene kunne da fortelle at manglende situasjonsforståelse var noe hen hadde pekt på som en risiko i sin virksomhet.

[...] Det er den risken som jeg har vist til flere ganger. At vi ikke har en tilstrekkelig situasjonsoppfattelse[...].

Dette hang sammen med både forståelse av risiko og måten risiko ble identifisert på. I tillegg ble det pekt på utfordringer knyttet til manglende erkjennelse av risiko.

5.3.2. Risikoerkjennelse

Manglende erkjennelse av alvoret og risiko var et elementene informantene pekte på som utfordrende. Ifølge informant 4 har ikke virksomhetene tilstrekkelig tatt innover seg alvoret.

> *[...]Vi har ikke tatt inn over oss at vi faktisk har krig i Europa. Vi lever i utkanten av Europa og har ikke sett alvoret i situasjonen.*

Informantene beskrev at det hadde vært utfordrende å skape en forståelse både av hva som kan skje, men også konsekvensene av mulige utfall. Det ble gjennomgående pekt på at sikringscenariet ofte ble sett på som lite sannsynlig.

Den økte aktiviteten fra forsvaret bidro til en økt erkjennelse av alvoret i situasjonen. Plutselig ble det veldig synlig og nært for enkelte installasjoner. En av informantene beskrev det på følgende måte:

> *[...] Når krigen kom, og når det plutselig befant seg NATO-fartøy ved innretningen, forstod våre ansatte alvoret i situasjonen.*

Sitatet viser hvordan tilstedeværelse av militære fartøy bidro til å øke forståelse av den alvorlige situasjonen. Samtidig som droneobservasjonene bidro til å øke erkjennelse av sikringsrisikoen, bidro det også til at de begynte å se på andre scenario. Ifølge informant 3 så medførte hendelsen [droneobservasjonene]:

> *«[...]at vi begynte å vurdere andre hendelser, og fokuserte dermed blant annet på risiko knyttet til eksportnettet» [undersjøisk rørsystem som frakter olje og gass].»*

Informantene pekte på at de i stor grad var hendelsesstyrt når det gjaldt sikring. En av informantene uttalte:

> *[...]Vi er i grunnen veldig hendelsesstyrt. Når det tidligere har vært hendelser, har det vært høyt fokus, men det har dabbet av[...]*

Dette sitatet tyder på at fravær av hendelser påvirker oppmerksomheten og bevisstheten om sikring.

5.4. Evne til å håndtere

5.4.1. De første observasjonene

Håndtering og informasjonstilgang

En viktig del av det å kunne respondere er at virksomheten vet hva man skal respondere på. Varsling og informasjonsdeling var sentralt for at operatørselskapene kunne respondere på droneobservasjonene høsten 2022, spesielt for de virksomhetene som ikke umiddelbart hadde observasjoner eller var direkte berørt av droneobservasjonene.

De første observasjonene ble gjort i juli 2022 og i begynnelsen var det begrenset informasjon om dette i det offentlige rom. Enkelte av operatørene som da ikke selv hadde hatt observasjoner fikk relativt raskt informasjon ved at dette ble delt internt mellom enkelte av operatørene. En av informantene forklarte:

> *[...]Vi hadde ikke selv noen observasjon de første ukene, men jeg fikk informasjon om dronene fra et annet selskap. Det hadde gått noe tid fra de hadde gjort sine observasjoner til de informerte meg. De hadde brukt tid på å forstå hva dette var.*

Dette ble også bekreftet av en informant som pekte på at godt samarbeid mellom operatørene bidro til informasjon og rask respons:

> *«[...]Vår respons kom veldig raskt, og det er fordi at vi fikk informasjon fra en annen operatør. Dette var godt samarbeid[...].”*

Det var ingen systematisk varsling, enkelte av operatørene fikk først vite om dette gjennom møter i sikringsnettverket eller i media. Informant 5 fikk for eksempel informasjon først gjennom sikringsnettverket eller media uker etter at første observasjon var gjort.

Observasjonene ble meldt til Petroleumstilsynet og anmeldt til politiet ettersom det kunne tyde på at de var innenfor sikkerhetssonen. Ca. 2-3 uker etter første observasjoner ble det sendt ut informasjon til alle operatørene om observasjonene gjennom sikringsnettverket i Offshore Norge. Ifølge informantene var det i tillegg også enkelte operatører som hadde en direkte dialog seg imellom. Dette gjorde at enkelte operatører fikk et tidlig varsel om at det var gjort droneobservasjoner, mens for andre måtte de vente enten på media eller få informasjon gjennom de offisielle kanalene som for eksempel sikringsnettverket.

Hemmelighold

Noe av det som informantene gav uttrykk for var at det innledningsvis ble opplevd hemmelighold knyttet til selve observasjonene. Det var vanskelig å forstå hva som faktisk skjedde, og hvordan de skulle håndtere dette. Informant 1 forklarte at:

> *«Det var gjort observasjoner hos en av operatørene, og det var veldig, veldig hemmelighetskremmeri rundt det. I begynnelsen når det var observert droner, så visste de ikke helt hva dette var, og hvorfor de var der.»*

Selv om det i intervjuene kom frem at det var stor vilje til å dele informasjon mellom operatørene, viser intervjuene at i enkelte situasjoner, og spesielt når situasjonen var uklar, ble kortene ble holdt tett mot kroppen. En av informantene forklarte at:

> *[...] Du fikk ikke fortelle det til noen. Så åpnet det seg mer og mer opp. Men likevel er det ikke den åpenheten som man hadde med COVID-19.*

Dette peker på en annen utfordring som flere av informantene tok opp og som omhandler behovet for å skjerme informasjon. Hensikten med å skjerme er ifølge informantene blant annet å skape en usikkerhet hos trusselaktøren. Operatørene ønsker å skape en usikkerhet om hvilke tiltak som er på plass og hvordan hendelser blir håndtert. Det er dermed et behov for hemmelighold av hvilke vurderinger virksomheten har gjort, og hvilke planer de har. Det blir også pekt på at spesielt sårbarheter er noe virksomhetene ønsker å skjerme. Informant 2 begrunnet behov for skjerming med usikkerhet

> *[...]Vi holdt det skjermet fordi at vi ikke visste hva det var, hvilken konsekvens det hadde på operasjonene og de som reiste ut.*

Informanten pekte her også på et behov for å unngå å skape frykt i egen organisasjon. Det brukes her også to ulike begreper, skjerming og hemmelighold. I denne sammenheng kan det tyde på at den som holder informasjon bruker begrepet skjerming, mens de som ikke får tilgang til informasjonen bruker begrepet hemmelighold.

5.4.2. Den umiddelbare responsen

En rask respons kan være avgjørende for å håndtere en uønsket hendelse. Det var varierende hvor raskt de ulike operatørene reagerte, men når de reagerte var det et relativt likt handlingsmønster.

Loggføring og rapportering

Ett av tiltakene som de fleste operatørene raskt fikk på plass var å etablere en loggføring og deretter en rapportering til myndighetene. Det ble rapportert både til politi og Petroleumstilsynet. I utgangspunktet er det kun hendelser innenfor sikkerhetssonen som skal rapporteres, men i en periode ble alt rapportert, før man etter hvert grunnet mengden kun rapporterte til politiet. En av informantene forklarte det slik:

> *[...]vi fikk jo droneobservasjonene inn. Alle droneobservasjonene som vi fikk inn, de la vi inn i en egen logg. Denne loggen delte vi med politiet[...].*

Dette ble også bekreftet fra flere av informantene. En av informantene forklarte:

> *[...]Vi har jo et eget skjema der vi har loggført alle observasjoner hos oss. Vi rapporterte jo inn til myndighetene.*

Økt sikringsnivå

Et viktig tiltak som samtlige operatører utførte var å heve sikringsnivå for sine installasjoner, samtidig ble det pekt på at det var summen av hendelser, og det generelle økte trusselnivået som medførte at operatørene økte sine sikringsnivå. Det var ikke dronetrusselen alene som førte til nivå-økning. Ved å øke sikringsnivået innførte operatørene flere og strengere tiltak. Dette kunne være økt vakthold, observasjon, redusert aktivitet osv.

> *[...]Men det var nok kombinasjonen droner og rørledningen og den økende trusselen mot infrastruktur som i sum gjorde at det ble hevet til gult beredskap. Men det var jo hvert enkelt selskap som hevet beredskapen. Det var ikke noe sånn at bransjen gjorde det. Du tok en selvstendig avgjørelse på det. Men det skulle jo mye til at du ikke gjorde det.*

Dette sitatet viser at det var summen av hendelser, og ikke bare droneobservasjon som medførte økt trussel. I tillegg kan det tyde på at tiltak som en operatør gjør påvirker hvordan andre vurderer og håndterer situasjonen. I praksis så kan det tyde på at operatørene ser til hverandre og koordinerer heving av sikringsnivå.

«Task-force»

Hos de fleste operatørene ble det etablert en egen «task-force» eller en gruppe som jobbet med håndtering av droneobservasjonene. Ifølge informant 4 var dette noe de etablerte tidlig:

> *[...]Nei, vi satt jo ned en gruppe tidlig, når det begynte å komme inn flere observasjoner. Da ble det satt ned en gruppe, som så diskuterte hvordan vi skulle gå videre og håndtere det. Gruppen skulle blant annet holde kontakt med myndighetene, vi måtte oppdatere prosedyrene våre. Vi satte sammen en flerfaglig gruppe, og involverte ulikt fagpersonell, blant annet involverte vi de som kunne dette med droner og sprengstoff.*

Informant 3 kunne fortelle om en tilsvarende organisering:

> *[...] Ved behov så oppretter vi arbeidsgrupper. F.eks. når dronehendelsen oppstod, og rørledningen ble sprengt [«Nord Stream»] så vi at dette var en større hendelse og mer omfattende enn hva vår interne sikringsgruppe kunne håndtere. Vi etablerte dermed en task-force. Den ble ledet av en fra hovedledelsen. I starten hadde vi nærmeste daglige møter, men ble etterhvert til månedlig statusmøter. Den er nå i hvilemodus.*

Samtidig kom det i intervjuene fram at de operatørene med en mindre organisasjon ikke nødvendigvis etablerte egne grupper for å håndtere hendelsen. Det ble hos disse håndtert av fag og i operasjonslinjen. En av informantene kunne fortelle:

> *[...]Vi er jo en mindre organisasjon, så vi trengte egentlig ikke det. Jeg og en sikringsrådgiver hadde flere møter, og involverte organisasjonen. Vi etablerte ikke en egen en task-force. Men vi jobbet kontinuerlig med det [...].*

Tilsvarende kunne også enkelte andre informanter fortelle om. «Task-force» gruppen var sentral i å håndtere observasjonene. Det som ble fremhevet som viktig var at det var en bred deltakelse i gruppen, både fra ansattrepresentanter, til drift og ulike fag som sikring og logistikk. Informanten trakk også fram at denne gruppen bidro til å øke forståelse av konsekvensene som kunne den økte trussel kunne medføre.

I intervjuene fremkom det også at i tillegg til at interne ressurser ble mobilisert, ble det også økt dialog med myndighetene og økt møteaktivitet i de ulike fora og nettverk som for eksempel sikringsnettverket og helikopteroperatørenes brukerforening (HBK). I HBK er også alle operatørene medlemmer, men her sitter det ulik kompetanse, alt fra sikring, til personell som

jobber med logistikk og sikkerhet. Et annet viktig element med «task-force»-gruppen var at den tverrfaglige sammensetningen bidro til å etablere en felles situasjonsforståelse, samt koordinere fellestiltak og utveksle erfaring internt i organisasjonen.

Kommunikasjon og informasjon

Deltakelse fra kommunikasjonsavdelingen viste seg å være sentralt. Det å få kommunisert raskt ut til organisasjonen var sentralt i den umiddelbare håndteringen. Den ene informanten fortalte:

> *Vi gikk ganske raskt bredt ut i organisasjonen og informerte. Vi brukte vårt "intranett", tok det med fagforeninger, deltok på møter. Fra den interne arbeidsgruppen ble det også etablert en kommunikasjonsplan. Det var viktig å ta ned bekymring fra de offshore-reisende. Det ble også laget pakker som de kunne vise familiene for å betrygge dem.*

Dette viser at operatørselskapene var raskt ute med å lage kommunikasjonspakker til ansatte på innretningene. En informant kunne fortelle at dette var noe som hadde høy prioritet og var et viktig tiltak

> *[...]For oss var det helt avgjørende å få ut informasjon tidlig, usikkerheten skapte bekymring og redsel, så det var viktig at vi tok raskt hånd om det, og fikk ut god informasjon.*

I starten var det noe bekymring fra ansatte og deres familier, men både på grunn av hvordan det ble håndtert og kommunikasjon om trusselen og tiltak, var tilbakemelding at det ikke var store bekymringer fra de ansatte.

Samarbeid og «dronegrupper»

I tillegg til en «task-force» ble det også i de største operatørselskapene etablert egne «dronegrupper» som skulle vurdere hvordan trussel skulle håndteres. Informant 2 forklarte hvordan dette ble etablert i hens virksomhet.

> *Det ble etablert en gruppe internt i organisasjonen som skulle jobbe med droneproblematikken, og vurdere ulike løsninger. Det ble også etablert et samarbeid mellom flere operatører om dette. Ettersom trusselen gikk ned, har arbeidet i hovedsak*

foregått hos de ulike operatørene. Vi samarbeidet med tre andre operatører som også hadde etablert en slik arbeidsgruppe. Denne gruppen skulle også se på regelverket.

Det ble dermed også raskt etablert et samarbeid mellom de ulike operatørselskapene, hvor erfaringer ble delt. En utfordring var mengden av selskaper som kunne tilby løsninger for å detektere droner. Det var også en utfordring i å finne løsninger som faktisk virket i miljøet det skulle virke i offshore. Ved å samarbeide kunne næringen lettere etablere beslutningsgrunnlag. Det var spesielt utfordringer knyttet til regelverket og avklaringer av hva man faktisk hadde muligheter til innfor innretningens sikkerhetssone (et område rundt innretningen som strekker seg 500 meter ut fra innretningen hvor fartøy ikke har lov til ferdes uten tillatelse fra plattformsjefen).

Beredskapsorganisasjon og kompetanse

I intervjuene kom det fram at hendelsene ble håndtert av beredskapsorganisasjonen både offshore, som er førstelinje, og beredskapsorganisasjonen på land. En av informantene forklarte at:

«[...]ved konkrete droneobservasjoner var det beredskapsorganisasjonen som trådde inn for å håndtere konkrete situasjoner der og da. Men de lente seg på råd og støtte fra task-force gruppen, som hadde et veldig godt og sømløst samarbeid».

Det samme kunne bekreftes av en annen informant som også var tydelig på at håndtering av sikringshendelser er del av beredskapen.

[...]Det er beredskapsorganisasjonen som skal håndtere sikringshendelser. Vi har inkludert sikringshendelser som del av beredskapen, det vil si det som omhandler den reaktive fasen[...]

Dette var også noe som var felles for flere av operatørene. Det er krav i petroleumsregelverket om at operatørselskapene skal kunne håndtere definerte fare- og ulykkeshendelser. Dette betyr at alle operatører dermed har en beredskapsorganisasjon på plass. I de fleste virksomhetene ble observasjonene varslet og håndtert gjennom beredskapsorganisasjonen. Når respondentene ble spurt om hva dette kunne bety for håndtering av hendelsen, var de tydelige på at dette er viktig for å lykkes med håndtering, det er heller ingen reelle alternativer til håndtering. De pekte på at den erfaring og metodikk som

beredskapsorganisasjonen har tilegnet seg over tid gjør at organisasjonen i større grad evner å håndtere utforutsette hendelser. I det ene intervjuet fremkom det at:

> *«[...]det har vært helt avgjørende å ha med erfarne medarbeidere for å håndtere denne situasjonen[...]»*

Vedkommende pekte da både mot beredskapsorganisasjonen og deltakere i «task-force»-gruppen.

Selv om informantene pekte på at virksomhetene evnet å håndtere hendelsen, pekte de samtidig på at hendelsen viste at det var stor usikkerhet og manglende kompetanse på håndtering av sikringshendelser. Informant 5 opplevde det som handlingslammelse i sin virksomhet, hvor hen forklarte at:

> *[...]Innenfor safety-hendelser har vi som operatør ansvar for å håndtere hendelsene. Jeg opplever at i denne type hendelser, sikringshendelser, hvor myndighetene har et ansvar, så blir det handlingslammelse og usikkerhet i organisasjonen.*

En annen informant pekte i tillegg til manglende kompetanse, også på manglende operativ forståelse i organisasjonen. Dette var relatert til manglende erfaring med å håndtere sikringshendelser, og at dette ikke var noe de i tilstrekkelig grad hadde prioritert å bruke tid på.

> *[...]Det har også vært en utfordring å få riktig kompetanse me hensyn til sikring inn i organisasjonen. Flere mangler den operative forståelse, men det betyr ikke at de ikke er flinke. Vi har en vei å gå[...].*

Sitatene kan tyde på at informantene har en oppfatning av at deres virksomhet ikke har prioritert å bygge tilstrekkelig sikringskompetanse over tid.

Funn fra intervju så langt viser at respondentene mente de hadde en rask respons, de pekte på at rapportering både internt og mot myndighetene var viktig. Internt ble det etablert en «task-force» for koordinering og håndtering. I tillegg ble etablerte interne og eksterne nettverk brukt, samt det ble etablert samarbeid i næringen. I tillegg pekte de på at selve observasjonen ble håndtert av beredskapsorganisasjonen.

Normalisering og avslutning av håndtering

Noe av det informantene ikke var så tydelig på, var avslutning av håndteringen. Å vite når situasjonen normaliseres er viktig for å unngå å bruke opp ressursene.

Droneobservasjonene som isolerte hendelser og observasjoner hadde en tydelig start og slutt, men utfordringen var å få en forståelse av når trusselen var redusert. Samtidig var det en erkjennelse hos informantene om at denne type trusler og trusselnivået var den nye normalen.

Observasjon av dronene foregikk over flere måneder, og avtok senhøsten 2022. Informasjonen fra respondentene tydet på at det var en glidende normalisering. Møtefrekvens ble redusert, fra daglig, til ukentlig, til månedlig. Etter hvert ble «task-force»-gruppen satt i hvilemodus. Det kunne dermed tyde på at mangel på observasjoner gjorde at operatørene gikk over i en normaliseringsfase, og at det ikke var en tydelig avslutning på håndteringen. I et av intervjuene kunne respondenten fortelle at de først nå [vår 2023] var inne i en normaliseringsfase hvor de var i ferd med å legge ned «task-force»-gruppen, og overføre studier til driftsorganisasjonen.

5.4.3. Kapasitet og ledelsesfokus

Hollnagel peker på at et av elementene som må være på plass for å kunne respondere på hendelsen er ressurser (Hollnagel, 2018, s. 30). Ressursbehov har sammenheng med den situasjonen man står ovenfor, men basert på informantenes tilbakemelding var det en meget krevende situasjon.

Antall observasjoner og hendelser varierte, men i all hovedsak var de fleste observasjonene tilknyttet feltene i Nordsjøen. I tillegg var det operatørene med flest innretninger som fikk flest observasjoner. Informantene kunne fortelle at det etter hvert ble en betydelig mengde observasjoner. Selv om mange av observasjonene i ettertid viste seg å være observasjoner av fly, lys eller stjerner, så opplevde informantene at det etter hvert ble en uhåndterlig mengde observasjoner. I tillegg var de også tydelige på at de ikke er dimensjonert for å håndtere denne type hendelser som skyldes en statlig aktør. En av informantene uttrykte det på denne måten:

> *[...]Da er vi litt tilbake til at vi ikke er dimensjonert til å selv håndtere denne type hendelser. Det vi kan gjøre er å observere, melde ifra, innføre de tiltakene vi selv kan gjøre for å begrense en risiko, og eventuelt sikre eget personell.*

Informanten uttrykte videre at å håndtere hendelsen egentlig ikke var noe problem. Grunnen til dette var nettopp at de ikke var, og heller ikke skulle være dimensjonert for å håndtere denne type hendelser. Når informantene ble spurt som de opplevde at de hadde tilstrekkelig ressurser til å håndtere situasjonen tenderte svarene mot at de opplevde manglende ressurser, noe som skyldes manglende prioritering over flere år.

[...]Nei, det er veldig lite robusthet i det hele tatt. I utgangspunktet før Ukraina var vi ganske skviste på ressurser, og etter Ukraina var det åpenbart at vi ikke har innsett fremtidens behov[...].

Det var samtidig en erkjennelse av at: «[...]kapasitet vil alltid være en utfordring[...]».

Samtidig kunne flere informere om at etter observasjonene begynte, så *[...]skulle det ikke stå på ressurser, det fikk vi tilgang til[...]»*. Dette var ikke ensbetydende med at det var ubegrenset bruk av ressurser, men oppmerksomhet og prioritering endret seg.

Ressursbehov har en sammenheng med ledelsens prioritering, og flere av informantene pekte på at sikring ikke var noe som hadde hatt høy prioritering. En av informantene pekte på at:

«[...]Vår ledelse er nødvendigvis ikke de som er veldig flinke til å tenke på sikring».

Informanten pekte på at manglende kompetanse hos ledelsen kunne være en årsak til dette.

Oppmerksomheten fra myndighetene og en økt forståelse og erkjennelse av trusselen, bidro ifølge informantene til at bevissthet og prioritering endret seg. Det ble en tettere oppfølgning og mer involvering fra ledelsen, med krav om hyppigere rapportering.

Etter at mengden observasjoner økte, ble det vurdert at dette var mer enn virksomhetene kunne håndtere alene. En av informantene utrykte at dette var mer enn de hadde kapasitet til. Det ble deretter tatt et initiativ til å eskalere dette mot myndighetene, og det ble gjennomført et møte med relevante departement, og andre næringslivsorganisasjoner som Næringslivets Sikkerhetsråd, Rederiforbundet med mer. I møtet ble det fra petroleumsnæringen gjort tydelig at de nå var avhengige av at myndighetene kom på banen. Ifølge en av informantene kom myndighetene mye sterkere på banen etter dette møtet. Det ble vist til økt tilstedeværelse av militære skip og fly offshore, statsministerens besøk offshore, og plassering av sensorer på enkelte innretninger.

5.4.4. Var operatørene forberedt?

Et av spørsmålene som ble stilt informantene var om de var forberedt på denne hendelsen.

Dette kunne si noe om deres evne til å forutse, i tillegg til evnen til å respondere. Dette punktet er dermed relevant både for håndtering og evne til å forutse. Selv om respondentene kunne fortelle om en rask respons, var det også en oppfatning av at de ikke var forberedt på hendelsen.

Informant 5. var veldig tydelig på hvorvidt de var forberedt på hendelsen.

[...]Nei, vi var ikke så godt forberedt. Vi så ikke den komme[...].

Droner brukt i denne type offensive operasjoner eller som del av hybrid krigføring var heller ikke noe informantene hadde tatt tilstrekkelig høyde for. En informant forklarte:

«Når det gjelder droner, så var det jo en trussel vi ikke egentlig hadde identifisert.».

Videre kunne informant 3 forklare at:

[...]Vi var ikke forberedt. Hva skulle vi gjøre hvis dronene landet på innretningen. Det sa ikke vår sikringsplan noe om, da måtte vi oppdatere planverket[...]

Beredskapsplaner og sikringsplaner er verktøy som bidrar til å sikre en god og planlagt respons, og tilrettelegger samtidig for at virksomhetene skal kunne trene og øve. Samtlige operatører har etablert både beredskapsplaner og sikringsplaner, slik de er pålagt gjennom petroleumsregelverket. Ifølge informantene var dette sterkt medvirkende til at håndteringen allikevel gikk så bra som det gikk.

Drone-trussel var ikke ukjent for operatørene, og selv om enkelte av operatørene hadde identifisert drone som et scenario, var dette mer rettet mot aktivisters bruk av droner (miljøvernaksjoner). En av informantene forklarte at:

[...]man hadde jo tiltakskort for dronene. Men det var mer med tanke på miljøvernorganisasjoner.

Flertallet av informantene kunne stille seg bak svaret til en av informantene når hen ble spurt om hva de hadde på plass, hen svarte:

«Ingenting, vi hadde ikke tiltakskort på plass.»

Utvikling av nytt tiltakskort for droner var derfor et av de umiddelbare tiltakene som flere iverksatte. Informantene kunne fortelle at tiltakskortet ble delt i sikringsnettverket, slik at de som ikke hadde fått det etablert, raskt fikk det på plass. Etter hvert bidro også politiet med innspill til tiltakskortene, spesielt med hensyn til rapportering og håndtering av droner som for eksempel kunne ha landet ulovlig på innretningen. Samarbeid og informasjonsdeling var dermed essensielt for å kunne forbedre operatørene sin respons, noe som sitat fra informant 2 underbygger:

[...]Jeg synes vi kom oss relativt greit opp, men mye av årsaken til at vi var raskt oppe var at vi fikk informasjon fra et annet operatørselskap om observasjonene. I tillegg fikk vi oversendt et utkast til tiltakskort. Vi var ikke på bar bakke, men kunne dermed starte på et annet nivå.

5.5. Evne til læring

5.5.1. Læring - Trening og øvelse

Flere av informantene trakk fram at de opplevde at de hadde lært mye på organisatorisk nivå etter håndtering av COVID-19. Dette var også en omfattende hendelse, som de ikke var forberedt på å håndtere. Spesielt arbeidet med «task-force», tverrfaglig involvering, og informasjonsdeling i organisasjonen var relevante områder de hadde tatt med seg nyttig erfaring fra. Dette bidro til en bedre og mer effektiv håndtering av dronene. I tillegg påpekte de at den etablerte beredskapsorganisasjonen, som har mye erfaring og trening, var viktig for håndteringen.

Det var også en erkjennelse av at det var for lite trening og kompetanse på sikring. Et av tiltakene som ble iverksatt av flere av informantene var umiddelbart å øke trening på sikringsscenario, og flere gjennomførte «table-top»/skrivebordsøvelser. I tillegg økte man mengden informasjon om sikring ut til organisasjonen slik at både bevissthet og kompetanse økte.

I intervjuene kom det også fram at de operatørene som hadde flere observasjoner ble bedre over tid, de hadde lært både av det de hadde gjort riktig og det de kunne gjøre bedre. De som ikke hadde observasjoner eller få observasjoner trakk fram samarbeid og deling av informasjon blant annet gjennom sikringsnettverket som avgjørende for å lære av andre.

5.5.1. Samarbeid

Ifølge informantene var det etablerte sikringsnettverket helt sentralt for å sikre en rask og koordinert respons. Det bidro også til deling av læring. Dette punktet er også relevant for både respons og evne til å forutse.

Informant 1 forklarte at det i august ble kalt inn til et ekstraordinært møte i sikringsnettverket, hvor hensikten var at de som hadde gjort observasjoner kunne dele informasjon om dette. I tillegg ble politi og forsvar koblet inn, men på det tidspunktet var tilbakemelding at operatørene foreløpig bare skulle rapportere inn observasjonene.

Nettverket var også avgjørende for å dele informasjon og erfaring mellom operatørene. En av utfordringene nettverket løste, var at det tilrettela for å dele sensitiv informasjon. Flere av informantene er tydelige på at de ikke er konkurrenter når det gjelder sikring, men det betyr ikke at informasjon deles ukritisk, og at selskapene ikke skjermer kritiske sårbarheter, men erfaringer, interne rapporter, metoder og vurderinger deles. Sitat fra informant 3 illustrerer dette:

> *[...] I Offshore Norge, sikringsnettverket, så ble dronetrusselen diskutert. Der er det lite hemmeligheter mellom oss. Delingsviljen er stor mellom selskapene, både når det gjelder observasjoner, når det gjelder tiltakskort, og når det gjelder prosedyrer[...]*

Informanten pekte videre på nettverket hadde vært aktivt, og at både NSM, PST og Ptil deltok i disse møtene. Flere av informantene pekte på at deltakelse fra myndighetene i nettverket var viktig. Dette bidro til å etablere nødvendig tillitt og bygge relasjon slik at det i situasjoner som dette kan deles informasjon fritt. Tilbakemelding var også at terskelen for å ta kontakt med myndighetene var lavere. Sitat fra en annen informant underbygger også betydningen av nettverket

> *[...]Sikringsnettverket er avgjørende for håndtering av hendelser som dette, vi får veldig mye gratis gjennom dette nettverket. Jeg opplever at vi deler veldig åpent Jeg har fått tilbakemelding om at dette er ekstra viktig for de mindre operatørene, som ikke har samme ressurser som de største.*

Informantene kunne også fortelle at det ikke bare er informasjon som blir delt, men det ble også gjennomført koordinering av hvilke tiltak som skulle implementeres på helikopterbase og forsyningsbase. Det er viktig å merke seg at tiltakene hos de ulike operatørene ikke er førende. De representerer snarere en erfaringsoverføring og viser hvordan situasjonen ble håndtert internt hos hver enkelt operatør. Et sitat fra informant 4 underbygger betydningen av nettverket:

> *[...]I tillegg har nettverk og kontakt med myndighetene var utrolig viktig for å få til en god respons, samt få tilgang til informasjon[...]*

Funn fra intervjuene tyder dermed på at det etablerte sikringsnettverket har vært sentralt i både å dele informasjon, men også koordinere tiltak og dele erfaring. Dette har bidratt til å etablere bedre situasjonsforståelse og økt evne til respons.

5.5.2. Læring fra COVID-19

Ifølge informantene hadde de fleste operatørene fersk erfaring med å håndtere en uventet hendelse. I forbindelse med håndtering av COVID-19 hadde de fleste etablerte en «task-force» eller en gruppe som håndterte hendelsen. Dette var noe operatørene bygde videre på. En av informantene forklarte:

> *[...]Vi hadde jo nettopp avviklet task-force for COVID-19. Og vi var vant til å jobbe tverrfaglig med å håndtere en global utfordring som vil treffe vår næring. Så det vi gjorde ganske tidlig når dronetrussel oppstod var at vi satte ned en tverrfaglig task-force. Alt fra logistikk til sikringsfolk til operasjon. Vi hadde også vernetjenesten og HR og tillitsvalgte.*

En annen informant kunne fortelle at de hadde en «task-force» som var etablert før dronehendelsen oppstod.

> *[...] Vi hadde allerede en task-force på plass, som var ledet av meg fra security. En task-force ble opprettet rett før invasjonen, i forhold til å håndtere blant annet sanksjoner og eksponering, supply chain issues og selvsagt security issues. Den task-forcen ble også involvert i forhold til å håndtere dronetrussel.*

Informanten var også tydelig på at en slik tverrfaglig gruppe var avgjørende for hvordan dette ble håndtert av virksomheten.

> *[...] Det å ha et tverrfaglig team, som møttes omtrent daglig til tider, eller i hvert fall ukentlig og ad hoc ved behov, det var ekstremt viktig. Det var et suksesskriterium som støttet beredskapsorganisasjonen og driftsorganisasjonen for å håndtere dette[...]*

Dette kunne tyde på at operatørene hadde tatt med seg læringspunkter fra håndtering av COVID-19, og overført og tilpasset dette til en tilsvarende situasjon, men hvor konteksten var annerledes.

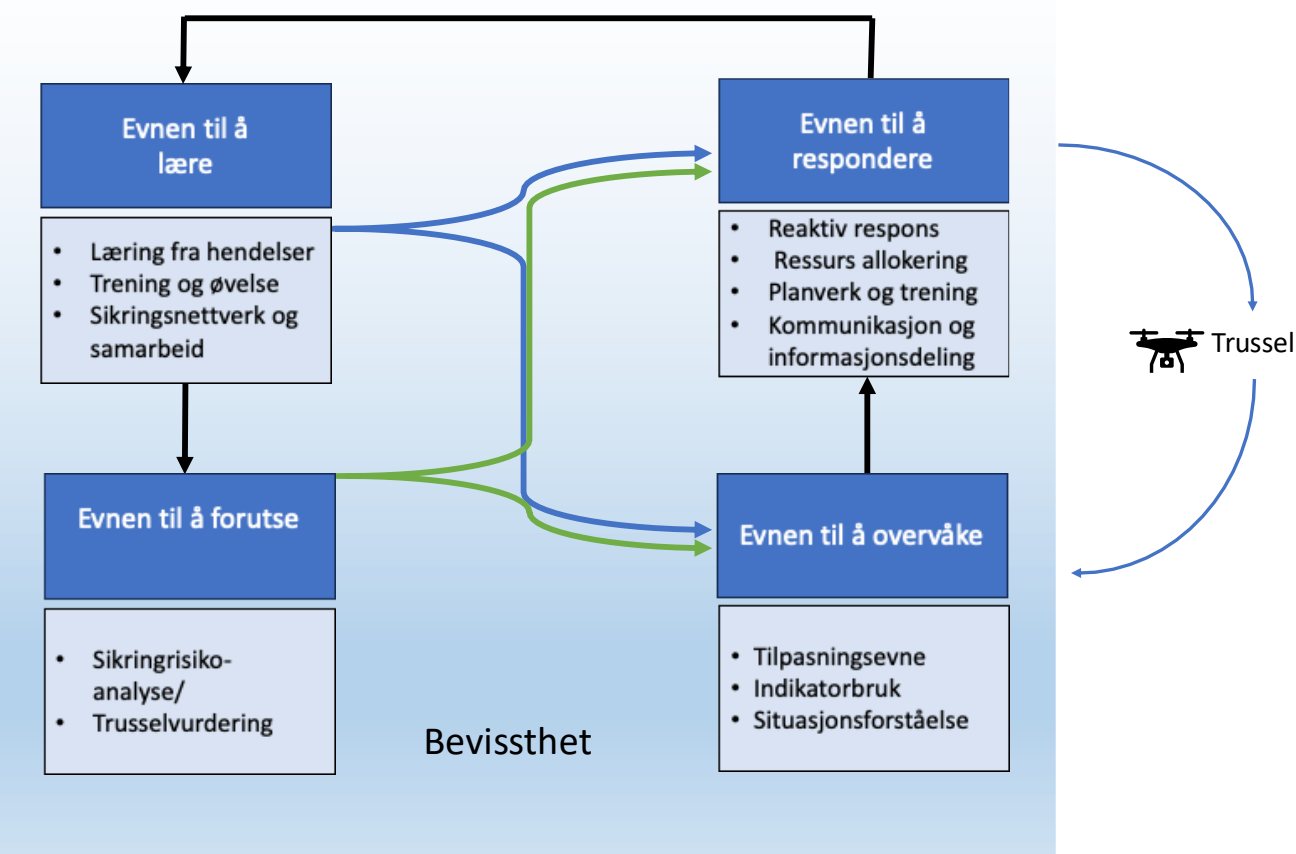
6. Diskusjon

I dette kapittel skal jeg drøfte funn fra intervju i forhold til teori, for å komme fram til et svar på studiens problemstilling:

> *Hvordan har operatørene operasjonalisert prinsippene fra «resilience engineering» i forbindelse med håndtering av dronetrusselen høsten 2022.*

I lys av den tiltagende dronetrusselen høsten 2022, stod operatørene overfor nødvendigheten av å ha robuste og fleksible strategier for å ivareta sikringen. «Resilience engineering» (RE) tilbyr et rammeverk for å gjøre noe med slike utfordringer, ved å fokusere på organisasjonens evne til å tilpasse seg endringer, møte uventede hendelser og lære fra dem. For å forstå hvordan disse prinsippene har blitt operasjonalisert i møte med dronetrusselen, vil jeg i denne delen diskutere den praktiske gjennomføring opp mot teorien. Analysen vil ikke bare vise hvordan prinsippene ble satt ut i livet, men også kaste lys over de primære utfordringene og faktorene som operatørene stod overfor ved håndtering av droneobservasjonene.

Diskusjonen er organisert rundt de fire egenskapene forutse, overvåke, respondere og lære. Basert på den tematiske analysen, samt funn fra empiri er det identifisert ulike forhold som påvirker disse egenskapene. I figuren under er de ulike egenskapene og underkategoriene oppsummert. Dette danner grunnlag for diskusjon. I tillegg vil jeg innledningsvis kort diskutere hvor bevisst forhold operatørene har til «resilience». I figuren er bevissthet noe som ligger som et bakteppe for å nå potensialet til disse «evnene». Illustrasjonen er basert på Hollnagel sin modell som viser sammenheng mellom de ulike evnene (se figur 9 s.22). Jeg har byttet ut «the enviroment» med trussel som i denne kontekst er omgivelsene som påvirker og blir påvirket av evnen til å overvåke og respondere.



Figur 11 Egenskapene som bidrar til "resilience"

6.1. Bevissthet

I denne delen skal jeg diskutere temaet bevissthet som den tematiske analysen avdekket. Denne diskusjonen bidrar til å belyse graden av bevisst og systematisk arbeid med «resilience» blant operatørene.

Hollnagel argumenterer for at en organisasjon bør ha en bevissthet om «resilience» og egenskapene som er nødvendige for å bygge «resilience» (Hollnagel, 2011a). Dette påvirker graden av målrettet innsats organisasjonen legger i arbeidet med å utvikle «resilience»

Intervjuene avslører varierende grader av bevissthet og begrepsbruk blant informantene. Når informantene ble spurt om hva de legger i begrepet «resilience» og i hvilken grad de jobber bevisst med dette var det flere som brukte begrepet robust og viste til at med «resilience» forstod de en robust beredskapsorganisasjon. De viste til en organisasjon som har kompetanse og tilstrekkelig ressurser. Dette underbygges også av Hollnagel (Hollnagel, 2018, s. 17). I

tillegg var det også enkelte som viste til at man innen cyberdomenet[3] (i motsetning til det fysiske domene) var flinkere til å tenke «resilience» eller robusthet. Samtidig ble det også pekt på at sikring inngår i en helhet og at sikring er del av beredskapen. Selv om informantene ikke bevisst bygde «resilience» innen sikringsfaget, inkluderte de dette som en del av en helhetlig tankegang. Funnene indikerer at hovedfokus er å etablere motstandsdyktighet snarere enn å komme styrket ut av en hendelse. Dette vil kunne påvirke for eksempel hvordan de tilnærmer seg læring.

Hovedinntrykket viser at operatørene i liten grad er bevisste på hvordan de skal bygge «resilience», selv om dette er en del av aktivitetene de utfører innen beredskap. Samtidig som Hollnagel peker på at man bør ha en bevissthet om «resilience», trekker han også fram at i praksis vil ikke organisasjonen måle dette, men «resilience» kan være summen av alle de aktivitetene som gjennomføres (Hollnagel, 2011a). Selv om funnene ikke viser en tydelig tilnærming til «resilience», betyr det ikke at informantene nødvendigvis unnlater å utføre aktiviteter som styrker «resilience», noe som vil fremkomme i den videre diskusjon.

6.2. Evne til å forutse

I den tematiske analysen hvor jeg tok utgangspunkt i hovedkategori «evne til å forutse» var det i all hovedsak ett tema som skilte seg ut og det var bruk av sikringsrisikovurdering og trusselvurdering. Jeg vil diskutere dette opp mot den valgte teori.

Trusselvurdering og sikringsrisikovurdering

Ifølge Hollnagel er formålet med å forutse ikke bare å støtte pågående aktiviteter (overvåke), men også å vurdere alternative fremtidige scenarier (Hollnagel, 2018, s. 43). Hensikten er blant annet å identifisere irregulære trusler, i motsetning til overvåkning som har fokus på regulære trusler (Hollnagel et al., 2009, s. 126).

Intervjuene avdekket at operatørene i stor grad bruker trussel- og sikringsrisikovurderinger (SRA), heretter referert til som 'analysene', som overvåkingsverktøy. Risikovurdering er ifølge Hollnagel aktiviteter som hjelper oss med å se inn i fremtiden. Forutsetningen er at systemet som overvåkes er «tractable», det vil si at problemer kan løses ved hjelp av lineære

[3] Med domene forstås et fagområde eller et spesifikt miljø der hendelser finner sted for eksempel cybersikring – det digitale verden, fysisksikring – den fysiske verden, personellsikring viser for eksempel de menneskelige aspektene ved sikring.

tilnærminger (Hollnagel, 2018, s. 43). «Systemet» operatørene opererer i kan derimot beskrives som «intractable». Dermed er ikke risikoanalyse et egnet verktøy ifølge Hollnagel. I intervjuene fremkom det også at denne type vurderinger ofte var basert på tidligere erfaring og hendelser. Utfordringen med dette er at denne type data og tilnærming er lite egnet til å forutse framtidige hendelser (Patriarca, Di Gravio, et al., 2018, s. 267; Stavland & Bruvoll, 2019, s. 15). Samtidig argumenterer Aven for at en vesentlig hensikt med risikoanalyser er å forstå risiko, og at de dermed bidrar til risikoforinformerte beslutninger (Aven, 2022, s. 7). Funnene antyder at operatørenes vektlegging av analysene ikke er gunstige for å forutse fremtidige scenarier.

Når Hollnagel peker på «intractable» systemer og viser til kompleksiteten, er det nettopp dette en trusselaktør kan utnytte. En aktør som har evne til å bevisst utnytte «ytelsesvariasjon» og kompleksitet kan være noe som skiller sikring fra sikkerhet. Det er nettopp mangel på mulighet til å overvåke disse variasjonene Leveson kritiserer RE for (Leveson, 2020, s. 100–102). Analysene kan bidra til å identifisere og overvåke disse variasjonene, for eksempel sårbarheter. Det er også variasjon i bruk av droneteknologi som kan utnyttes av trusselaktøren (størrelse, fart, teknologi til å styre den, GPS). Analysene kan dermed allikevel være sentrale verktøy for å identifisere ledende indikatorer, samt fremtidige scenario.

Informantene pekte på manglende dynamikk i analysene som en utfordring. Etter at analysene var utført var de utdatert og i liten grad oppdatert. Dette er også relevant for evnen til å overvåke trusselbildet. Utfordringen er her mangel på oppdatert trusselbilde, noe som er en hensikt med å overvåke (Hollnagel, 2018, s. 44).

En annen utfordring er valget av risikoperspektiv som analysene baserer seg på; det tradisjonelle (sannsynlighet x konsekvens) eller det kunnskapsbaserte, hvor usikkerhet i større grad ble vektlagt. Enkelte av informantene pekte på at en tradisjonell tilnærming ble lagt til grunn. Det er denne tilnærmingen og dette risikoperspektivet (SxX=risiko, hvor grunnlag er historiske data) Hollnagel legger til grunn når han sier at risikoanalyse ikke er egnet til å forutse komplekse situasjoner som er omhandlet i denne studien (Hollnagel, 2011a, s. 286).

Samtidig var det flere informanter som pekte på at de hadde tatt i bruk en mer «moderne» tilnærming til vurdering av sikringsrisiko, blant annet basert på standarden NS5814:2021 (se teori for utdypende informasjon om risikoperspektiv). Denne legger til grunn et perspektiv som blant annet er i tråd med det som Steen og Aven presenterer. De argumenterer for at dette perspektivet i større grad er forenlig med «resilience». De beskriver dette som A, C, U, hvor hendelse A, konsekvens C, og tilhørende usikkerhet U, gir en bedre forståelse av risikoen

(Steen & Aven, 2011). Det er den kvalitative, kunnskapsbaserte tilnærmingen som bidrar til at man i analysen kan konsentrere seg om konsekvensen av framtidige hendelser, og dermed bidrar til «resilience» (Stavland & Bruvoll, 2019, s. 16). En slik forståelse av risiko skiller seg fra det Hollnagel legger til grunn for sin argumentasjon, og det kan dermed indikere at sikringsrisikoanalysen kan bidra til å styrke evnen til å forutse.

Informantene trakk fram at flere av dem nå jobbet med en mer dynamisk tilnærming til analysene, hvor de i mye større grad skulle ta i bruk teknologi. Her oppstår en sammenheng mellom teknologi og menneskelig faktor, noe som også er en vesentlig del av et sosioteknisk system. Hollnagel peker på at i en slik kobling er det viktig å forstå samhandlingen, som kan ha uventede koblinger. I dette tilfellet kan det tyde på at operatørene nettopp tar i bruk teknologi for å styrke evnen til å forutse (Hollnagel, 2011a). Selv om innføring av teknologi i seg selv kan øke kompleksiteten, viser det også en evne til tilpasning og læring.

Oppsummering

I denne delen har jeg diskutert hvordan operatørene har operasjonalisert evnen til å overvåke ved bruk av trusselvurdering og SRA. Til tross for at analysene er nyttige til overvåkning, viser studien at de ikke nødvendigvis egner seg optimalt for forutsigelse av fremtidige scenarioer siden de hovedsakelig baserer seg på tidligere erfaringer. Analysene har dessuten vist seg å mangle dynamikk, og det har vært en tendens til å stole for mye på tradisjonelle, sannsynlighetsbaserte risikovurderingsmetoder. Enkelte informanter anerkjente behovet for en mer moderne, dynamisk tilnærming som i større grad vektlegger usikkerhet og mulige konsekvenser. For å forbedre forutsigelsesevnen arbeider mange med teknologiintegrasjon for en mer dynamisk tilnærming. Dette fremhever nødvendigheten av å forstå samspillet mellom teknologi og mennesker innen sosiotekniske systemer.

6.3. Evne til å overvåke

Empiriske funn og tematisk analyse identifiserer tre nøkkeltemaer som grunnlag for operatørenes overvåkningspraksis. Disse er «tilpasningsevne», «indikatorbruk» og «situasjonsforståelse». I denne delen vil dette bli diskutert.

Tilpasningsevne

Evnen til å overvåke omfatter både å ha kontroll over hendelser i omgivelsene, trusselbildet og interne forhold i organisasjonen. Ifølge Hollnagel handler dette også om å være oppmerksom på potensielle trusler som kan oppstå i fremtiden (Hollnagel, 2011a, s. xxxvii).

Informantene fortalte at overvåkning var basert på myndighetens råd og vurderinger, media og bruk av eksterne firma. Operatørene manglet egne offshore sensorer, som radar, for drone-deteksjon. Dette tyder på at de gjennomfører en overvåkning, men at de i hovedsak har søkelys på overvåkning av det eksterne trusselbildet, og at de i hovedsak baserer overvåkning på eksterne kilder. Ved å legge for mye vekt på eksterne kilder, noe som informasjon fra informantene kan tyde på, kan dette begrense systemets evne til tidlig deteksjon og føre til en forsinket respons (Hollnagel, 2011a).

For sikringshendelser er trussel en vesentlig driver for risiko (Smith & Brooks, 2013, s. 64). Dette skiller sikring fra sikkerhetshendelser (Jore, 2019). Hollnagel peker også på at eksterne drivere er noe av det som fører til endring i for eksempel risikobildet (Hollnagel et al., 2006, s. 19). Overvåkning av trusselbildet kan dermed være viktig for å fange opp endringer.

For å kunne overvåke er det nødvendig at virksomheten har tilstrekkelig evne og ressurser til å gjennomføre dette (Hollnagel et al., 2009, s. 123–124). Empiri tyder på at overvåkning i stor grad baseres på eksterne kilder. Dette kan være en indikasjon på at operatørene har mangler i både kapasitet og evne til å gjennomføre egen overvåkning. Det kom frem i intervju at operatørene vurderte ulike løsninger for overvåkning med radar offshore. I tillegg, for overvåkning av trusselbildet pekte de på et (data)system som i større grad fanget opp dynamikken og de raske endringene i trusselbildet, samt i større grad kunne identifisere trender og utvikling. Dette kan signalisere at de har erkjent mangler i kapasitet og evne. Det kan også indikere en svekkelse i evnen til å overvåke. Dette demonstrerer også en bevissthet om egne svakheter, essensielt for læring og forbedring.

En vektlegging av eksterne kilder kan tyde på en reaktiv tilnærming, der man avventer rapporter om tidligere hendelser i stedet for å aktivt overvåke situasjonen selv. I følge Hollnagel er en reaktiv tilnærming utilstrekkelig, og overvåkning må være proaktiv. Overvåkning bør identifisere mulige fremtidige «avvik» før de utvikler seg til en utfordring (Hollnagel, 2018, s. 31, 98). Samtidig peker han også på at overvåkning kan være reaktiv og trigges av kontinuerlig overvåkning av indikatorer (Hollnagel, 2011a, s. 84). Dette betyr for eksempel at overvåkning kan intensiveres, noe som også operatørene gjorde. Når observasjoner ble gjort, intensiverte operatørene overvåkningen. Personell offshore ble bedt om å fysisk se etter droner, og de søkte

også mer aktivt etter informasjon om trusselbildet. Hollnagel peker på at bruk av menneskelige sensorer kan være nødvendig ved fysiske hendelser (som droner) (Hollnagel, 2018, s. 34). Dette kan dermed bety at selv om de har en reaktiv tilnærming til overvåkning, noe som kan svekke overvåkning, har de samtidig vist en evne til å tilpasse og intensivere overvåkning ved behov. Dette kan videre tyde på en adaptiv evne, noe som bidrar til «resilience» (Hollnagel, 2018, s. 59). Hollnagel peker også på at evnen til å overvåke må være fleksibel, og tilpasses slik at den ikke begrenses av rutiner og vaner (Hollnagel et al., 2009, s. 124). Funnene indikerer at operatørene har demonstrert fleksibilitet og tilpasningsevne.

Indikatorbruk

Hollnagel peker på at bruk av indikatorer er sentralt i å overvåke et systems ytelse, og kan samtidig si noe om en framtidig situasjon eller utvikling (Hollnagel, 2018, s. 35–36). Intervjuene indikerer en begrenset bruk og bevissthet om indikatorer for måling av ytelse innenfor sikringsfunksjon. I all hovedsak ble det henvist til at bruk av indikatorer var relatert til trusselvurdering. Hendelser, intensjoner og aktørens vilje ble fremhevet som typiske indikatorer. En slik tilnærming støttes blant annet av forskningen til Schuurman og Eijkman som peker at dette er sentrale elementer for å forstå trusselbildet (Schuurman & Eijkman, 2015). Dette kan forstås som framoverskuende indikatorer og kan dermed gi et varsel om en utvikling av trusselbildet. En slik forståelse av indikatorer, brukt i en trusselvurdering, kan også tyde på at trusselvurdering dermed kan ha en effekt på å forutse.

Et sitat viser samtidig at selv om indikatorene var der, så greide ikke denne operatøren å forstå eller gjøre bruk av dem:

> *[...] Droner har jo vært brukt i Ukraina-krigen. Hvorfor greide vi ikke å forutse bruk av droner, indikatorene var der med vi greide ikke å bruke dem.*

Utvikling og bruk av indikatorer er ifølge Klaus Thomas med flere et nøkkelelement ved RE, nettopp ved at de gir innsikt i en tilstand eller trend (Thoma et al., 2016, s. 15). Mangel på bruk av (ledende) indikatorer kan dermed redusere evnen til å overvåke (Hollnagel, 2018, s. 31).

Få hendelser innen sikring kan være en årsak til den begrensede bruken av indikatorer. I følge Hollnagel vil virksomheter som opplever å ha fravær av hendelser, eller liten endring i omgivelsene, heller ikke ha samme behov for overvåkning som en virksomhet med mange hendelser (Hollnagel, 2018, s. 33). Det kan også forklare mangel på bruk av indikatorer.

Intervjuene indikerte også en økning i overvåkningen, med informantene som rapporterte om en mer aktiv bruk av trusselindikatorer ved flere observasjoner.

Situasjonsforståelse

En viktig egenskap ved å overvåke er ifølge Patriarca med flere «[...] *understanding actual threats timely and precisely.[...]*», og omtales her som situasjonsforståelse (Patriarca, Di Gravio, et al., 2018, s. 267). Empiriske data antyder at operatørene slet med å etablere en forståelse av situasjonen. De pekte på usikkerhet knyttet til hva de stod ovenfor. De forsto ikke umiddelbart hvilken trussel de stod ovenfor og hva som var trusselaktørens hensikt. Et hybrid trusselbilde kan være en årsak til at det er vanskelig å etablere en situasjonsforståelse. Patrick Cullen, beskriver dette som et «wicked-problem». Et problem som er vanskelig å løse fordi det er ukomplett, mangler informasjon, og stadig endring gjør det vanskelig å gjenkjenne. En utfordring er nettopp at det er statlige aktører som står bak (Cullen, 2018, s. 2). Noe også informantene påpekte *«[...]Vi så primært på det som en strategisk kommunikasjon mellom nasjonalstater der vi egentlig ikke var en part»*. Informantene pekte også på at det var en *«begrenset fenomenforståelse»* både hos operatørene og myndighetene. Dette er også noe som politiet selv bekreftet i et intervju: *«[...]Jeg tolker det som at det var usikkerhet knyttet til hvordan man skulle håndtere dette. Både hos operatørselskapene og i politiet[...]»* (Stormark, 2023a). Dette kan være årsak til for eksempel reaktiv respons og manglende forståelse av trusselindikatorer. Funn kan så langt tyde på at kompleksiteten i trusselbildet fører til manglende situasjonsforståelse. Dette kan ha sammenheng med funn i delkapittel overvåke, hvor det ble pekt på manglende evne og kapasitet til å overvåke og avhengighet av eksterne kilder til overvåkning.

Mange operatører påpekte at hemmelighold hindret forståelsen av situasjonen, noe som igjen forsinket responsen og svekket situasjonsforståelsen for enkelte. Dette ble ytterligere forsterket av det faktum at to av operatørene nå opererer under sikkerhetsloven, og dermed kan ha tilgang til informasjon som ikke kan deles med andre operatører (Hovland & Holmes, 2022). Malerud med flere peker på at for å kunne bygge og vedlikeholde et situasjonsbilde, må man ha tilgang på informasjon fra ulike kilder på tvers av sektorer og nivåer. *«Tilgang til relevant informasjon om omgivelsene er fundamentalt for å kunne oppnå god situasjonsforståelse»* (Malerud et al., 2021, s. 28, 19). Å forstå hva man responderer på er ifølge Hollnagel viktig for å kunne respondere (Hollnagel, 2018, s. 29). Hemmelighold kan dermed forstås som at enkelte av operatørene pekte på manglende tilgang til, eller deling av informasjon, noe som svekket

evne til å forstå situasjonen eller trusselbildet. Samtidig sier også informantene at det er høy grad av deling av informasjon mellom operatørene. Det er altså inkonsistens i informantenes utsagn. Dette kan skyldes at det er en opplevelse av manglende deling, og at det er noe som holdes tilbake, til tross for deling av informasjon, eller at det pekes på informasjon som er gradert etter sikkerhetsloven og ikke kan deles uten at man har sikkerhetsklarering. Dette er ikke undersøkt i studien.

Informantene fremhevet også manglende risikoerkjennelse som et annet aspekt som kan påvirke forståelsen av situasjonen. Før Ukraina-krigen, droneobservasjonene, og sprenging av «Nord Stream» var det ifølge informantene er lav erkjennelse av at sikring innebar en betydelig risiko, og det var en tilfredshet rundt tilstanden. Det kan føres tilbake til mangel på hendelser. Det er veldig sjelden det oppstår sikringshendelser, og dette kan påvirke oppfattelsen av risiko (Jore, 2020; Jore & Egeli, 2015). James Reason argumenterer for at mangel av «bad events», bidrar til en oppfattelse av at systemet fungerer optimalt, det han omtaler som «unrocked boat» (Reason, 2016, s. 19). En metafor som beskriver en organisasjon som blir vant med tilstanden og driver ut av kurs uten å korrigere den. Dette kan tolkes som selvtilfredshet, noe som igjen kan underminere situasjonsforståelsen (Dekker & Hollnagel, 2004). Engen med flere peker på at evne til å behandle informasjon, og tilgang til informasjon kan påvirke vår risikopersepsjon (Engen et al., 2016, s. 94). Dette kan kobles til foregående funn om manglende evne til overvåkning og hemmelighold. Mangel på egen kapasitet til overvåkning, tilgang til tilstrekkelig informasjon, mangel på hendelser og også kompleksitet i trusselbildet («wicked-problem») kan dermed påvirke risikoerkjennelse, og dermed situasjonsforståelse. Dette igjen påvirker evne til overvåkning og dermed «resilience».

Oppsummering

I denne delen har jeg diskutert funn fra empirien mot teori som omhandler hvordan operatørene har operasjonalisert evnen til å overvåke. Funn tyder på at overvåkning hovedsakelig var basert på eksterne kilder som myndighetens råd, media, og tjenester fra eksterne overvåkningsfirma. Operatørene manglet egen kapasitet til å detektere droner offshore. For stor avhengighet av eksterne kilder kan føre til forsinkelser i deteksjon og respons. Selv om operatørene viste en evne til å tilpasse seg ved behov, tyder funnene på at deres overvåkning var mer reaktiv enn proaktiv.

Bruk av indikatorer er sentralt for å vurdere et systems ytelse. Selv med identifiserte indikatorer for trusselvurdering, slet operatørene med å utnytte disse effektivt. Mangelen på indikatorbruk kan kanskje tilskrives sjeldne sikringshendelser.

Effektiv overvåkning krever god situasjonsforståelse. Imidlertid hadde operatørene utfordringer med å etablere en klar situasjonsforståelse, spesielt i lys av komplekse trusselbilder. Jeg identifiserte flere barrierer mot klar situasjonsforståelse, deriblant hemmelighold og manglende erkjennelse av risiko

6.4. Evne til å respondere

For å besvare studiens problemstilling, vil jeg i dette kapittel diskutere tre temaer som illustrerer operatørenes operasjonalisering av responskapasitet i forbindelse med håndtering av dronetrusler høsten 2022.. Dette er «reaktiv respons», «ressursallokering», «planverk og trening» og «kommunikasjon og informasjonsdeling».

Reaktiv respons

Evnen til å respondere omhandler virksomhetens evne til å håndtere det aktuelle. Dette innebærer å forstå at det kreves en respons, hva denne responsen skal være rettet mot, og til slutt hvordan den skal utføres. Det er blant annet viktig å kunne reagere på riktig tidspunkt slik at ressursene brukes på best mulig måte. En virksomhet kan reagere enten proaktiv eller reaktivt. (Hollnagel, 2011a, s. 44). Intervjuene viser at operatørene hadde en reaktiv respons på observasjon av droner. De reagerte først når dronene hadde blitt observert. Samtidig hadde de etablert en prosess for å øke egen beredskap og evne til å til å håndtere hendelser. Dette refereres også til som "økning av sikringsnivået". Utfordringen var at disse tiltakene ikke ble iverksatt før dronene faktisk ble observert. Samtidig medførte det at de mobiliserte ressurser og økte bevisstheten om trusselbildet. Videre bidro det til at ytterliggere tiltak raskt kunne bli etablert. Dette kan fremme en raskere respons og kan indikere aktiviteter som styrker systemets «resilience»(Hollnagel, 2015, s. 3, 2018, s. 30).

Intervjuene avdekket varierende oppfatninger blant informantene om hvor godt forberedt de var. Informantene påpekte at hendelsen delvis kom uventet, og at det ikke var utført spesifikke forberedende tiltak i forkant av denne hendelsen. En sentral aspekt ved «resilience» er at det skal være uavhengig av spesifikke scenarioer. Man skal være forberedt og i stand til å håndtere det uventede. Intervjuene viser samtidig at de gjennomførte ulike aksjoner som viser en klar respons på hendelsen. En årsak til at operatørene her forklarer at de opplever at de ikke

var forberedt, kan ses i sammenheng med en lav bevissthet om «resilience»-begrepet, og aktivitetene som beskrives under kan tyde på at de i sum gjennomførte aktiviteter som kan anses som å bidra til «resilience». Informantene bemerket, for eksempel, at både offshore- og onshore-beredskapsorganisasjonene (på første og andre linje) mobiliserte og adresserte situasjonen som en beredskapshendelse. I tillegg ble det etablert en intern tverrfaglig arbeidsgruppe («task-force»). Denne gruppen koordinerte aktiviteter både internt og eksternt. Det ble også opprettet loggføring av observasjonene, og basert på dette en videre rapportering både til myndigheter og andre operatører. Dette bidrar til koordinering og samordning, som er sentrale elementer i et «resilient» system (Hollnagel, 2011a, s. 219–236; Steen & Molde, 2021). Selv om reaksjonen ofte var reaktiv, tok operatørene skritt for å øke sikringsnivået i lys av observasjonene. Dette demonstrerer en proaktiv tilnærming til sikring, der organisasjoner ikke bare reagerer på hendelser, men også tar skritt for å forhindre fremtidige hendelser eller forbedre håndteringen av dem (Hollnagel, 2017, s. 139).

Ressursallokering

Funn fra empirien antyder at sikkerhetstiltakene fikk fornyet fokus som følge av observasjonene samt hendelser som «Nord Stream». Ifølge Hollnagel er evnen til å omprioritere ressurser og ta hensyn til omkringliggende faktorer en kritisk egenskap innen RE (Hollnagel et al., 2009, s. 68). Informantene signaliserte at det eskalerende trusselbildet medførte en omprioritering av ressurser. Betydelige midler ble allokert for trusselhåndtering, noe som inkluderte etablering av spesialiserte arbeidsgrupper. Videre erkjente operatørene at håndtering av dronetrusselen oversteg deres kapasitet, og de anmodet derfor myndighetene om støtte til håndtering av hendelsen. Evnen til å omprioritere ressurser basert på en forståelse av omgivelsene og relevante faktorer kan tolkes som en indikasjon på «resilient» kapasitet.

Planverk og trening

Planverk og prosedyrer er fundamentale elementer som bidrar til et styrket grunnlag for effektiv respons(Hollnagel, 2018, s. 30). Operatørene understreket at de hadde utformet beredskaps- og sikringsplaner, men identifiserte en svakhet i mangel på spesifikke planer for håndtering av droneobservasjoner. Dette kan forstås som at de peker på behov for et mer rigid planverk, noe som ikke nødvendigvis fremmer «resilience». Et rigid planverk kan blant annet redusere fleksibiliteten og variasjonsrommet for å håndtere hendelser (Bergström et al., 2015), (Steen et al., 2022, s. 10). Planverk i seg selv har heller ingen verdi uten at det øvd og trent på

(Reason, 2016). Operatørene pekte selv dette som en mangel. Beredskapspersonell var i liten grad trent på å håndtere sikringshendelser, og dette skapte en usikkerhet. Dette kan ha påvirket forståelsen av situasjonen, noe som igjen gjorde at noen informanter fant det utfordrende å håndtere observasjonene i den innledende fasen.

For å imøtekomme mangel på planverk, oppdaterte de planene med konkrete tiltakskort for å håndtere droner. En slik tilpasning er noe som kan bidra til å styrke evnen til å respondere. I følge Steen og Molde handler tilpasning ikke bare om å endre eksisterende planer eller tilnærminger, men om potensielle til å revidere og modifisere dem (Steen & Molde, 2021, s. 11). Operatørene demonstrerte her sin evne til å reagere og justere sin respons.

Kommunikasjon og informasjonsdeling

Kommunikasjon og informasjonsdeling ble fremhevet som et suksesskriterium og en driver i håndteringen av droneobservasjonene. Hollnagel understreker også viktigheten av kommunikasjon og informasjon ikke bare for respons, men også for å forutse, overvåke og lære (Hollnagel, 2018, s. 50). Selv om de utviste forsiktighet ved deling av informasjon, ga respondentene uttrykk for at de var raske til å kommunisere og dele opplysninger, både internt og eksternt. Enkelte informanter opplevde også at visse opplysninger ble tilbakeholdt i den innledende fasen, delvis for å unngå unødvendig frykt og delvis fordi det manglet klarhet i forståelsen av situasjonen.

Informasjonen som var rettet mot ansatte offshore bidro til å skape en økt bevissthet. Ansatte fikk informasjon om situasjonen, at de skulle være årvåkne og rapportere, samt hva og hvordan de skulle rapportere. Dette resulterte i omfattende rapportering, ikke bare av faktiske droneobservasjoner, men også av stjerner, fly og andre objekter som feilaktig ble tolket som droner (TV2, 2023). Dette førte også til en oppfatning om at situasjonen var mer omfattende enn den faktisk var.

Det fremkom også informasjon om at hvordan dette ble håndtert, reduserte bekymring hos ansatte og bidro til å etablere en psykologisk trygghet hos ansatte. Dette er også et viktig element for å oppnå en organisatorisk «resilience» (Hollnagel, 2017, s. 4–5; Hollnagel et al., 2006, s. 223–233). Dette underbygges også i en studie av Scharffscher og Engen, som viser at god kommunikasjon i en krise er viktig trygghet for de som er rammet, og bygger på en tillitt til de som kommuniserer (Scharffscher & Engen, 2022). Disse funnene indikerer at operatørenes vektlegging på kommunikasjon og deling av informasjon fremmet «resilience».

Oppsummering

Funnene fra diskusjonen av temaene «reaktiv respons», «ressursallokering», «planverk og trening», og «kommunikasjon og informasjonsdeling» indikerer at operatørene, på tross av en reaktiv respons, iverksetter tiltak med en proaktiv tilnærming. Operatørene viste evne til å oppdatere og justere sine planer i lys av nye utfordringer, som i dette tilfellet var droneobservasjoner. Dette er demonstrasjon på organisasjonens tilpasningsevne under endrede forhold, noe som er en kjernekomponent i «resilience engineering». Da droneobservasjonene ble identifisert som en betydelig trussel, omdisponerte operatørene raskt ressurser for effektivt å håndtere utfordringen Rask mobilisering av ressurser og koordinert respons gjennom tverrfaglige team, som den tverrfaglige arbeidsgruppen, vitner om organisasjonens evne til effektiv håndtering av uventede hendelser. En slik koordinert respons kan dermed bidra til å oppnå positive utfall i kritiske situasjoner. Operatørene fokuserte også sterkt på kommunikasjon og deling av informasjon.

6.5. Evne til å lære

I denne delen skal diskusjonen konsentrere seg om tre hovedtemaer fremhevet fra analysen av empiriske data: «læring fra hendelser», «trening og øvelse», samt «sikringsnettverk – samarbeid». Målet er å drøfte hvordan operatørene operasjonaliserte sin evne til å lære fra håndteringen av dronetrusselen.

«Læring fra hendelser»

Læring innebærer at operatørselskapene må kunne tilegne seg ny kunnskap, kompetanse eller nye egenskaper. Læring har først funnet sted når det har medført en endring (Hollnagel, 2011b, s. 194). I intervjuene ble det påpekt at deltakerne opplevde læring som utfordrende, og at de i stor grad hadde en reaktiv tilnærming til læringsprosessen. Dette innebar at de hovedsakelig baserte sin læring på tidligere erfaringer og situasjoner som ikke hadde gått som planlagt. Engen beskriver dette som en hendelsesorientert tilnærming. Vi forbereder oss på den forrige krisen, og lar oss allikevel overraske når den først oppstår (Engen et al., 2016, s. 265). Vi har dermed ikke lært. Videre bemerket informantene at det sjelden eller aldri fant sted sikringshendelser. Dette understreker betydningen av å lære av det som går bra og de daglige aktivitetene (Hollnagel, 2018, s. 39). Selv om intervjuene kunne tyde på at det var liten bevissthet og systematisk tilnærming til å lære fra det som går bra og det vi gjør daglig, viste det seg allikevel i praksis at de gjennomførte aktiviteter som bidro til læring.

Selv om hendelser er sjeldne og kan antyde reaktiv læring, indikerer empirien at evnen til å lære fra andre relevante hendelser med lignende frekvens (sjelden) faktisk fant sted. Erfaring fra COVID-19 ble trukket fram. Det var spesielt bruk av «task-force», tverrfaglige grupper og samarbeid med andre operatører som ble trukket fram. Evnen til å lære fra andre tilsvarende hendelser er ifølge Hollnagel noe som underbygger evnen til å lære, og dermed bidrar til en «resilient» håndtering (Hollnagel, 2018, s. 37).

For at organisasjonene skal kunne lære, må de først erkjenne at det foreligger en hendelse som gir muligheter for læring (Hollnagel, 2018). Samtidig peker Hollnagel på at telling og registrering av hendelser i seg selv ikke bidrar til læring. Uten å forstå hvorfor hendelsen oppstår eller ikke oppstår er det vanskelig å lære (Hollnagel, 2018, s. 37). Dette kobler læring til utfordringer knyttet til situasjonsforståelse, og viser at utfordringer knyttet til å etablere en situasjonsforståelse også er koblet mot evnen til å lære.

Operatørene jobber med å utvikle bedre metoder blant annet ved bruk av teknologi for å kunne etablere situasjonsforståelse og forutse. Dette i seg selv tyder på læring og en endring av tilnærming. Ved å lære fra endringer i trusselbildet, og forståelse av trusselbildet, kan dette bidra til å oppdage større farer (Nemeth et al., 2016, s. 121). Det er dette trussel- og sikringsrisikovurdering kan bidra til, og dermed styrke evnen til læring.

Det kan også tyde på at egenskapen til å justere kursen og tilpasse seg, var basert på læring fra det de gjorde rett. Dette kan indikere at operatørene ikke bare lærer fra det som går galt, men også fra håndteringen og den daglige driften. Dette er i seg selv en egenskap som ifølge Hollnagel er sentral i «resilience engineering» (Hollnagel, 2011a, s. 194).

Trening og øvelse

I intervjuene ble det pekt på at operatørene gjennomfører trening og øvelse, spesielt når trusselnivået øker, rettet mot å håndtere dronetrusselen. Hollnagel peker på at kompetent personell er en forutsetning for å lære (Hollnagel, 2018, s. 37). Flere av informantene pekte på at deres inntrykk var at organisasjonen manglet kompetanse og trening på sikringshendelser. Til tross for dette fremkom det at de var i stand til å håndtere hendelsen. Det ble pekt på at et suksesskriterium var nettopp kompetent personell. Dette var basert på at det over tid var bygget opp en kompetanse i å håndtere ulike typer hendelser. Dette tyder ikke bare på kompetent personell, men også en evne til å bruke læring fra andre hendelser inn i nye hendelser. Noe av kjernen i RE er at virksomheten skal være i stand til å håndtere det uventede. Dette kan forståes som en vesentlig egenskap i en «resilient» organisasjon. Funn tyder dermed på at dette er noe

operatørene har fått til. Dette kan også tyde på en tilstedeværelse av organisatorisk læring, noe som bidrar til å styrke evnen til «resilient» håndtering (Ptil, 2013; Steen et al., 2022). Resultatene antyder at beredskapsorganisasjonen, til tross for manglende kompetanse innen sikringshendelser, hadde utviklet en hendelseshåndteringskompetanse som var anvendbar selv i situasjoner de ikke hadde spesifikk trening for. I tillegg var de i stand til å øke treningsmengden.

Sikringsnettverk – samarbeid

Empirien viser at samarbeid er en vesentlig egenskap som ikke bare bidrar til læring, men også til respons, overvåkning og evnen til å forutse hendelser. Det etablerte sikringsnettverket i regi av Offshore Norge ble spesielt fremhevet for å bidra til å overføre kunnskap og erfaring. Selv om samarbeid i seg selv ikke er læring, forutsetter det at operatørene har ressurser, vilje og evne til å overføre informasjon for å implementere endringer i egen organisasjon, noe som ser ut til å ha vært tilfelle (Hollnagel, 2018, s. 37). I tillegg er læring fra andre og andres feil et element i å bygge «resilience» (van der Merwe et al., 2018, s. 9). I intervjuene ble det for eksempel nevnt at noen operatører lærte av andre ved å implementere en «task-force» og dele tiltakskort for droner. Dette ble tatt i bruk og videreført i egen organisasjon.

I tillegg til å lære fra hverandre i nettverket, var dette også sentralt i å koordinere internt, for eksempel økte operatørene sikringsnivået på heliport og baser, samt koordinerte dialogen mot myndigheter. Bjørn Ivar Kruke og Odd Einar Olsen har i en undersøkelse av humanitære organisasjoner i et kriseområde funnet at:

> *Coordination among the humanitarian actors is therefore a key factor when seeking reliability in humanitarian operations, making both flexibility and diversity foundations for resiliency in humanitarian operations, and thus, also reliability (Kruke & Olsen, 2005, s. 284).*

I sin forskning har de funnet at evnen til å samarbeide på kryss av "virksomhetene" bidrar til å nyttiggjøre seg av ressurser utover sine egne, for eksempel med hensyn til kompetanse og andre ressurser. Samarbeid bidrar dermed til «resilience». Dette underbygges også av nyere forskning, hvor Riana Steen med flere har undersøkt beredskapshåndtering av COVID-19 og argumenterer for at nettverksbygging og samarbeid styrker «resilience» (Steen et al., 2022, s. 1). Det etablerte nettverket bidrar dermed til samvirke og koordinering, og styrker dermed selskapenes «resilience» med hensyn til håndtering av droneobservasjonene.

Oppsummering

Til tross for en tilsynelatende reaktiv tilnærming til læring, basert hovedsakelig på tidligere erfaringer, har operatørene vist evne til å lære fra hendelser, selv de som skjer sjelden. Interessant nok brukte de erfaring fra COVID-19, et eksempel på å lære fra andre relevante hendelser for å forbedre deres håndtering.

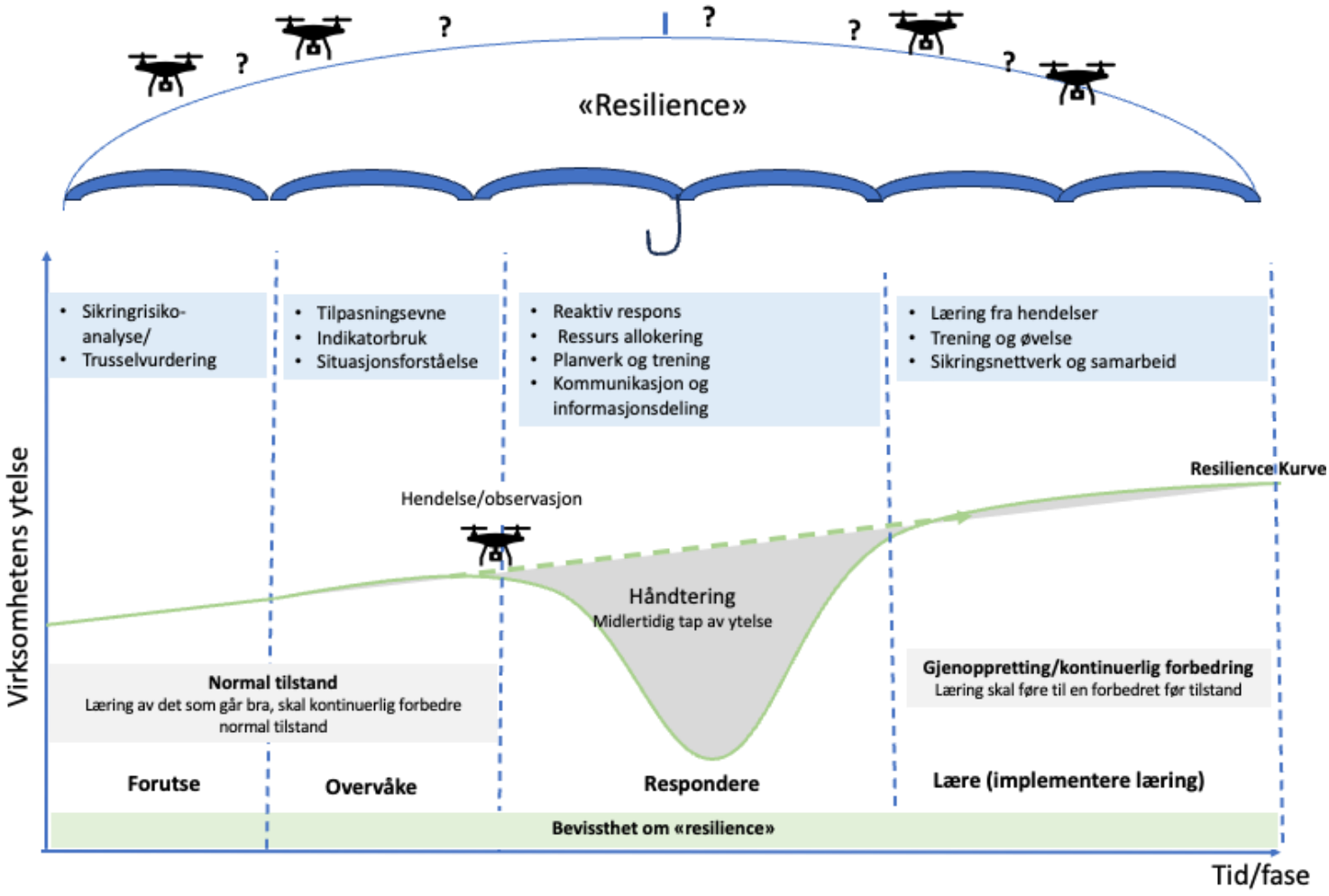
Selv med en opplevd mangel på kompetanse i sikringshendelser, har operatørene kontinuerlig utført trening på andre typer hendelser. Denne tilnærmingen, sammen med tidligere ervervet kompetanse fra ulike hendelser, har utrustet operatørene til å håndtere uforutsette utfordringer, hvilket er kjernen i «resilience engineering».

Samarbeid viser seg som en kritisk komponent. Det etablerte sikringsnettverket i regi av Offshore Norge har vært et viktig verktøy for å overføre kunnskap og erfaring. Gjennom dette nettverket har operatørene kunnet lære fra hverandre, spesielt når det gjelder å møte nye trusler. Dette understreker også viktigheten av koordinering, ikke bare internt, men også med eksterne organisasjoner og myndigheter.

6.6. Fra teori til praksis

Figuren under er en forenklet illustrasjon av hvordan «resilience» ble operasjonalisert. Bildet viser teori anvendt i praksis, i forhold til kontekst av studien, og oppsummerer diskusjon.

Illustrasjon viser de ulike egenskapene satt opp som faser (i realiteten er ikke dette en lineær prosess, men iterativ og kontinuerlig). De blå tekstboksene oppsummerer elementene som har påvirket operatørenes «resilience», disse ble identifisert gjennom den tematiske analysen. I tillegg til de fire evnene er det det også tatt inn «bevissthet om resilience». Funn fra studien kan tyde på at til tross for at bevisstheten om «resilience» ikke var høy, så har operatørene allikevel en rekke aktiviteter som bidrar til «resilience». Det er dermed summen av aktiviteter som bidrar til å etablere «resilience», i denne kontekst mot droneangrep.



Figur 12 Operasjonalisering av «resilience»

7. Konklusjon

7.1. Konklusjon

Denne studien skal besvare følgende problemstilling:

> *Hvordan har operatørene operasjonalisert prinsippene fra «resilience engineering» i forbindelse med håndtering av dronetrusselen høsten 2022.*

For å svare på denne problemstillingen er det tatt utgangspunkt i Hollnagel sine fire evner; forutse, overvåke, respondere og lære. Det er gjennom en empirisk undersøkelse identifisert ulike tema som påvirker og bidrar til å operasjonalisere disse evnene.

Operasjonaliseringen av prinsippene fra «resilience engineering» (RE) i håndtering av dronetrusselen høsten 2022 har vært en kompleks prosess for operatørene. På bakgrunn av funnene kan det konkluderes med følgende:

Operatørene har lagt vekt på overvåking ved bruk av trussel- og sikringrisikovurderingen. Selv om disse metodene er verdifulle for overvåking, er de mindre velegnet for å forutse fremtidige scenarioer. Kjernen i utfordringen ligger i at disse vurderingene ofte bygger på tidligere erfaringer, med begrenset vektlegging av dynamiske forhold og usikkerhet.

Overvåkningens avhengighet av eksterne kilder fremhever et kritisk område for forbedring. Fraværet av egen deteksjonskapasitet offshore, kombinert med utfordringene knyttet til situasjonsforståelse, viser behovet for styrking av proaktive overvåkningsmetoder.

Selv med en reaktiv respons har operatørene vist en proaktiv tilnærming til iverksettelse av tiltak. Deres evne til raskt å omdisponere ressurser og koordinere responsen vitner om en robusthet og tilpasningsevne innen organisasjonen.

Operatørene har operasjonalisert evnen til å lære i håndtering av dronetrussel ved å dra nytte av lærdommer fra tidligere hendelser, legge vekt på trening og øvelse og forsterke tverrfaglig samarbeid og nettverksbygging. Disse mekanismene tjener sammen som en robust tilnærming til å styrke evnen til å håndtere fremtidige dronetrusler. Samlet sett viser dette at operatørene har investert betydelig i å forstå og takle dronetrusselen. Mens det er områder som krever forbedring, som overvåkning og forutseende metoder, er det også klare styrker, spesielt i deres evne til å reagere på og lære av trusler. For å håndtere de identifiserte utfordringene bør det legges vekt på å kombinere teknologiske løsninger med organisatoriske tilnærminger for å styrke det sosiotekniske systemet ytterligere. Noe som det i denne studien har blitt pekt på er potensialet i bruk av «datasystemer» og AI for å gjennomføre sikringsrisikovurderinger som holdes kontinuerlig oppdatert.

Funnene indikerer en blandet tilnærming til RE-prinsippene. Mens det er klare styrker i operatørenes evne til å reagere på og lære fra trusler, er det også rom for forbedring i deres evne til å forutse og overvåke slike trusler. En forståelse av disse styrkene og svakhetene kan bidra til å informere fremtidig håndtering ved å forbedre praksis forbindelse med dronetrusler og andre komplekse utfordringer.

Det er viktig å peke på at funnene i denne studien kan være begrenset av datagrunnlaget og de metodene som ble benyttet. Videre kunne en dypere gransking av hvordan operatørene konkret integrerer ny teknologi og praksis i sitt arbeid gitt et mer helhetlig bilde.

Denne studien understreker viktigheten av en kontinuerlig evaluering og tilpasning av praksis for å håndtere komplekse trusler i en verden i stadig endring. Avslutningsvis, sitatet under fra den kjente militær strategen og filosofen Sun Tzu illustrerer på mange måter «resilience» og viktigheten av å være forberedt, samt ha en sterk strategi på plass før en hendelse inntreffer.

«Forbered deg alltid på kamp, selv når du søker fred."

7.2. Videre forskning

Under utarbeidelse av denne studien har jeg måttet utelate flere spennende tema som det kan være interessant å forske videre på. Et av temaene jeg har måttet utelate er myndighetenes ansvar og rolle, og hvordan dette er knyttet til virksomhetenes håndtering. Dette er et veldig aktuelt tema som kun delvis berørt i studien. Både NOU 14:2023 og NOU 17:2023 adresser virksomhetenes ansvar i «totalforsvaret» og betydningen av samarbeid og informasjonsutveksling for å skape en helhetlig situasjonsforståelse (Beredskapsdepartementet, 2023; Forsvarsdepartementet, 2023).

Utfordring knyttet til myndighetenes effektivitet og respons var noe av det som kom fram i forbindelse med intervjuene. Det ble pekt på manglende intern koordinering hos myndighetene, manglende forståelse og kompetanse, herunder situasjonsforståelse. Det kunne vært interessant å forske videre på hvordan myndighetenes effektivitet og respons påvirker eller hindrer virksomhetenes respons. Det kom tydelig fram i min studie at operatørene legger stor vekt på informasjon fra myndighetene, men at det i begrenset grad kommer noe andre veien. Hvordan påvirker dette for eksempel den helhetlige situasjonsforståelsen og håndteringen av sikringshendelser?

8. Referanser

Aftenposten. (2023, januar 5). Stoltenberg advarer mot avhengighet av Kina. *Aftenposten*. https://www.aftenposten.no/norge/politikk/i/ve6odB/stoltenberg-advarer-mot-avhengighet-av-kina

Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *231*(3), 286–294. https://doi.org/10.1177/1748006X17699145

Andersen, S. S. (2006). Aktiv informantintervjuing. *Norsk statsvitenskapelig tidsskrift*, *22*(3), 278–298. https://doi.org/10.18261/ISSN1504-2936-2006-03-03

Aven, T. (2007). Risikostyring: Grunnleggende prinsipper og ideer. I *Norbok*. Universitetsforl. https://urn.nb.no/URN:NBN:no-nb_digibok_2013071705159

Aven, T. (2013). On the meaning of a black swan in a risk context. *Safety Science*, *57*, 44–51. https://doi.org/10.1016/j.ssci.2013.01.016

Aven, T. (2017). How some types of risk assessments can support resilience analysis and management. *Reliability Engineering & System Safety*, *167*, 536–543. https://doi.org/10.1016/j.ress.2017.07.005

Aven, T. (2022). A risk science perspective on the discussion concerning Safety I, Safety II and Safety III. *Reliability Engineering & System Safety*, *217*, 108077. https://doi.org/10.1016/j.ress.2021.108077

Beredskapsdepartementet, J. (2023). *NOU 2023: 17* [NOU]. regjeringen.no. https://www.regjeringen.no/no/dokumenter/nou-2023-17/id2982767/

Bergström, J., van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering & System Safety*, *141*, 131–141. https://doi.org/10.1016/j.ress.2015.03.008

Berling, T. V., & Petersen, K. L. (2020). Designing resilience for security in the Nordic region. I S. Larsson & M. Rhinard, *Nordic Societal Security* (1. utg., s. 131–153). Routledge. https://doi.org/10.4324/9781003045533-10

Botnan, J. I., & Lausund, R. (2016). *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart* (FFI-RAPPORT 16/00702). FFI.

British Library. (2023). *Peter Drucker: Father of management thinking*. The British Library; The British Library. https://www.bl.uk/people/peter-drucker

Brooks, D. J. (2010). What is security: Definition through knowledge categorization. *Security Journal*, *23*(3), 225–239. https://doi.org/10.1057/sj.2008.18

Busmundrud, O., Maal, M., Endregard, M., & Hagnes, J. (2016). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. https://doi.org/10.13140/RG.2.1.1443.3048

Cooper, M. D. (2022). The Emperor has no clothes: A critique of Safety-II. *Safety Science*, *152*, 105047. https://doi.org/10.1016/j.ssci.2020.105047

Cullen, P. (2018). *Hybrid threats as a new 'wicked problem' for early warning*.

Dagens næringsliv. (2021, oktober 22). OPERASJON LAZAREV: Slår alarm om kartlegging av Norges kritiske infrastruktur (+). *www.dn.no*. https://www.dn.no/magasinet/dokumentar/spionasje/russland/etterretningstjenesten/operasjon-lazarev-slar-alarm-om-kartlegging-av-norges-kritiske-infrastruktur/2-1-1085420

Dekker, S., & Hollnagel, E. (2004). Human factors and folk models. *Cognition, Technology & Work*, *6*(2), 79–86. https://doi.org/10.1007/s10111-003-0136-9

Engen, O. A. (2023). Sabotasje. I *Store norske leksikon*. https://snl.no/sabotasje

Engen, O. A., Kruke, B. I., Lindøe, P., Olsen, K. H., Olsen, O. E., & Gould, K. A. P. (2016). *Perspektiver på samfunnssikkerhet* (1. utgave. 2. opplag). Cappelen Damm akademisk. https://www.nb.no/search?q=oaiid:"oai:nb.bibsys.no:999920149375502202"&mediatype=bøker

FN-Sambandet. (2023, mars 27). *Ukraina*. Ukraina. https://www.fn.no/konflikter/ukraina

Forsvarsdepartementet. (2023). *NOU 2023: 14* [NOU]. regjeringen.no. https://www.regjeringen.no/no/dokumenter/nou-2023-14/id2974821/

Gjerstad, T., & Kibar, O. (2022, november 4). *En drone flyr mot en plattform – hvem tar ansvaret? (+)*. www.dn.no. https://www.dn.no/magasinet/dokumentar/en-drone-flyr-mot-en-plattform-hvem-tar-ansvaret/2-1-1344632

Gjørv, A. B. (2012). *Rapport fra 22. Juli-kommisjonen* (NOU 2012:14; Norges offentlige utredninger). Departementenes servicesenter. Informasjonsforvaltning. https://urn.nb.no/URN:NBN:no-nb_digibok_2020013107050

Grøtan, T., Størseth, F., Eitrheim, M. H., & Skjerve, A. (2008). *Resilience, Adaptation and Improvisation–increasing resilience by organising for successful improvisation*.

Guillaume, E. G. (2011). *Identifying and responding to weak signals to improve learning from experiences in high-risk industry*. https://repository.tudelft.nl/islandora/object/uuid%3Af455e8a0-cce5-4a36-8a98-f83371dc2a2a

Hale, A. (2014). Foundations of safety science: A postscript. *Safety Science, 67*, 64–69. https://doi.org/10.1016/j.ssci.2014.03.001

Hollnagel, E. (Red.). (2011). *Resilience Engineering in Practice: A Guidebook*. CRC Press. https://doi.org/10.1201/9781317065265

Hollnagel, E. (2014). Resilience engineering and the built environment. *Building Research and Information, 42*. https://doi.org/10.1080/09613218.2014.862607

Hollnagel, E. (2015). *RAG – Resilience Analysis Grid*. https://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf

Hollnagel, E. (2017). *Safety-I and Safety-II: The Past and Future of Safety Management*. CRC Press. https://doi.org/10.1201/9781315607511

Hollnagel, E. (2018). *Safety-II in Practice: Developing the Resilience Potentials*. CRC Press LLC. http://ebookcentral.proquest.com/lib/uisbib/detail.action?docID=4891078

Hollnagel, E. (2016). *Resilience Engineering*. Erik Hollnagel. Resilience Engineering. https://erikhollnagel.com/ideas/resilience-engineering.html

Hollnagel, E., Nemeth, C. P., & Dekker, S. (Red.). (2009). *Resilience Engineering Perspectives, Volume 2: Preparation and Restoration*. CRC Press. https://doi.org/10.1201/9781315244389

Hollnagel, E., Wears, R. L., & Braithwaite, J. (2015). *From Safety-I to Safety-II: A White Paper*. https://doi.org/10.13140/RG.2.1.4051.5282

Hollnagel, E., Woods, D. D., & Leveson, N. (Red.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate.

Hovland, K. M., & Holmes, M. (2022, september 28). *Equinor og Gassco lagt under sikkerhetsloven: – Naturlig at vi skjerper beredskapen* [Nettavis]. E24. https://e24.no/i/xg8Awn

ISO. (2018). *ISO 31000:2018(en), Risk management—Guidelines*. www.iso.org. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Jacobsen, D. I. (2022). *Hvordan gjennomføre undersøkelser?: Innføring i samfunnsvitenskapelig metode* (4. utgave.). Cappelen Damm akademisk. https://www.nb.no/search?q=oaiid:"oai:nb.bibsys.no:999920298324802202"

Jore, S. H. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*, *4*(1), 157–174. https://doi.org/10.1007/s41125-017-0021-9

Jore, S. H. (2020). Security and Safety Culture—Dual or Distinct Phenomena? I C. Bieder & K. Pettersen Gould (Red.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (s. 43–51). Springer International Publishing. https://doi.org/10.1007/978-3-030-47229-0_5

Jore, S. H. (2023). Is Resilience a Good Concept in Terrorism Research? A Conceptual Adequacy Analysis of Terrorism Resilience. *Studies in Conflict & Terrorism*, *46*(1), 1–20. https://doi.org/10.1080/1057610X.2020.1738681

Jore, S. H., & Egeli, A. (2015). *Risk management methodology for protecting against malicious acts: Are probabilities adequate means for describing terrorism and other security risks?* 807–815.

Kruke, B. I., & Olsen, O. E. (2005). Reliability-seeking networks in complex emergencies. *International Journal of Emergency Management*, *2*(4), 275. https://doi.org/10.1504/IJEM.2005.008740

Kvale, S., & Brinkmann, S. (2009). *Det kvalitative forskningsintervju* (2. utg.). Gyldendal akademisk. https://urn.nb.no/URN:NBN:no-nb_digibok_2020112307061

Larsen, C. I., & Østensjø, C. (2015). *Operatørselskapene i petroleumssektoren sitt syn på sikringskultur: Bruk eller ikke bruk av begrepet sikringskultur* [Master thesis, University of Stavanger, Norway]. https://uis.brage.unit.no/uis-xmlui/handle/11250/298602

Leveson, N. (2020). *Safety III: A Systems Approach to Safety and Resilience*.

Lunde, I. K. (2014). *Praktisk krise- og beredskapsledelse*. Universitetsforl.

Madni, A., Erwin, & Sievers, M. (2020). Constructing Models for Systems Resilience: Challenges, Concepts, and Formal Methods. *Systems*, *8*, 3. https://doi.org/10.3390/systems8010003

Malerud, S., Hennum, A. C., & Toverød, N. (2021). *Situasjonsforståelse ved sammensatte trusler—Et konseptgrunnlag* (21/00246). FFI. https://www.ffi.no/publikasjoner/arkiv/situasjonsforstaelse-ved-sammensatte-trusler-et-konseptgrunnlag

Marquez-Tejon, J., Jimenez-Partearroyo, M., & Benito-Osorio, D. (2022). Security as a key contributor to organisational resilience: A bibliometric analysis of enterprise security risk management. *Security Journal*, *35*(2), 600–627. https://doi.org/10.1057/s41284-021-00292-4

Nemeth, C. P., Hollnagel, E., & Dekker, S. (2016). *Resilience Engineering Perspectives, Volume 1: Remaining Sensitive to the Possibility of Failure*. CRC Press. https://doi.org/10.4324/9781315244396

Norsk Petroleum. (2023). *Norskpetroleum.no—Fakta om norsk olje- og gassvirksomhet*. Norskpetroleum.no. https://www.norskpetroleum.no/

NRK. (2022, oktober 7). *Politiet bekrefter samarbeid med Forsvaret i drone-etterforskningen*. NRK. https://www.nrk.no/rogaland/politiet-bekrefter-samarbeid-med-forsvaret-i-drone-etterforskningen-1.16131326

NSM. (2020, juni 10). *Dette er NSM - Nasjonal sikkerhetsmyndighet*. https://nsm.no/om-oss/dette-er-nsm/

NTB. (2014, august 27). Norske bedrifter utsatt for det største dataangrepet i historien. *Teknisk Ukeblad*. https://www.tu.no/artikler/norske-bedrifter-utsatt-for-det-storste-dataangrepet-i-historien/230443

NTB. (2022, juni 30). Ti tonn tung undersjøisk kabel forsvant i Vesterålen – nå er saken henlagt. *www.dn.no*. https://www.dn.no/ti-tonn-tung-undersjoisk-kabel-forsvant-i-vesteralen-na-er-saken-henlagt/2-1-1249481

Offshore Norge. (2023). *Om oss*. Offshore Norge. https://offshorenorge.no/om-oss/

Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2018). Resilience engineering: Current status of the research and future challenges. *Safety Science*, *102*, 79–100. https://doi.org/10.1016/j.ssci.2017.10.005

Patriarca, R., Di Gravio, G., Costantino, F., Falegnami, A., & Bilotta, F. (2018). An Analytic Framework to Assess Organizational Resilience. *Safety and Health at Work*, *9*(3), 265–276. https://doi.org/10.1016/j.shaw.2017.10.005

Peace Research Institute Oslo: New European Commission-Funded Research on Countering Drone Threats. (2020). Targeted News Service.

PST. (2023). *NTV-2023* [Threat Assessment]. https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/

Ptil. (2013). *En bok om læring*. https://www.ptil.no/contentassets/17aa07f6f5e44e4a91244835509bb70e/laringshefte_lavopplost-norsk.pdf

Ptil. (2023a). På vakt for verdiene. *Dialog*. https://www.ptil.no/fagstoff/utforsk-fagstoff/reportasjer/2023/pa-vakt-for-verdiene2/

Ptil. (2022a). *IKT-tryggleik i industrielle system*. https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2022/ikt-tryggleik-i-industrielle-system/

Ptil. (2022b). *Sikringsdagen 2022*. https://www.ptil.no/fagstoff/utforsk-fagstoff/video/2022/sikringsdagen-2022/

Ptil. (2023b). *Hvem har ansvar for samfunnssikkerhet og sikring?* https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2023/samfunnssikkerhet-og-sikring--ptils-ansvar/

Ptil. (2023c). *Kontinuerlig forbedring*. https://www.ptil.no/regelverk/alle-forskrifter/styringsforskriften/VI/23/

Ptil. (2023d). *Olje- og energiministeren overtar ansvaret for Ptil*. https://www.ptil.no/tilsyn/viktige-meldinger/2023/olje--og-energiministeren-overtar-ansvaret-for-petroleumstilsynet/

Ptil. (2023e). *Petroleumstilsynets rolle og ansvarsområde*. https://www.ptil.no/om-oss/rolle-og-ansvarsomrade/

Ptil. (2023f). *Risikonivå i norsk petroleumsvirksomhet—RNNP Petroleumstilsynet*. Petroleumstilsynet RNNP. https://www.rnnp.no/

Ptil. (2023g). *Sikkerhet og sikring må sees i sammenheng*. https://www.ptil.no/fagstoff/utforsk-fagstoff/reportasjer/2023/sikkerhet-og-sikring-ma-sees-i-sammenheng/

Ptil. (2023h). *Styrket IKT-sikkerhet*. https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2023/styrket-ikt-sikkerhet/

Ptil. (2023i). *Trusselbildet og norsk petroleumsvirksomhet*. https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2023/trusselbildet-og-norsk-petroleumsvirksomhet/

Reason, J. (2016). *Managing the Risks of Organizational Accidents (eBook)*. Routledge. https://doi.org/10.4324/9781315543543

Reichborn-Kjennerud, E., & Cullen, P. (2016). *What is Hybrid Warfare?* https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2380867

Scharffscher, K. S., & Engen, O. A. (2022). Pandemi, tillit og kommunikasjon. *Stat & Styring*, *32*(2), 6–9. https://doi.org/10.18261/stat.32.2.3

Schuurman, B., & Eijkman, Q. (2015). Indicators of Terrorist Intent and Capability: Tools for Threat

Assessment. *Dynamics of Asymmetric Conflict*. https://doi.org/10.1080/17467586.2015.1040426

Shukla, A., & Solbakken, E. A. (2022). *Hvordan kan anvendelse av resiliens styrke cyber-beredskap i virksomheter* [Master thesis, uis]. https://uis.brage.unit.no/uis-xmlui/handle/11250/3037553

Skare, E. (2022). *Norsk petroleumssektor, rolleforståelse og hybride trusler – kan Resilience Engineering være en hensiktsmessig tilnærming?* [Master thesis, uis]. https://uis.brage.unit.no/uis-xmlui/handle/11250/3016379

Smith, C., & Brooks, D. (2013). *Security Science: The Theory and Practice of Security*.

SRA. (2015). *Society for Risk Analysis Glossary*.

Standard Norge. (2012). *NS 5830:2012 Samfunnssikkerhet—Beskyttelse mot tilsiktede uønskede handlinger—Terminologi*. https://online.standard.no/ns-5830-2012

Standard Norge. (2021). *NS 5814 Krav til risikovurderinger*. https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1352200

Stavland, B., & Bruvoll, J. A. (2019). *Resiliens – hva er det og hvordan kan det integreres i risikostyring?* (FFI rapport 19/00363). FFI. https://publications.ffi.no/nb/item/asset/dspace:6458/19-00363.pdf

Steen, R. (2019). On the Application of the Safety-II Concept in a Security Context. *European Journal for Security Research*, *4*(2), 175–200. https://doi.org/10.1007/s41125-019-00041-0

Steen, R., & Aven, T. (2011). A risk perspective suitable for resilience engineering. *Safety Science*, *49*(2), 292–297. https://doi.org/10.1016/j.ssci.2010.09.003

Steen, R., Haakonsen, G., & Patriarca, R. (2022). «Samhandling»: On the nuances of resilience through case study research in emergency response operations. *13*. https://uis.brage.unit.no/uis-xmlui/handle/11250/3004558

Steen, R., & Molde, A. I. (2021). Håndtering av langvarige beredskapshendelser: Læringspunkter etter covid-19-utbrudd på West Phoenix. *Magma - Tidsskrift for økonomi og ledelse*.

https://uis.brage.unit.no/uis-xmlui/handle/11250/3011670

Stormark, K. (2023a, mars 1). *Dronebølgen*. Politiforum. https://www.politiforum.no/dronebolgen/236136

Stormark, K. (2023b, mars 2). *Slik etterforsket de dronehendelsene*. Politiforum. https://www.politiforum.no/slik-etterforsket-de-dronehendelsene/236181

Stornes Stålesen, J. (2011). *Security styring i petroleumssektoren* [Master thesis, University of Stavanger, Norway]. https://uis.brage.unit.no/uis-xmlui/handle/11250/184873

Thoma, K. (2014). *Resilien-Tech. «Resilience by Design»: A strategy for the technology issues of the future*. acatech. https://en.acatech.de/publication/resilien-tech-resilience-by-design-a-strategy-for-the-technology-issues-of-the-future/

Thoma, K., Scharte, B., Hiller, D., & Leismann, T. (2016). Resilience Engineering as Part of Security Research: Definitions, Concepts and Science Approaches. *European Journal for Security Research*, *1*(1), 3–19. https://doi.org/10.1007/s41125-016-0002-4

Tjora, A. H. (2021). *Kvalitative forskningsmetoder i praksis* (4. utgave.). Gyldendal.

TV2. (2023, januar 20). *Derfor henla politiet alle dronesakene*. TV 2. https://www.tv2.no/nyheter/innenriks/derfor-henla-politiet-alle-dronesakene/15443488/

van der Merwe, S. E., Biggs, R., & Preiser, R. (2018). A framework for conceptualizing and assessing the resilience of essential services produced by socio-technical systems. *Ecology and Society*, *23*(2). https://www.jstor.org/stable/26799110

VG.no. (2020, august 17). PST: Nordmann pågrepet for å ha delt statshemmeligheter. *VG*. https://www.vg.no/i/lA7z1L

VG.no. (2023, mars 17). *Stoltenberg og von der Leyen er på Troll-plattformen: Takker Norge*. https://www.vg.no/i/xg9qvX

Vivoll, T. (2015). Resilience Engineering – Nøkkelen til bygging av god sikringskultur innen petroleumsvirksomheten? [Master thesis, University of Stavanger, Norway]. I *84*.

https://uis.brage.unit.no/uis-xmlui/handle/11250/2367003

Woltjer, R. (2015). *Darwin D1.1* (HORIZON 2020: Secure Societies TOPIC DRS-7-2014 653289; Darwin D1.1 Consolidation of resilience concepts and practices for crisis management.). Darwin. https://h2020darwin.eu/wp-content/uploads/2017/10/DARWIN_D1.1_Consolidate_resilience_concepts_and_practices_for_crisis_management.pdf

Woods, D. (2018). Resilience is a verb. I *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems.: Bd. Vol 2*. IRGC - CH: EPFL International Risk Governance Center. https://irgc.org/wp-content/uploads/2018/12/Woods-for-IRGC-Resilience-Guide-Vol-2-2018.pdf

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, *141*, 5–9. https://doi.org/10.1016/j.ress.2015.03.018

Åklagarmyndigheten. (2022). *Bekräftat sabotage vid Nord Stream*. Åklagarmyndigheten. https://www.aklagare.se/nyheter-press/pressmeddelanden/2022/november/bekraftat-sabotage-vid-nord-stream/

9. Vedlegg

9.1. Intervjuguide

Introduksjon

Formålet med denne masteroppgaven er å undersøke hvilke egenskaper ved operatørenes håndtering av dronetrussel høsten 2022 som har bidratt til en «resilient» håndtering?

Spørsmålene er ment som en pekepinn på hvilke elementer vi kan komme inn på i intervjuet, og vil nødvendigvis ikke gjennomgås i sin helhet.

Innledende spørsmål og begrepsavklaring

- Kan du si litt om din rolle i organisasjonen og hvordan din virksomhet jobber med sikringsrisiko
- Hvilket forhold har din virksomhet til begrepene robusthet og resilience?

Styring

- Hvilken tilnærming til styring av sikringsrisiko har dere, hvordan er sikring integrert i virksomhetsdriften/styringssystem.

Respondere – vite hva man skal gjøre

Hovedspørsmål: Kan du beskrive hvordan din virksomhet har håndtert den økte trussel fra Russland og dronetrussel spesielt, har denne trussel endret noe med håndtering hos dere?

- Hva har vært viktige drivere for håndteringen/endringen

Støttespørsmål/indikatorspørsmål:

- Er det noe spesielt med denne situasjonen (økte trussel), noe som skiller seg spesielt ut, eller en ordinær hendelse som organisasjonen var forberedt på å håndtere.
- Har dere hatt tilstrekkelig ressurser, og har dette endret seg (personell, kompetanse, utstyr etc.)
- Hvordan har virksomheten tilpasset seg trusselen, du gi eksempler på konkrete endringer, aksjoner, tiltak som har blitt gjort/iverksatt
- Har dere beredskaps/sikringsplaner, og evt. Tiltakskort for håndtering av droner og har dere måttet endre planverk?

Overvåke – vite hva man skal se etter

Hovedspørsmål: Kan du beskrive hvordan dere jobber med å overvåke og identifisere dronetrussel og endring i trusselbildet, og har dette endret seg på grunn av økt trussel

- *Hva* har vært viktige drivere for håndteringen/endringen

Støttespørsmål/indikatorspørsmål:

- Hva slags verktøy eller systemer bruker dere for å overvåke og hva overvåker dere (hva er viktige faktorer for å overvåke)
    - Risiko/trusselbilde, Ytelsen til komponentene i systemet, kompetanse osv)
- Hvordan har dere tilpasset deres overvåkningssystemer etter hvert som trusselnivået har økt? (hvilke tiltak og reaksjoner har blitt iverksatt for eksempel økt opplæring)
- Overvåker dere området rundt installasjon for droner, og hvordan (manuelt eller teknisk)
- Hva slags respons og reaksjon har dere iverksatt når drone har blitt oppdaget
- Hvordan sørger dere for at ansatte og andre interessenter er oppmerksomme på og klar over sikkerhetstrusler og -risikoer?

Forvente – vite hva man kan forvente

Hovedspørsmål: Kan du beskrive hvordan dere har jobbet og jobber med å identifisere framtidige sikringshendelser som kan påvirke dere for eksempel utfordring knyttet til droner.

- *Hva* har vært viktige drivere for håndteringen/endringen

Støttespørsmål/indikatorspørsmål:

- Hvordan har denne hendelsen påvirket forståelsen og fokus på trusler.
- Hvordan bruker dere data og analyser for forutse potensielle dronetrusler mot installasjonene, og hvordan bruker dere informasjon til å tilpasse overvåkning og responsplaner.
- Hvordan har dere vurdert fremtidige trusler som kan true innretningene, og hva er drivere for denne vurderingen.
- Hvilke ressurser og kompetanse har dere, og har behovet endret seg. Hvilken rolle har dette mht. til å kunne forutse hva som skjer.
- Har ledelsens prioritering endret seg.

Lære – vite hva som har skjedd

Hovedspørsmål: Kan du beskrive hvordan dere jobber med (kontinuerlig) læring - og har dette endret seg på grunn av økt trussel

- Hva har vært viktige drivere for håndteringen/endringen

Støttespørsmål/indikatorspørsmål:

- Hvordan har dere evaluert og lært av tidligere hendelser og i hvilken grad har denne læringen vært relevant?
- Hvordan har næringen samarbeidet, og har dette endret seg. Hvor viktig har dette vært, og hvorfor?
- Hvordan bruker der informasjon og data fra tidligere hendelser til å forbedre egen respons.
- Hvordan sikre at man har rett kompetanse på tvers av organisasjonene, felles kurs etc.

Vi har så langt vært innom 4 forhold som er viktig for at en organisasjon kan ha en «resilient» ytelse (respondere, overvåke, forutse og lære). Hvilke av disse 4 mener du er eller har vært viktigst for at dere har hatt eller ikke hatt en «resilient» ytelse (robust), og hvorfor?

Oppsummering og avslutning

- Har du noen utfyllende kommentarer eller andre refleksjoner om det vi har vært gjennom?
- Er det andre aktører eller potensielle informanter/virksomheter jeg bør kontakte?

9.2. Samtykke

Samtykke for behandling av personopplysninger i forskningsprosjekt

Vil du delta i forskningsprosjektet

Hvilke egenskaper ved operatørenes håndtering av dronetrussel høsten 2022 har bidratt til en «resilient» håndtering

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvordan operatørselskapene har håndtert dronetrussel som oppstod høsten 2022. I studien skal jeg identifisere drivere for håndteringen, og analyser funn opp mot teori som sier noe om elementer som bør være til stede for å ha en «resilient» ytelse.

I dette skrivet gir jeg deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg. Bakgrunn for studien er en observasjon over flere år av at de ulike sikringsdisiplinene har en ulik tilnærming til sikring. Myndigheter, beste praksis, og et komplekst trusselbilde peker på behov for en helhetlig tilnærming. Det kan derfor være nyttig å operasjonalisere dette.

Formål

Prosjektet inngår i en masteroppgave i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger.

Resultat av studien vil brukes i en masteroppgave, men kan også bli kommunisert som en presentasjon på konferanse avhengig av hvilke funn og resultat studien gir.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Du får spørsmål om å delta fordi du har eller hatt en rolle i håndtering av dronetrussel i ditt selskap. Datainnsamling i prosjektet foregår ved personlige intervjuer med et utvalg personer

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det at du deltar på et intervju av ca en times varighet. Intervjuet vil foregå såkalt «semistrukturert», det vil si at du får anledning til å fortelle om og utdype din erfaring.

Intervjuet vil følge en intervjuguide, som er en mal for tema og aktuelle spørsmål. Denne vil sendes ut i forkant av intervjuet. Spørsmålene omhandler din egen og din virksomhets erfaring med håndtering av dronetrussel. Jeg vil ta lydopptak og notater fra intervjuet.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Personopplysninger inkluderer kontaktinformasjon (navn, e-post, telefonnummer) som benyttes for å opprette kontakt og avtale tid for intervju. Øvrig informasjon og opplysninger som fremkommer i intervjuet vil anonymiseres, det vil si at ditt navn og kontaktinformasjon erstattes med en kode som lagres på en egen navneliste adskilt fra øvrige data. Opplysninger vil kun være tilgjengelig for student (Tommy Hansen) og veileder ved Universitetet i Stavanger. I masteroppgaven vil alle data og opplysninger som har fremkommet i intervjuene være anonymisert, slik at det ikke vil være mulig å knytte noen utsagn til hverken enkeltperson eller enkeltvirksomhet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Prosjektet skal etter planen avsluttes oktober 2023. All informasjon som er innhentet vil slettes ved prosjektslutt.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

innsyn i hvilke personopplysninger som er registrert om deg,

- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet)
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Stavanger har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan du finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Universitetet i Stavanger ved student Tommy Hansen, XXXXX

- Universitetet i Stavanger ved XXXXXXXX
- Vårt personvernombud kan nåes på epost: personvernombud@uis.no
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17.

Med vennlig hilsen

Tommy B Hansen

Student

Samtykkeerklæring

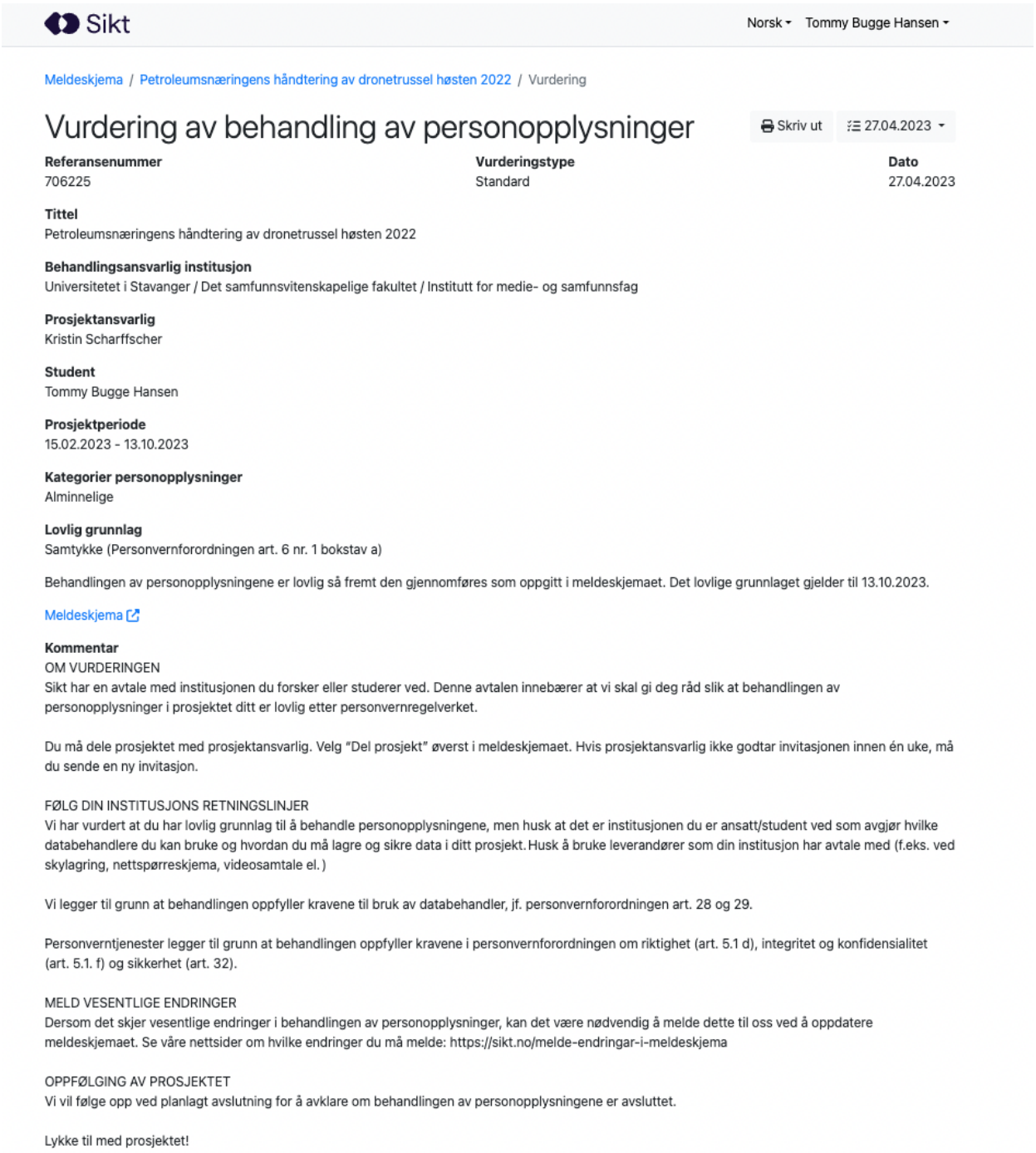
Jeg har mottatt og forstått informasjon om prosjektet og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju
- ☐ at personopplysninger kan oppbevares som beskrevet
- ☐ at data og informasjon som fremkommer i intervjuet kan sammenstilles, analyseres og benyttes i masteroppgaven i anonymisert form
- ☐ at mine opplysninger behandles frem til prosjektet er avslutt
- ☐ at det gjennomføres lydopptak
- ☐ Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

(Signert av prosjektdeltaker, dato)

Samtykkeerklæringen kan signeres skriftlig og returneres fysisk, eller ved skriftlig samtykke på e-post.

9.2.1. Godkjenning fra NSD



Sikt

Norsk ▾ Tommy Bugge Hansen ▾

Meldeskjema / Petroleumsnæringens håndtering av dronetrussel høsten 2022 / Vurdering

Vurdering av behandling av personopplysninger

Skriv ut | 27.04.2023 ▾

Referansenummer
706225

Vurderingstype
Standard

Dato
27.04.2023

Tittel
Petroleumsnæringens håndtering av dronetrussel høsten 2022

Behandlingsansvarlig institusjon
Universitetet i Stavanger / Det samfunnsvitenskapelige fakultet / Institutt for medie- og samfunnsfag

Prosjektansvarlig
Kristin Scharffscher

Student
Tommy Bugge Hansen

Prosjektperiode
15.02.2023 - 13.10.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 13.10.2023.

Meldeskjema

Kommentar
OM VURDERINGEN
Sikt har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

Du må dele prosjektet med prosjektansvarlig. Velg "Del prosjekt" øverst i meldeskjemaet. Hvis prosjektansvarlig ikke godtar invitasjonen innen én uke, må du sende en ny invitasjon.

FØLG DIN INSTITUSJONS RETNINGSLINJER
Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandører som din institusjon har avtale med (f.eks. ved skylagring, nettspørreskjema, videosamtale el.)

Vi legger til grunn at behandlingen oppfyller kravene til bruk av databehandler, jf. personvernforordningen art. 28 og 29.

Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Se våre nettsider om hvilke endringer du må melde: https://sikt.no/melde-endringar-i-meldeskjema

OPPFØLGING AV PROSJEKTET
Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!