UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Vår 2022

FORFATTER: Eivind Skare

VEILEDER: Sissel Haugdal Jore

TITTEL PÅ MASTEROPPGAVE:

Norsk petroleumssektor, rolleforståelse og hybride trusler – kan Resilience Engineering være en hensiktsmessig tilnærming?

EMNEORD/STIKKORD:

Hybride trusler, Sammensatte trusler, Rolleforståelse, Resilience Engineering, Samfunnssikkerhet

SIDETALL: 116 totalt, inkludert 22 sider vedlegg, forside og annet.

STAVANGER, 16. mai 2022

DATO/ÅR

Sammendrag

Hybride trusler er et begrep som er vanskelig å definere og avgrense nøyaktig. Likevel er det liten tvil om at komplekse, sammensatte trusler som rettes mot et bredt spekter av samfunnsfunksjoner kan påvirke og ramme både stats- og samfunnssikkerhet, viktige sektorer og enkeltvirksomheter.

Norsk petroleumsvirksomhet har stor betydning, både i kraft av å være en vesentlig bidragsyter til norsk økonomi, men også i forhold til energileveranse og -sikkerhet for andre nasjonalstater. Hvordan petroleumssektoren oppfatter sin egen rolle i forhold til et hybrid trusselscenario, og i hvilken grad virksomhetene kan legge til rette for å opprettholde sine aktiviteter og drift under slike krevende og komplekse betingelser, danner utgangspunkt for denne studien.

Studien er både basert på en empirisk del, der data er samlet inn gjennom informantintervjuer med et representativt utvalg personer fra norsk petroleumsvirksomhet. Disse empiriske dataene benyttes som grunnlag for å beskrive og drøfte hvilken oppfatning sektoren har av hybride trusler, og hvordan de ser sin egen rolle. Studien er videre teoriutforskende; de empiriske dataene drøftes og vurderes i forhold til det teoretiske Resilience Engineering-perspektivet og virksomhetenes evne til å opptre på en resilient måte beskrives ut fra dette perspektivet. Videre drøftes rolleforståelsens betydning for virksomhetenes evne til å opptre på en resilient måte ut fra organisasjonsteori, og hvilke premisser som ligger til grunn i Resilience Engineering-perspektivet.

Studien gir to primære konklusjoner: Virksomhetene i petroleumssektoren tar bare i liten grad hensyn til betydningen av komplekse og sammensatte sektoroverskridende trusler og trusler på samfunnsnivå. I stedet fokuserer de på å beskytte sin egen virksomhet mot enkelthendelser. Større trusler som er rettet mot sektor- eller samfunnsnivået oppfattes som myndighetenes ansvar, og virksomheter i petroleumssektoren vil ikke ta på seg en rolle eller ansvar her.

Dersom petroleumssektorens rolle i samfunnssikkerhet begrenses til å kun omfatte deres evne til å opprettholde normal drift, forutsetter det at sikkerhetsmyndighetene i større grad må dele konkret informasjon om hvilke potensielle indikatorer som har betydning og gir mening for virksomhetene å overvåke i forhold til egen funksjonsevne og -tilstand. Et ansvar og en rolle for samfunnssikkerhet som går ut over dette krever at det reguleres mer spesifikt gjennom lovverket.

Forord

Denne oppgaven representerer avslutningen på det erfaringsbaserte Masterstudiet i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger. Selv om det har vært krevende å finne ballansen mellom arbeidet med oppgaven og jobb, familie og privatliv, er jeg utrolig glad for å ha fått anledning til å bruke tid, fokusere og sette meg inn i en så spennende og omfattende tematikk. Det har vært bratte læringskurver og til tider har jeg følt at jeg vekslet mellom å gå i sirkel og å stange hodet i veggen. Det har likevel vært utrolig motiverende å se hvordan oppgaven har tatt form, fra en vag idé i begynnelsen til den fullstendige oppgaven jeg nå holder i hendene.

Jeg vil takke min veileder Sissel Haugdal Jore for alle råd, innspill og anbefalinger. Din evne til å peke meg i riktig retning har hatt stor betydning for oppgaven, men også gitt meg motivasjon til å grave litt ekstra i faglitteraturen og sette meg inn i temaer som jeg hadde lite kunnskap om på forhånd. Jeg må også rette en stor takk til alle informantene som har stilt til intervju og bidratt med sine betraktninger, innsikt og kompetanse. Uten dere ville ikke denne oppgaven vært mulig å skrive!

Til slutt må jeg rette en stor takk til Maren og Ulrik som har holdt ut mens jeg har tilbrakt lange dager og netter foran pc'en. Nå blir det endelig tid til å finne på noe sammen igjen!

Eivind Skare

Stavanger, 15.05.2022

Innholdsfortegnelse

Liste over figurer og tabeller

1. Innledning

Bakgrunn

Torsdag 24. februar 2022 rykket russiske styrker over grensen til Ukraina og innledet dermed de største krigshandlingene vi har sett i Europa i nyere tid. I dagene og ukene som fulgte invasjonen ble det innført stadig strengere sanksjoner mot Russland, og det ble advart om at også norske bedrifter og interesser kunne rammes av russiske gjengjeldelser (Sveen, 2022). I lys av denne nye sikkerhetspolitiske situasjonen i Europa og Norge har begrepet «hybride trusler» fått stor oppmerksomhet.

Men begrepene «hybride trusler» og «hybrid krigføring» er ikke nye. De siste årene er disse blitt mer og mer brukt i akademiske, forsvars- og politiske kretser, og ikke minst i media. Spesielt etter Russlands annektering av Krimhalvøya i 2014 har bruken av begrepene økt (Reichborn-Kjennerud og Cullen, 2016). Til tross for dette eksisterer det fremdeles ikke en entydig klar og omforent definisjon på hva begrepene innebærer (Reichborn-Kjennerud og Cullen, 2016, Cullen og Wegge, 2019). Noen særegne kjennetegn går riktignok igjen: Begrepene beskriver hvordan en trusselaktør vil søke å oppnå sine mål ved å true med eller å aktivt bruke en kombinasjon av politiske, militære, sivile, informasjonsrettede og økonomiske maktmidler. Som oftest gjennom en lang rekke og et bredt spekter av koordinerte og synkroniserte tiltak og virkemidler som hver for seg kan oppfattes som selvstendige hendelser, men som likevel til sammen kan gi stor effekt i forhold til å oppnå det gitte målet (Reichborn-Kjennerud og Cullen, 2016). Trusselaktørene har med andre ord en intensjon om å utføre en tilsiktet handling som kan utnytte og ramme sårbarheter og skape uro på tvers av samfunnet (Cullen og Wegge, 2019).

Til tross for at hybride trusler altså involverer et sterkt element av maktbruk eller trussel om maktbruk (Reichborn-Kjennerud og Cullen, 2016), er det likevel i trusselaktørens interesse å holde konfliktnivået lavt og dermed gjøre det mulig å utnytte gråsonen mellom en åpen konflikt og tradisjonell politisk interaksjon (Cullen, 2018, Cullen og Wegge, 2019). Denne effekten kan oppnås ved å spre virkemidlene over et bredt spekter av virksomheter og næringer, både offentlige og private, og hybride trusler kan dermed også betraktes som grense- eller sektorovergripende problemer (Cullen og Wegge, 2019). Fordi hybride trusler kan ramme på tvers av sektorer, nivåer og domener, vil «evnen til å vedlikeholde et samordnet nasjonalt situasjonsbilde som fanger opp og setter hendelser i sammenheng» (Nasjonal

sikkerhetsmyndighet, 2021a, s. 9) være spesielt utfordrende. I publikasjonen «Støtte og samarbeid - En beskrivelse av totalforsvaret i dag» (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018) beskrives betydningen av begrepet hybride trusler slik: «Begrepet har kanskje sin fremste verdi i å øke bevisstheten om hvordan aktører kan påvirke gjennom en kombinasjon av åpenlyse og fordekte militære og ikke-militære virkemidler» (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018, s. 14).

Hybride trusler kan altså påvirke og ramme både offentlige myndigheter og private virksomheter. For å kartlegge og sette søkelys på norsk næringslivs eksponering for og forståelse av hybride trusler gjennomførte Opinion AS en undersøkelse på vegne av Næringslivets sikkerhetsråd i 2018 (Næringslivets sikkerhetsråd, 2019). Denne undersøkelsen peker på at heller ikke næringslivet har tilstrekkelige kapasiteter eller forutsetninger til å oppdage og avdekke hybride trusler eller se de i sammenheng. Videre fremhever et flertall av virksomhetene i Hybridundersøkelsen at de anser seg som et potensielt mål for hybride trusler, basert på virksomhetenes posisjon og funksjon i samfunnet (Næringslivets sikkerhetsråd, 2019).

Tidligere forsvarssjef Admiral Haakon Bruun-Hanssen har også pekt på dette som en av hovedutfordringene i fremtidige hybride trusselscenarier: «Håndteringen av enkelthendelser vil først og fremst foregå sektorvis og gjerne på lavere nivå. Hovedutfordringene er derfor å oppdage, forstå og attribuere eventuell hybrid virkemiddelbruk og vurdere sammenhenger og intensjon. Det er et behov for å forbedre evnen til tverrsektoriell situasjonsforståelse, informasjonsflyt og samarbeidsmekanismer.» (Forsvaret, 2019, s.83).

Bernhard Christoffer Caspari peker i sin masteroppgave (Caspari, 2021) på nødvendigheten av at forskning også beskriver hvilken rolle private virksomheter ser for seg å ha i forhold til hybride trusler, samt hva virksomhetene forventer av myndighetene. Caspari (2021) fremhever videre hvordan statsapparatet er fragmentert i sitt syn på hybride trusler, og hvordan dette påvirker etableringen av en felles situasjonsforståelse. Stian Schnelle (2018) peker i tillegg på at en trusselaktør nettopp kan ønske å påvirke motstanderens situasjonsforståelse, for å dermed bidra til usikkerheten og gjøre det utfordrende å forstå hvorvidt det faktisk pågår et angrep eller ikke – og hvem som eventuelt står bak angrepet.

Hybride trusler innebærer altså stor grad av usikkerhet, både i forhold trusselaktørens mål og virkemiddelbruk, men også i forhold til hvordan en skal forsvare og beskytte seg mot slike

trusler. Hvordan roller og ansvar oppfattes er derfor interessant å studere, ikke bare fra et offentlig- eller myndighetspespektiv, men også fra næringslivets side. Norsk petroleumsvirksomhet er i denne sammenhengen spesielt interessant, både på grunn av petroleumssektorens betydning for Norge og hvordan den er avhengig av og tett knyttet til andre sektorer, men også på grunn av det høye skade- og risikopotensialet som petroleumsvirksomhet kan innebære.

Også Politiets sikkerhetstjeneste (PST) vurderer at norsk petroleumssektor blir utsatt for og er sårbar for trusler fra utenlandsk etterretning (Politiets sikkerhetstjeneste, 2020). Spesielt fremheves hvordan informasjon om teknologi, norske myndigheters strategi og økonomiske forhold innhentes, samt hvordan infrastruktur kartlegges. Det vises til hvordan denne informasjonen kan utnyttes og at skadepotensialet for Norge er både stort og langsiktig, «både militært, økonomisk og for nasjonal sikkerhet» (Politiets sikkerhetstjeneste, 2020, s. 3). Det er derfor interessant å studere hvordan olje- og gasselskaper på norsk sokkel oppfatter sin rolle i forhold til å håndtere hendelser knyttet til hybride trusselscenarier.

Sikkerhetsloven

Hvordan olje- og gasselskaper på norsk sokkel oppfatter sin rolle må også forstås på bakgrunn av det gjeldende lovverket. I denne sammenhengen er sikkerhetsloven av spesiell interesse. For å styrke det helhetlige sikkerhetsarbeidet i Norge og regulere hvordan sikkerhetstruende virksomhet skal forebygges, avdekkes og motvirkes trådte «Lov om nasjonal sikkerhet» (sikkerhetsloven, 2019) i kraft 1. januar 2019. Loven regulerer hvordan grunnleggende nasjonale funksjoner og skjermingsverdige verdier beskyttes (Nasjonal sikkerhetsmyndighet, 2021a). Dette gjelder verdier som finnes «på tvers av sektorene og i form av samfunnsfunksjoner, virksomheter, infrastrukturer og systemer» (Nasjonal sikkerhetsmyndighet, 2021a, s. 15), men det er likevel et dillemma at en trusselaktørs mål ikke nødvendigvis samsvarer med den nasjonale trussel- og verdivurderingen, og derfor også kan ramme virksomheter som ikke er underlagt sikkerhetsloven (Nasjonal sikkerhetsmyndighet, 2021a). Spesielt i forhold til hybride trusler, som kan ramme virksomheter i alle sektorer og utnytte svakheter på tvers av hele samfunnet, kan det altså være krevende å regulere sikkerhetsnivået gjennom sikkerhetsloven.

Sikkerhetsloven stiller krav til forebygging, avdekking og motvirkning av sikkerhetstruende virksomhet mot grunnleggende nasjonale funksjoner (Sikkerhetsloven, 2019). Her er sikkerhetstruende virksomhet definert som «tilsiktede handlinger som direkte eller indirekte

kan skade nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 2019, § 1-5). Med nasjonale sikkerhetsinteresser menes: «landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til:

a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet
b) forsvar, sikkerhet og beredskap
c) forholdet til andre stater og internasjonale organisasjoner
d) økonomisk stabilitet og handlefrihet
e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet»

Som en stor internasjonal oljeprodusent, og viktig leverandør av gass til Europa, er det naturlig å relatere norsk petroleumsvirksomhet til sikkerhetsloven og definisjonen over. Primært gjennom Norges sikkerhetspolitiske interesser knyttet til «økonomisk stabilitet og handlefrihet», men også i noen grad gjennom «forholdet til andre stater og internasjonale organisasjoner».

«Beskyttelse av norsk petroleumsvirksomhet mot sikkerhetstruende virksomhet» er pr. 15. oktober 2021 innmeldt som en av 42 grunnleggende nasjonale funksjoner (Nasjonal sikkerhetsmyndighet, 2021b). Sikkerhetsloven definerer grunnleggende nasjonale funksjoner som: «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 2019, § 1-5).

I Prop. 153 L (2016-2017) kommer det frem en forventning om at alle virksomheter som er underlagt sikkerhetsloven skal foreta risikovurderinger som grunnlag for å etablere de tiltakene som er nødvendig for å opprettholde et forsvarlig sikkerhetsnivå i virksomheten. I tillegg har også virksomhetene en plikt til å varsle om sikkerhetstruende virksomhet.

Sikkerhetsloven er med andre ord utformet som en funksjonell lov. Det vil si at loven ikke peker på konkrete sikkerhetskrav, men at de funksjoner og virksomheter som er underlagt loven har selvstendig ansvar for å oppnå et forsvarlig sikringsnivå. Dette innebærer at risikovurderinger og forebyggende tiltak må kontinuerlig vurderes og holdes oppdatert for å kunne avgjøre hva som til enhver tid er et forsvarlig sikringsnivå. Gjennom å stille funksjonelle krav til sikkerhetstiltak tar sikkerhetsloven altså utgangspunkt i at den enkelte virksomhet har ansvar for sikkerheten (Prop. 153 L (2016-2017), s. 8). Dette er på linje med

hvordan det sektorspesifike lovverket er utformet i petroleumssektoren, for eksempel representert ved «Lov om petroleumsvirksomhet» (petroleumsloven, 1996). I forhold til hybride trusler er petroleumslovens § 9-3 av spesiell betydning, da denne omhandler beredskap mot bevisste anslag.

Problemstilling

Mye av den eksisterende forskningen rundt hybride trusler og deres betydning dreier seg rundt betraktninger om stats- og samfunnssikkerhet. Men som det beskrives over, legger blant annet sikkerhetsloven opp til at også enkeltvirksomheter kan ha en rolle og et ansvar i et samfunnsikkerhetsperpektiv. Det vil derfor være interessant å betrakte hybride trusler fra næringslivets perspektiv. Som det er vist til tidligere, uttrykker Caspari (2021) at det nettopp er et behov for å beskrive hvilken rolle private virksomheter ser for seg å ha i forhold til hybride trusler, samt hva disse virksomhetene forventer av myndighetene. Jeg anser petroleumssektoren som spesielt interessant i denne sammenhengen, da de nåværende omstendighetene i Europa har gjort det tydelig at energi og energileveranse også er effektive virkemidler i en spisset sikkerhetspolitisk situasjon. Krigen i Ukraina danner et dystert bakteppe, men gjør tematikken i denne oppgaven desto mer aktuell og relevant.

Gjennom arbeidet med denne oppgaven ønsker jeg å øke bevisstheten om hvordan trusselaktører kan påvirke samfunnet, og altså spesielt norsk olje- og gassvirksomhet. Jeg vil gjøre det gjennom å analysere hvordan olje- og gasselskaper oppfatter sin rolle i forhold til å identifisere og håndtere hybride trusler, og hvordan bevissthet rundt hybride trusler kan bidra til å opprettholde normal funksjonalitet og drift i sektoren under de krevende og skiftende omstendighetene som et hybrid trusselscenario representerer.

Olje- og gasselskapenes oppfatning av hybride trusler påvirker også virksomhetenes forståelse av sine roller i et hybrid trusselscenario. Hvorvidt dette påvirker deres evne til å opprettholde normal funksjonalitet og drift, leder til følgende problemstilling:

> *Hvilken betydning har rolleforståelse for hvordan norske olje- og gasselskaper kan legge til rette for å fungere på en resilient måte i et hybrid trusselscenario?*

Begrepet *rolleforståelse* peker her på ansvar og oppgaver som virksomheter i norsk petroleumssektor oppfatter og forstår at de har, eller eventuelt oppfatter at de *ikke* har, i forhold til å kunne operere på en sikker måte og bidra til samfunnets sikkerhet i et hybrid

trusselscenario. Dette innebærer dermed at det kan være ulike oppfatninger knyttet til hva som er forventet av petroleumssektoren, og er bakgrunnen for valg av fokus på rolleforståelse.

Valg av teoretiske perspektiv

Problemstillingen er valgt og formulert ut fra et ønske og motivasjon om å utvikle en dypere forståelse og innsikt i tematikken. Men for å kunne gå i dybden er det først viktig å kartlegge hvilken oppfatning norske olje- og gasselskaper har av hybride trusler, og hvordan denne oppfatningen kan ses i forhold til eksisterende forskning innen temaet. Dette legger videre grunnlag for å kunne forstå hva hybride trusler betyr for norske olje- og gasselskapers evne til å kunne opprettholde sin normale funksjonalitet og drift i et slikt scenario.

For å nettopp kunne forstå og beskrive hvordan olje- og gasselskaper oppfatter sin evne til å opprettholde og eventuelt gjenopprette normal funksjonalitet og drift i et hybrid trusselscenario tar jeg utgangspunkt i det teoretiske perspektivet «Resilience Engineering» (Hollnagel, Woods og Leveson, 2006). Dette perspektivet fokuserer på hvordan organisasjoner kan legge til rette for å kunne håndtere og operere under både kjent og ukjent kompleksitet i krevende omstendigheter (Woods og Hollnagel, 2006, s. 6).

Resilience Engineering-perspektivet tar utgangspunkt i hvordan en organisasjon, og menneskene som utgjør organisasjonen, utfører sine oppgaver for å oppnå de forventningene som stilles til organisasjonen. Det vil derfor være interessant å også vurdere dette teoretiske perspektivet i forhold til et hybrid trusselscenario, som kan betraktes som en sektoroverskridende- og samfunnsmessig trussel, og ikke bare noe som har betydning på et individ- og organisasjonsnivå. Spesielt er dette interessant i forhold til hvordan ansvar og oppgaver kan oppfattes og forstås i et hybrid trusselscenario. Hollnagel (2018, s. 17) viser til hvordan en organisasjon styres gjennom å tildele ulike roller og funksjoner til ulike deler av organisasjonen, men også at ytre omgivelser og organisasjonen selv påvirker hvordan roller og funksjoner oppfattes, og hvordan oppgaver og aktiviteter utføres (Hollnagel, 2018, s. 20).

For å kunne utdype hvilken betydning olje- og gasselskapers rolleforståelse knyttet til hybride trusselscenarier kan ha i Resilience Engineering-perspektivet, vil jeg også betrakte rolleforståelse med utgangspunkt i to ulike perspektiver hentet fra organisasjonsteori: det instrumentelle perspektivet og det institusjonelle perspektivet. Det instrumentelle perspektivet beskriver hvordan formelle organisasjonsstrukturer kan bidra til at hendelser håndteres effektivt (Andreassen og Bjørkelo, 2020), mens det institusjonelle perspektivet knyttes til

kulturelle og symbolske handlinger i organisasjonene (Andreassen og Bjørkelo, 2020). Ved å betrakte rolleforståelsen i olje- og gasselskaper fra ulike perspektiver, kan flere aspekter belyses og forstås.

Forskningsspørsmål

For å kunne utdype og besvare spørsmålet som stilles i problemstillingen, kreves det både utforskning av teori og innsamling av empiriske data for å kunne belyse sammenhenger. Oppgaven er altså både teoriutforskende og empirisk, noe som kommer til uttrykk i følgende tre forskningsspørsmål:

1. *Hvilke utfordringer oppfatter olje- og gasselskapene at hybride trusler representerer, både for dem selv spesielt og for sektoren generelt?*
2. *Er utfordringene av en slik art at Resilience Engineering-perspektivet kan være en hensiktsmessig tilnærming?*
3. *Kan olje- og gasselskapers eventuelle utfordringer i forhold til å kunne fungere på en resilient måte i et hybrid trusselscenario forklares ut fra hvordan deres rolleforståelse kan beskrives?*

Det første forskningsspørsmålet er av empirisk art, og for å kunne besvare dette er det samlet inn empiriske data gjennom informantintervjuer med et utvalg personer tilknyttet norsk petroleumsvirksomhet. Disse har alle relevante funksjoner og ansvar i sine respektive virksomheter i forhold til oppgavens tematikk og problemstilling. De valgte teoretiske perspektivene har dannet grunnlag for utforming av spørsmål i intervjuene. I tillegg er det formulert et case som omfatter hybride trusler sett i forhold til petroleumsaktivitet i Barentshavet. Dette caset er kun benyttet som grunnlag for utvelgelse av informanter, og for å gjøre det enklere for informantene å gi konkrete eksempler i forhold til tematikken.

De to neste forskningsspørsmålene er av mer teoretisk art. Gjennom å besvare disse forskningsspørsmålene vil det empiriske datagrunnlaget kunne tolkes og forstås på bakgrunn av relevante teoretiske perspektiver. De vil også bidra til å belyse eventuelle kunnskapshull. Til sammen vil de tre forskningsspørsmålene også bidra til å strukturere og avgrense forskningsstudien.

Avgrensninger og presiseringer

Norsk petroleumsvirksomhet har i dag et stort omfang og inkluderer både offentlige og private virksomheter i flere sektorer. Bare innenfor petroleumssektoren finnes det et stort spekter av virksomheter, for eksempel operatørselskapene[1] som har ansvar for utforskning, utvikling og utvinning av petroleumsforekomster, leverandørselskaper som leverer tjenester til operatørselskapene, virksomheter med ansvar for drift og vedlikehold av infrastruktur, og offentlige tilsynsmyndigheter som har ansvar for å føre tilsyn med at aktivitetene som utføres i sektoren skjer forvarlig og i tråd med gjeldende lovregulering. I tillegg er det en lang rekke aktører innen tilgrensende sektorer som bidrar til norsk petroleumsvirksomhet, for eksempel innen IT, finans, luftfart, maritim sektor og transport. Det totale bildet av norsk petroleumssektor er altså meget omfattende, så det er derfor nødvendig å avgrense studiet til å omhandle et utvalg.

På grunn av den sentrale plassen i verdikjeden i norsk petroleumsaktivitet, har jeg valgt å avgrense studiet til å kun fokusere på operatørselskaper. Jeg har valgt middels store operatørselskaper som enten allerede er eller vil bli operatør for produserende felt og innstallasjoner i nær fremtid. I tillegg inkluderer jeg informanter fra to offentlige tilsynsmyndigheter med tilknytning til norsk petroleumsaktivitet. Disse vil kunne bidra med større oversikt og vil kunne se helheten i petroleumssektoren på en annen måte enn det de enkelte operatørselskapene er i stand til. Dette er et begrenset utvalg, men like fullt representerer de ansvarsområder innenfor norsk petroleumsvirksomhet som vil være svært relevante i forhold til oppgavens tema og problemstilling.

Hybride trusler er et begrep som er vanskelig å definere og beskrive, og selve begrepsbruken er omdiskutert. Min forståelse og oppfatning av begrepet bidrar til å prege oppgavens utforming, prioriteringer og fokusområder, og vil derfor kunne kritiseres. Spesielt har jeg valgt å så langt som mulig bruke begrepet «hybride trusler» fremfor «sammensatte trusler», som er en annen vanlig betegnelse på det samme fenomenet. Jeg har valgt å gjøre dette for å være konsekvent i begrepsbruken og unngå ytterligere begrepsforvirring, ikke fordi jeg mener at dette begrepet nødvendigvis er best eller mest beskrivende.

[1] Et operatørselskap er et selskap som har blitt tildelt rettigheter til å lete etter olje og gass i en blokk eller en lisens på norsk sokkel, og å bygge ut og produsere olje og/eller gass ved et eventuelt kommersielt drivverdig funn. Operatørselskapet opptrer og driver lisensen på vegne av et partnerskap av selskaper.

Oppgavens oppbygging

I oppgavens kapittel 1 er bakgrunnen og motivasjonen for den valgte problemstillingen presentert. For å kunne utdype og svare på problemstillingen er det nødvendig å etablere et teoretisk grunnlag: Kapittel 2 fokuserer på begrepsavklaring og å gi en oversikt over hvordan hybride trusler kan defineres, eller med andre ord hvordan begrepet kan gis mening og innhold, og settes inn i oppgavens kontekst. Videre introduseres Resilience Engineering-perspektivet som teoretisk grunnlag for å kunne forstå og beskrive hvordan olje- og gasselskaper oppfatter sin evne til å opprettholde og eventuelt gjenopprette normal funksjonalitet og drift i et hybrid trusselscenario. Dette er valgt som det primære teoretiske perspektivet for å kunne besvare forskningsspørsmålene og problemstillingen. Også rolleforståelsens betydning i Resilience Engineering-perspektivet beskrives, og i tillegg introduseres to ulike organisasjonsteoretiske perspektiver på rolle og rolleforståelse.

I kapittel 3 redegjøres det for metodevalg og forskningsstrategi. Forskningsstudiets utforming og gjennomføring presenteres, og utfordringer jeg har støtt på og valg som er gjort underveis beskrives og forklares. Betraktninger rundt validitet, reliabilitet og etiske hensyn og utfordringer gir grunnlag for at leseren skal oppnå større forståelse for forskningen som presenteres i oppgaven.

Det empiriske datagrunnlaget som er samlet inn og funn som er gjort presenteres i kapittel 4, før funnene drøftes på bakgrunn av det tidligere presenterte teorigrunnlaget i kapittel 5. Til slutt, i kapittel 6, trekkes hovedlinjene sammen og konklusjoner presenteres. Her legges det også frem forslag til hvordan videre forskning kan bidra til økt forståelse for temaet.

2. Teorigrunnlag

Det teoretiske grunnlaget som presenteres i dette kapitlet omhandler først hvordan begrepet «hybride trusler» kan forstås og gis innhold. Videre presenteres Resilience Engineering som teoretisk perspektiv, samt ulike perspektiver på hvordan roller kan beskrives og forstås i en organisasjon. Til sammen vil dette danne et teoretisk grunnlag for å besvare forskningsspørsmålene og problemstillingen som ble presentert i forrige kapittel.

Hva hybride trusler *er* og hva de *ikke* er?

Begrepet «hybride trusler» er mye brukt, men det eksisterer fremdeles ikke en entydig klar og omforent definisjon på hva dette begrepet innebærer (Reichborn-Kjennerud og Cullen, 2016, Cullen og Wegge, 2019).

Betydningen av ordet «hybrid» peker på et fenomen som er satt sammen eller kombinert av flere elementer med tilsynelatende ulike og mangfoldige opphav. Malerud, Hennum og Toverød (2021) velger å oversette begrepet «hybride trusler» til «sammensatte trusler», men veksler likevel mellom de to begrepene. I denne oppgaven benyttes benevningen «hybride trusler» så langt det er mulig for å unngå begrepsforvirring. Trussel kan i denne sammenhengen forstås som en risikokilde, som enten er varslet eller kan oppfattes som en intensjon om å angripe og ramme en gitt verdi (Society for Risk Analysis, 2018). Malerud, Hennum og Toverød (2021) beskriver trussel som hvordan en trusselaktørs formål, metode, fremgangsmåte og virkemiddel er satt sammen for å ramme et mål. Hybride trusler oppstår altså når en aktør har som formål og intensjon å oppnå et overordnet strategisk mål gjennom å kombinere ulike virkemidler.

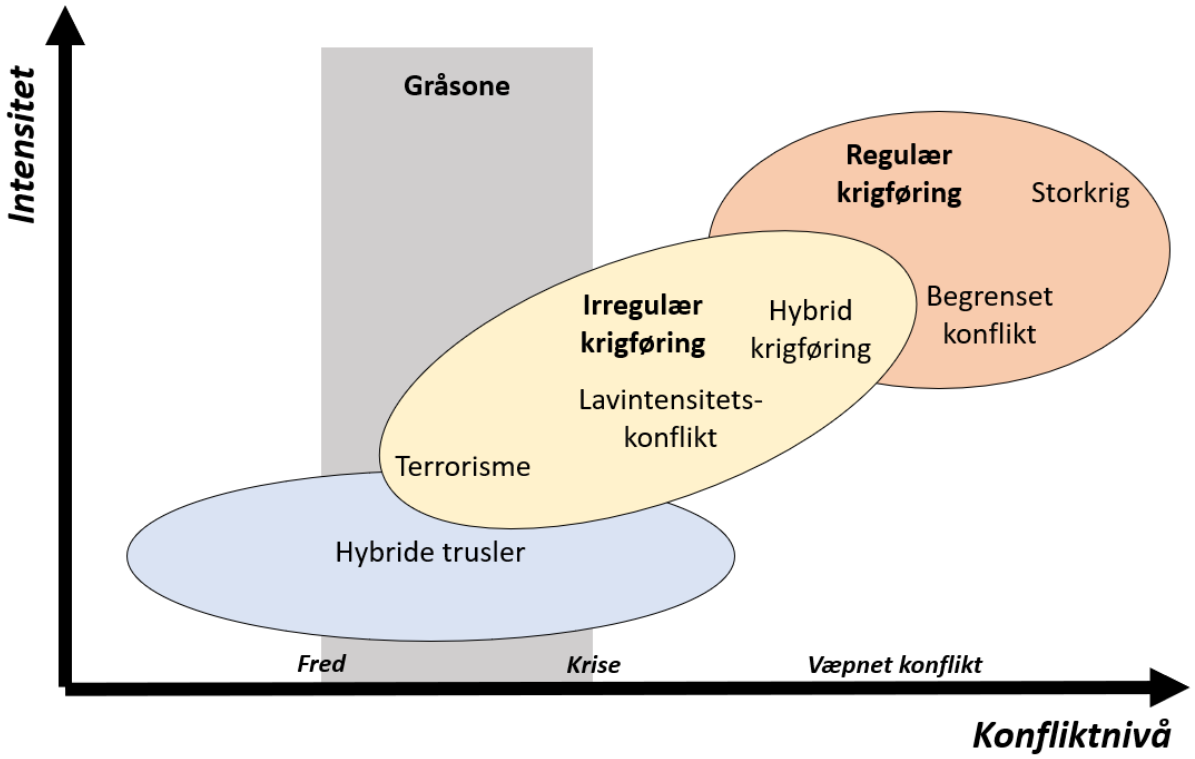
Et hybrid trusselscenario kan videre forstås ved at en trusselaktør søker å oppnå for eksempel militære, politiske, økonomiske, samfunnsmessige og/eller informasjonsrelaterte mål (Malerud et al., 2021) gjennom et bredt spekter av koordinerte og synkroniserte maktmidler, tiltak og virkemidler. Disse kan hver for seg oppfattes som selvstendige hendelser, men likevel er de utformet for å kunne forsterke hverandre og gi synergieffekter i forhold til å oppnå det gitte målet (Reichborn-Kjennerud og Cullen, 2016, Malerud et al., 2021). I Malerud et al. (2021) konkretiseres hybride trusler som «synkronisert bruk av ulike maktmidler for å ramme spesifikke sårbarheter i hele bredden av samfunnsfunksjoner for å oppnå synergistiske effekter» (Malerud et al., 2021, s. 3).

Trusselaktørene har altså en underliggende motivasjon og intensjon om å utføre en tilsiktet handling som kan utnytte og ramme sårbarheter på tvers av samfunnet (Cullen og Wegge, 2019). Men til tross for at hybride trusler involverer et sterkt element av maktbruk eller trussel om maktbruk (Reichborn-Kjennerud og Cullen, 2016), vil det likevel være i trusselaktørens interesse å holde konfliktnivået lavt. Slik kan trusselaktøren utnytte det potensielle styringsvakumet som ligger i gråsonen mellom daglig virksomhet i fredstid og utvikling til en krisesituasjon (Cullen, 2018, Cullen og Wegge, 2019).

Malerud et al. (2021) peker likevel på at hybride trusler kan opptre i hele konfliktspekteret. Derfor vil det være hensiktsmessig å skille mellom og avklare noen ulike begreper som ofte benyttes om hverandre, som for eksempel hybrid krigføring, asymetrisk krigføring, lavintensitetskonflikter og altså hybride, eller sammensatte, trusler. Monaghan (2019) presiserer at det er et klart skille mellom hybride trusler og hybrid krigføring. Hybrid *krigføring* peker på selve virkemiddelbruken i en kompleks væpnet konfliktsituasjon, og innebærer altså bruk av sammensatte og sektorovergripende maktmidler i en konflikt som allerede har eskalert til å inkludere væpnet maktbruk. Hybride *trusler* derimot innebærer å utnytte skjulte maktmidler for å oppnå gitte mål og samtidig unngå en åpenlys konfliktsituasjon.

I Monaghan (2019) beskrives hybride trusler som: «the use of multiple, ambiguous means to target vulnerabilities across society to achieve goals gradually without triggering decisive responses» (Monaghan, 2019, s. 87). Dette skilller seg altså noe fra Malerud et al. (2021) sin beskrivelse, i det at Malerud påpeker at hybride trusler kan opptre i hele konfliktspekteret, altså inkludert åpne konflikter, mens Monaghan (2019) spesifikt peker på at målet oppnås gradvis, ved lav intensitet i virkemiddelbruken. Resultatet av Monaghans (2019) perspektiv er at eventuelle hendelser hver for seg ikke trenger å karakteriseres eller betraktes som en krise eller kriseutløsende faktor, men til sammen kan de utgjøre en betydelig trussel for virksomheter, sektorer eller samfunnet som helhet.

Figur 1 illustrerer hvordan konfliktnivå og intensitet utvikler seg fra fred til krise og væpnet konflikt. Hybride trusler opptrer her over et stort spekter av konfliktnivå, og typisk i gråsonen mellom krisesituasjoner og normale daglige aktiviteter i fredstilstand, og med et gjennomgående relativt sett lavt intensitetsnivå.



Figur 1 *Hybride trusler, konfliktnivå og intensitet.*

Modifisert fra Malerud et al. (2021) og basert på Monagham (2019).

Det er også mulig å argumentere for at hybride trusler skiller seg fra for eksempel hybrid krigføring ved at den førstnevnte primært utfordrer og påvirker samfunnsikkerheten, for eksempel gjennom å true funksjonsevnen til kritisk infrastruktur og andre kritiske samfunnsfunksjoner, mens den sistnevnte også utfordrer statssikkerheten (Malerud et al., 2021), som blant annet innebærer beskyttelse av landets suverenitet og territorielle integritet.

Cullen (2018) peker på at hybride trusler har et tvetydig og ofte unnvikende utrykk og forløp. De er med hensikt utformet slik for å kunne ramme et bredt spekter av samfunnsfunksjoner, og for å skjule det egentlige bakenforliggende formålet ved trusselen. Cullen (2018) argumenterer også for at hybride trusler kan betraktes som «wicked problems», i tråd med hvordan for eksempel Ritchey (2013) beskriver at wicked problems er dynamiske og at nye problemer ofte oppstår som en konsekvens av forsøk på å løse tidligere identifiserte problemer. Reichborn-Kjennerud og Cullen (2016) beskriver hvor krevende det kan være å definere når og hvor en hybrid trussel egentlig oppstår, og ikke minst når og hvor den opphører. At hybride trusler av natur er og tvetydige, og dermed krevende å fullt ut identifisere og forstå, bidrar til den kompleksiteten som ofte omfattes av et wicked problem.

Også det faktum at det ikke eksisterer en klar og entydig definisjon på hva som faktisk utgjør en hybrid trussel bidrar til at de er krevende å identifisere og forstå (Cullen, 2018).

Cullen og Wegge (2019) peker på at hybride trusler kan utnytte alle samfunnets maktinstrumenter, og angripe eller ramme alle sektorer i et samfunn. Når en lang rekke institusjoner kan være involvert og rammet av hybride trusler samtidig, kan hver av disse ha ulike oppfatninger og perspektiver på hva som utgjør den egentlige trusselen og det egentlige bakenforliggende problemet. Hvordan samfunnet håndterer hybride trusler vil altså påvirkes av og variere avhengig av institusjonenes ståsted, og det er ikke utenkelig at måten ulike samfunnsinstitusjoner velger å håndtere trusler på kan komme i konflikt med andre. Dette bidrar dermed til at også samfunnets håndtering av hybride trusler i noen tilfeller kan betraktes som et wicked problem (Fischbacher-Smith, 2016).

Også næringslivet rammes og påvirkes av hybride trusler og angrep. For eksempel ble det danske selskapet A.P. Møller-Mærsk hardt rammet av cyberangrepet og skadevaren NotPetya i 2017, med et tallfestet tap på mellom 200 og 300 millioner dollar som følge (Jørgenrud, 2017, Matthews, 2017). Selve spredningen av dataviruset NotPetya settes i sammenheng med konflikten i Donbasprovinsen øst i Ukraina, og Russiske myndigheter ble anklaget for å stå bak dataangrepet som en del av en hybrid kanpanje for å destabilisere Ukraina (Greenberg, 2018, Kovacs, 2018). A.P. Møller-Mærsk var altså ikke det egentlige målet for angrepet, men ble rammet som en tredjepart. Et annet eksempel er sabotasjen og angrepene mot en rekke tankskip i Omanbukta i mai og juni 2019, der en ukjent aktør utplasserte eksplosiver og miner nær skipenes vannlinje (Altaher og Westcott, 2019, Cotovio, Regan og Fox, 2019). To av de rammede skipene har tilknytning til norske rederier: Front Altar som tilhører det norskeide rederiet Frontline, og M/T Andrea Victory som tilhører bergensrederiet Champion Tankers AS. Etterforskningen av hendelsene pekte på at en statlig aktør stod bak, og flere har i ettertid pekt på Iran som den mest sansynlige aktøren (for eksempel BBC, 2019). Dette ses i sammenheng med den pågående lavintensitetskonflikten i regionen, med Iran og Saudi Arabia som de største aktørene. Selv om disse angrepene var direkte rettet mot en rekke tankskip og rederier, må en altså kunne anta at den bakenforliggende intensjonen primært var å ramme politiske, økonomiske og samfunnssikkerhetsmessige sårbarheter på tvers av regionen.

Dette er eksempler på at også privat næringsliv kan rammes av hybride trusler og angrep, både indirekte som en tredjepart, der et angrep opprinnelig var rettet mot andre instutisjoner,

og direkte gjennom å være leverandør av tjenester til en eller flere samfunnsfunksjoner som trusselaktøren ønsker å ramme.

Næringslivets sikkerhetsråds studie om hybride trusler rettet mot norsk næringsliv (Næringslivets sikkerhetsråd, 2019) peker på at det primært er to forhold som gjør virksomhetene sårbare for hybride trusler: 70% av respondentene svarer at manglende evne til å gjennkjenne påvirkningsforsøk kamuflert som andre henvendelser gjør dem sårbare, og 63% peker i tillegg på at manglende sikkerhetsbevissthet og trusselforståelse i organisasjonen gjør dem sårbare (Næringslivets sikkerhetsråd, 2019).

Ut fra dette fremgår det at næringslivet ikke nødvendigvis har tilstrekkelige kapasiteter eller forutsetninger til å oppdage og avdekke hybride trusler. I Hybridundersøkelsen kommer det også frem hvilke verdier norsk næringsliv først og fremst anser som truet i et hybrid trusselscenario. Disse er:

- Tap av konfidensiell informasjon (67%)
- Driftsforstyrrelser (58%)
- Tap av omdømme (56%)
- Tap av fremtidige forretningsmuligheter (29%)
- Påvirkning av politiske beslutningsprosesser (17%)
- Tap av utenlandske partnere og kunder (15%)

Det pekes altså på verdier som både er unike for de enkelte virksomhetene, og verdier som dekker en bredere sektor- eller samfunnsdimensjon.

Resilience Engineering

I et stadig mer komplekst risikobilde, slik for eksempel et hybrid trusselscenario representerer, vil graden av usikkerhet og antall ukjente faktorer øke. For eksempel ved å ta utgangspunkt i hvordan sikringsrisiko utrykkes i trefaktormodellen (Busmundrud, Maal, Kiran og Endregard, 2015) som en funksjon av faktorene verdi, trussel og sårbarhet, vil et hybrid trusselbilde innebære stor usikkerhet. Her kan det for eksempel være vanskelig å forstå hvor sårbarhetene i et digitalt system eller i en lang og kompleks forsyningskjede egentlig ligger. Likedan kan det ved et fordekt angrep være vanskelig å forstå hvem trusselaktøren egentlig er, hvilken hensikt og kapasitet trusselaktøren har, og dermed også hvilken verdi

aktøren egentlig truer. I dette ligger at det er vanskelig – om ikke umulig – å etablere et fullstendig trusselbilde eller å kunne forutse og analysere absolutt alle sårbarheter og alt som kan gå galt.

Det teoretiske perspektivet «Resilience Engineering» (Hollnagel et al., 2006) fokuserer på hvordan organisasjoner kan legge til rette for å kunne håndtere både kjent og ukjent kompleksitet under krevende omstendigheter (Woods og Hollnagel, 2006, s. 6). Det er derfor interessant å vurdere hvordan olje- og gasselskaper forholder seg til et hybrid trusselscenario ut fra dette perspektivet. Selve ordet «engineering» kan være vanskelig å oversette, men betydningen innebærer at en ønsker å utarbeide og legge til rette for, iverksette eller iscenesette de mest ønskelige eller optimale løsningene på et problem. I denne sammenhengen kan det forstås som hvordan konseptet «resiliens» kan omsettes til observerbare eller målbare aktiviteter i en organisasjon.

SAFETY-I: et tradisjonelt syn på sikkerhet

Tiltak for å forbedre sikkerhet er ofte reaktive og basert på etterpåklokskap, det vil si at de er basert på en forståelse av tidligere hendelser som man ikke ønsker skal intreffe igjen (Woods og Hollnagel, 2006, s. 1). Woods og Hollnagel (2006) argumenterer for at et slikt tradisjonelt syn på sikkerhet handler om å kunne forklare tidligere hendelser, og dermed at sikkerhet kan opprettholdes så lenge en holder seg innenfor de rammene eller normene som erfaring og historikk tilsier (Woods og Hollnagel, 2006, s. 4). I et slikt perspektiv vil altså vår erfaring og oppfatning av tidligere hendelsesforløp prege hvordan vi forventer at et fremtidig risikobilde ser ut, og hvordan vi skal forberede oss og vurdere hvilke tiltak som kan iverksettes.

Woods og Hollnagel (2006, s. 5) hevder at det er vanskelig for en organisasjon å kunne forutsi hva som kan føre til feil og uønskede hendelser, og dermed også vanskelig å kunne etablere og opprettholde strategier for å unngå feil og uønskede hendelser. I tillegg vil det være krevende å opprettholde tilstrekkelige sikkerhetsmarginer når en utsettes for krav om økt effektivitet i arbeidsprosessene. I dette perspektivet kan feil og uønskede hendelser ses på som et uttrykk for manglende evne til å håndtere kompleksitet.

Et reaktivt og bakoverskuende syn på sikkerhet, som fokuserer på å forhindre gjentagelse av det som tidligere har ført til uønskede hendelser, medfører at sikkerhet kan defineres som «å forhindre ulykker og uønskede hendelser» (Hollnagel, 2018). Det er dette perspektivet på sikkerhet Hollnagel (2014) omtaler som «Safety-I».

Sentralt i dette perspektivet står oppfatningen om at alle uheldige eller uønskede utfall av en aktivitet kan spores tilbake til identifiserbare årsaker. Med andre ord at det ligger et årsak/virkning-forhold eller en kausalitet til grunn for alle uønskede hendelser. Så snart disse årsakene er identifisert kan altså sikkerhet i følge Safety-I perspektivet oppnås gjennom å elliminere eller beskytte aktiviteten fra disse årsakene (Hollnagel, 2018, s. 6). Safety-I handler altså om å legge til rette for at så lite som mulig ved en aktivitet skal kunne gå galt.

SAFETY-II: et nytt perspektiv som bakgrunn for Resilience Engineering

Resilience Engineering ble introdusert som et nytt paradigme for å snu oppfatningen som kommer frem i Safety-I i en mer proaktiv retning (Woods og Hollnagel, 2006, s. 2). Resilience Engineering åpner for en ny tilnærming, der feil og hendelser i stedet betraktes som en midlertidig manglende evne til å effektivt håndtere komplekse situasjoner. Dette innebærer at sikkerhet ikke er et resultat av reaktive barrierer og forsvarsverk, men av resiliente prosesser i virksomhetene (Woods og Hollnagel, 2006, s. 3). Forbedret sikkerhet er avhengig av at en er i stand til å oppfatte og beskrive hvordan sårbarhet endrer seg, og at organisasjonen er i stand til å møte nye utfordringer gjennom en kontinuerlig tilpasning av nye virkemidler (Woods og Hollnagel, 2006, s. 5).

Hollnagel og Woods (2006, s. 357) argumenterer for at Resilience Engineering fører til at organisasjoner kan endre seg fra å være avhengig av en reaktiv analytisk sikkerhetstilnærming til å kunne være mer fleksibel og tilpasningsdyktig. Sikkerhet kan dermed etableres gjennom å tilpasse bruk av ulike eller nye virkemidler til nye situasjoner som kan oppstå. Hollnagel og Woods (2006, s. 357) begrunner dette ved at en resilient organisasjon vil søke å unngå å overforenkle risikobildet, det vil si at en forstår og aksepterer at sikkerhet er en dynamisk tilstand og i stadig endring, i motsetning til en tilstand basert på et statisk øyeblikksbilde. Videre forutsettes det at en ikke fokuserer på enkeltfaktorer, men ser og vurderer et helhetsbilde, da uønskede hendelser typisk oppstår i tett koblede systemer med gjensidig avhengige funksjoner.

Sikkerhet kan ikke måles, men viser seg gjennom fravær av feil og hendelser. Sikkerhet kan dermed beskrives bedre som en tilstand eller aktivitet («hva virksomheten gjør») enn som en egenskap («noe virksomheten har»). Resilience Engineering-perspektivet tar høyde for at uønskede hendelser kan oppstå, men i stedet for å fokusere på feil og hendelser som fører til avbrudd i virksomhetens aktivitet må også evnen til å gjennopprette aktivitetsnivået ved

uregelmessige variasjoner og avbrudd inkluderes (Hollnagel og Woods, 2006, s. 347). Et syn på sikkerhet som «evnen til å kunne gjennomføre sine aktiviteter under varierende forhold og betingelser» omtaler Hollnagel (2014) som «Safety-II».

Hollnagel (2018, s. 7) beskriver hvordan Resilience Engineering betrakter både uønskede og ønskede hendelser fra samme utgangspunkt, eller med andre ord at både uønskede og ønskede hendelser oppstår på samme måte. Dette leder til at at en organisasjon kan oppnå sikkerhet ved å fokusere på at aktivitetene utføres så riktig som mulig, fremfor å rette sin innsats mot å identifisere og elliminere alle faktorer som kan føre til at aktivitetene feiler. Safety-II konseptet innebærer altså at fokus endres fra å beskytte et system eller en virksomhet fra uønskede hendelser og hvordan uønskede hendelser kan oppstå, til å fokusere på hvilke faktorer som gjør systemet eller virksomheten i stand til å faktisk fungere slik det skal. Safety-II tar også sikte på at organisasjonene skal være i stand til å utvikle sitt potensiale for å opptre og fungere på en resilient måte (Hollnagel, 2018).

Hollnagel (2011a, s. xxix) hevder at det er både lettere og mer effektivt å forbedre graden av sikkerhet gjennom å øke antall ting som går riktig enn ved å redusere antall ting som kan gå galt.

Hensikten med Resilience Engineering er altså å legge til rette for at organisasjonen har de egenskapene som gjør den i stand til å håndtere uforutsette og ukjente hendelser, og dermed kunne opprettholde og eventuelt gjennopprette normaltilstanden hvis organisasjonen utsettes for uforutsette påkjenninger. Resilience Engineering forutsetter altså at organisasjonen møter utfordringer proaktivt, og tilpasser seg nye ukjente og uventede forhold.

Konseptet «resiliens»

Resiliens kan beskrives på mange måter (se for eksempel Jore, 2020). Hollnagel (2018, s. 10) beskriver utgangspunktet for resiliens som hvordan mennesker justerer og tilpasser sine handlingsmønstre til de rådende forhold. En resilient organisasjon beskrives ut fra «i hvilken grad den er i stand til å opprettholde sin funksjonsevne under både normale og uforutsette betingelser» (Hollnagel, 2018, s. 15). Dette underbygges ved at resiliens kan betraktes som en karakteristikk ved måten en organisasjon utfører sin aktivitet: «hva den gjør og hvordan den gjør det» (Hollnagel, 2018, s. 11).

Woods og Hollnagel (2006, s. 6) peker på evnen til å være forutseende og kunne forvente endringer i risikobildet før feil og uønskede hendelser oppstår som sentrale faktorer i

konseptet resiliens, og Hollnagel og Woods (2006, s. 348) omtaler også resiliens som evnen til å gjenopprette kontroll og håndtere kompleksiteter. «Kontroll» beskriver her Hollnagel og Woods (2006, s. 348) som evnen til å minimere eller elliminere effekten av uønskede variasjoner i både et systems egen funksjonsevne og i systemets omkringliggende miljø. Feil og uønskede hendelser kan dermed ses på som en konsekvens av tapt kontroll innenfor de rammene som systemet er satt til å operere innenfor (Hollnagel og Woods, 2006, s. 348). For at en organisasjon skal kunne betraktes som resilient er det altså helt grunnleggende at den ikke mister kontroll, men er i stand til å gjenopprette og fortsette sine aktiviteter.

Det kan være flere grunner til at en organisasjon mister kontroll, men hovedsakelig vil det skyldes fire faktorer (Hollnagel og Woods, 2006, s. 349): (i) tidsmangel eller tidspress – som igjen ofte skyldes manglende evne til å være forutseende og dermed presser organisasjonen inn i et reaktivt mønster, (ii) mangel på kunnskap eller manglende evne til å vite hva en skal kunne forvente (og dermed hva en skal se etter og hvor en skal rette oppmerksomheten), (iii) mangel på kompetanse – altså å vite hva man skal gjøre og hvordan, samt (iv) mangel på de nødvendige resursene for å kunne opprettholde og gjenopprette aktiviteten.

Dersom en organisasjon skal kunne være resilient hevder Hollnagel og Woods (2006, s. 356) at det kreves en konstant form for uro i organisasjonen, i betydningen at en må unngå å bli selvtilfreds, avslappet eller komfortabel med den nåværende tilstanden, men i stedet være årvåken og jakte på tegn til endringer og avvik. Dette forutsetter at organisasjonen har et realistisk bilde av seg selv og sine egenskaper og evner, og at den har eller kan innhente nødvendig kunnskap om hva som har hendt tidligere, hva som hender nå og hva som kan hende i fremtiden – i tillegg til at den også har eller kan innhente kunnskap om hvilke tiltak organisasjonen kan og må innføre i tilfelle uønskede hendelser intreffer.

Resilience Engineering som teoretisk perspektiv betrakter hvordan resiliens i seg selv er en egenskap ved en aktivitet. Resiliens, eller evnen en virksomhet har til å kunne fungere på en resilient måte, handler ikke om å forhindre eller unngå avbrudd i normal drift. Utgangspunktet for perspektivet er at den tradisjonelle tilnærmingen til sikkerhet ikke er tilstrekkelig da den er reaktiv og kun basert på hva man har lært av tidligere uønskede hendelser. Dette innebærer en begrensning i forhold til evnen til å kunne forutse og inkludere nye og ukjente hendelser eller scenarier. Resilience Engineering fokuserer i stedet på at organisasjonen innehar de egenskapene som faktisk har betydning for hvordan uønskede hendelser håndteres, slik at

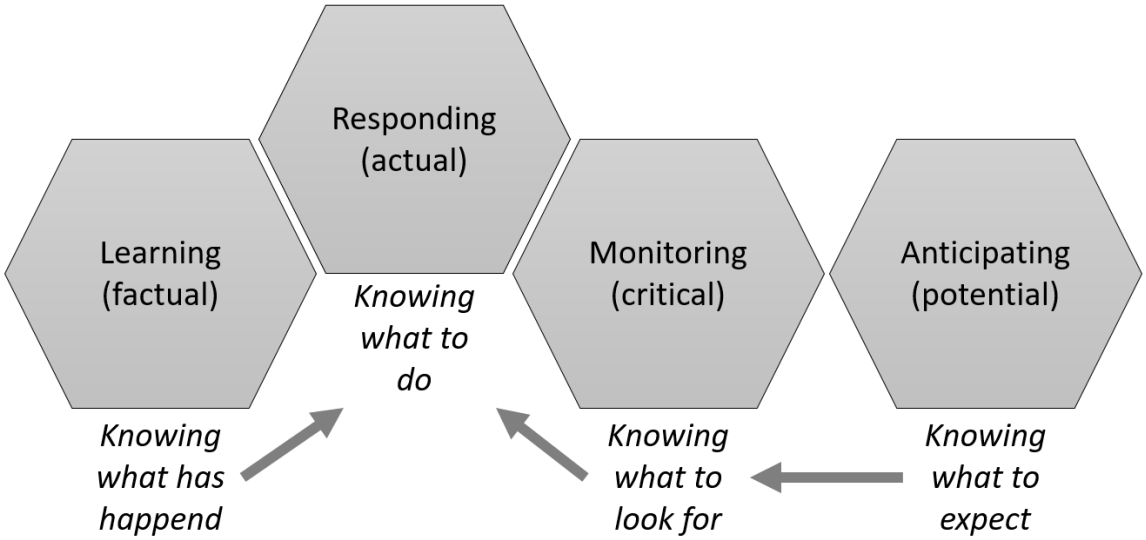
sikkerheten kan styres gjennom proaktive (resiliente) prosesser i stedet for reaktive barrierer og forsvarsverk (Woods og Hollnagel, 2006, s. 3). Proaktive prosesser innebærer at man kontinuerlig søker etter å forutse uventede hendelser eller endringer.

Et resilient system må altså være proaktivt, fleksibelt, tilpasningsdyktig og forberedt (Hollnagel og Woods, 2006, s. 356). Dette innebærer å være klar over både virkningen av ens handlinger, og konsekvensene av å ikke gjøre noe, eller slik Hollnagel (2014, s. 50) formulerer det, er en organisasjons evne til å fungere på en resilient måte et uttrykk for dens evner og potensiale.

Potensialet for å utvikle resiliens i organisasjoner

En organisasjon kan forbedre sin evne til å håndtere både forventede og uventede forhold gjennom å utvikle og styrke sin resiliens. I Resilience Engineering-perspektivet beskrives fire elementer (Figur 2) som påvirker og muliggjør organisasjoners evne til å fungere på en resilient måte (Hollnagel, 2011a, s. xxxvii):

- Å reagere («respond»): å kunne vite hva en skal gjøre, altså å reagere på det som skjer. Dette innebærer å vite hvordan uregelmessigheter, forstyrrelser og uventede hendelser skal håndteres – både gjennom forberedte handlinger og når nye ukjente og uventede forhold krever at handlingene er tilpasset en ny situasjon.
- Å overvåke («monitor»): å vite hva man skal se etter og at hele organisasjonen observerer, overvåker og er oppmerksom på indikasjoner og tegn på uregelmessigheter, både nå og i nær fremtid. Dette inkluderer å observere både organisasjonens eller systemets egen funksjonsevne og omgivelsene det fungerer i og er en del av.
- Å lære («learn»): å kunne forstå hva som har hendt og å kunne lære og utvikle seg gjennom erfaring. Det vil si å kunne hente ut den viktigste lærdommen fra hendelser som har betydning for sikkerheten, og dermed ha forståelse for hva som gjør at det går bra og fokusere på å utføre de rette handlingene.
- Å forvente («anticipate»): å være bevisst på hvilke utviklinger, forstyrrelser eller trusler man kan forvente i fremtiden, og hvordan man kan forutse disse.



Figur 2 *De fire grunnsteinene for å utvikle og styrke organisasjoners resiliens (Hollnagel, 2011)*

Disse fire elementene eller grunnsteinene for en organisasjons evne til å fungere på en resilient måte er ikke uavhengig av hverandre. Som indikert i Figur 2 er det for eksempel viktig å vite hva man kan forvente for å effektivt kunne monitorere et system, altså å vite hva man skal se etter. Likedan er det vanskelig å kunne respondere uten først å ha blitt varslet, noe som på sin side kommer gjennom overvåking av systemet. En respons er også avhengig av å ha forståelse for konsekvensene av hva som faktisk har skjedd, og hvilken respons som er nødvendig. Dette peker på læringselementet. Å forstå hvordan de fire elementene henger sammen og hvilken betydning de har for hverandre er med andre ord viktig for å kunne bygge og styre en resilient organisasjon.

Selve Resilience Engineering-perspektivet kan altså beskrives ut fra hvordan organisasjoner best kan legge til rette for å kunne reagere, overvåke, lære fra erfaringer og forutse mulige fremtidige scenarier (Hollnagel, 2011a).

Å kunne forholde seg til det som er kritisk: en obervant organisasjon

«The purpose of monitoring is to keep an eye on what happens in the operating environment and within the organization itself» (Hollnagel, 2018, s. 33).

Det er helt grunnleggende innen Resilience Engineering at organisasjonen kan overvåke og bygge erfaring fra skillet mellom virksomhetens faktiske tilstand og funksjonsevne og en ideal- eller ønsketilstand. Uten å kunne se dette skillet vil det være umulig for organisasjonen å «kalibrere sin egenoppfatning» (Hollnagel og Woods, 2006, s. 357), og dermed sin evne til å

forbedre seg. Det er nettopp forståelsen av hva som er årsaken til skillet mellom den faktiske tilstanden og ønsketilstanden som er grunnlaget for læring og organisatorisk forbedring.

For å kunne opptre på en resilient måte er det nødvendig å kunne observere og overvåke både virksomhetens egen funksjon (innenfor systemets egne definerte grenser) og virksomhetens omkringliggende miljø (omgivelsene som virksomheten fungerer i) (Hollnagel, 2018, s. 31). For en organisasjon som ikke er i stand til å overvåke og ha oversikt over hverken sin egen funksjon eller det omkringliggende miljø vil alle hendelser være uventet og komme uten forvarsel, og resultere i at organisasjonen er konstant uforberedt (Hollnagel, 2018, s. 27).

Å være bevisst på hva en skal overvåke uttrykker Hollnagel (2011) som evnen til å adressere det som er kritisk.

Effektiv overvåkning kan være basert på indikatorer eller trender som kan forutsi eller antyde at en endring, avvik eller faktisk hendelse er i ferd med å inntreffe (Hollnagel, 2018, s. 33). Hollnagel beskriver indikatorer som «signal, tegn eller symboler som representerer en nåværende verdi, størrelse eller retning». Videre beskrives trender som «en generell tendens i et hendelsesforløp over en viss tid». Indikatorer kan altså for eksempel angi om en terskelverdi er nådd eller er nær, mens trender kan angi om terskelverdien kan eller vil nås i (nær) fremtid – gitt at de underliggende omstendighetene er de samme som de nåværende, eller at en rådende utvikling fortsetter på samme måte (Hollnagel, 2018, s. 33). Hensikten med en observant organisasjon er ikke at den til en hver tid skal kjenne verdien av en spesifik indikator eller trend, men at organisasjonen kan tolke indikatorer og trender dit hen at den kan iverksette en respons eller en endring i organisasjonens tilstand hvis det er nødvendig – for eksempel å heve eller senke sikringsnivået, innføre strengere kontrollrutiner osv.

Hollnagel (2018, s. 35-36) skiller mellom tre typer indikatorer som kan være gunstig for å kunne beskrive hvordan en organisasjon eller et system opptrer:

a. *Bakoverskuende indikatorer*: indikatorer som peker på tidligere hendelser eller tilstander. Disse er basert på tidligere innsamlede data, uavhengig av om disse var kjent som eller brukt som indikatorer eller ikke. Hensikten er å bygge forståelse for tidligere hendelser, for eksempel som illustrasjon av et kjent hendelsesforløp eller for å dokumentere en trend.

b. *Indikatorer i nåtid*: indikatorer som viser til en nåværende hendelse eller tilstand, som for eksempel produksjonsrater eller kontantstrøm. Overvåking av indikatorer i nåtid kan bidra til å justere pågående aktiviteter («virker tiltakene eller må de justeres?»), og kan også beskrives som feedback eller tilbakemelding på iverksatte tiltak.

c. *Fremoverskuende indikatorer* peker på hendelser eller organisatoriske tilstander som kan intreffe i fremtiden. Fremoverskuende indikatorer er naturligvis ikke basert på faktiske målinger (noe som vil være umulig), men på tolkning av nåværende og bakoverskuende indikatorer med tanke på hva som potensielt kan inntreffe i fremtiden. Fremoverskuende indikatorer beskriver altså ikke en eksisterende tilstand, men brukes til å predikere fremtidige hendelser eller tilstander. Fremoverskuende indikatorer innebærer derfor ulik grad av usikkerhet, som igjen påvirker om en respons skal iverksettes eller ikke. For eksempel hvis usikkerheten anses som for stor kan det føre til at en respons vurderes som for kostbar å iverksette. Dette er et klassisk dilemma da det kan være betydelige kostnader knyttet til innføring av tiltak som viser seg å ikke være nødvendige, og samtidig betydelige kostnader knyttet til å *ikke* innføre tiltak som senere viste seg å være nødvendige.

Evnen til å kunne gjenkjenne trender og tendenser som kan ha alvorlige konsekvenser, selv om de potensielt er for små til å kunne beskrives som en reell endring, er sammen med evnen til å reagere på mindre endringer eller avvik påkrevd for å effektivt kunne styre en virksomhet eller aktivitet. Ved bruk av fremoverskuende indikatorer må overvåking altså være en proaktiv prosess, som kan gjøre det mulig å kjenne igjen når situasjoner eller hendelser nærmer seg (Hollnagel, 2018, s. 31). I motsetning til de tre andre grunnelementene for en organisasjons evne til å fungere på en resilient måte må overvåking derfor foregå kontinuerlig.

Overvåking må være fokusert, det vil si at både hva som skal overvåkes og hensikten eller formålet med overvåkingen må være kjent (hvorfor det overvåkes). Hollnagel (2018, s. 34) legger spesielt vekt på å forstå hensikten med overvåkningen, fordi indikatorer som ikke kan forstås eller tolkes har liten verdi samtidig som de likevel er ressurskrevende å overvåke.

Bruk av indikatorer vil være et kompromiss mellom hvor effektive de er og hvor grundig man skal gå til verks. En effektiv indikator betyr i denne sammenhengen at den er enkel å måle eller identifisere, mens grundighet peker på hvor meningsfull indikatoren er. For å kunne ta

stilling til hvor meningsfull indikatoren er, beskriver Hollnagel (2018, s. 59) at man for eksempel bør vurdere «hvor godt indikatoren faktisk måler eller indikerer den verdien den er antatt å representere, og i hvilken grad den kan sammenlignes med andre indikatorer eller allment aksepterte referanser eller kriterier». Videre peker Hollnagel (2018, s. 60) på at en meningsfull indikator også skal bidra til å gi beslutningsgrunnlag for å vurdere om en respons skal iverksettes eller ikke.

Å kunne forholde seg til det som faktisk skjer: hvordan organisasjonen reagerer

«An organization is doomed if it is unable to respond when something happens» (Hollnagel, 2018, s. 27).

Å være i stand til å reagere når uforutsette hendelser eller forhold påvirker en organisasjons normale og forventede tilstand, er naturligvis en forutsetning for å kunne opprettholde eller gjenopprette organisasjonens funksjonsevne. Dette krever at organisasjonen først er i stand til å detektere at noe har skjedd, for deretter å identifisere hva som har skjedd og så vurdere hvordan en best skal reagere. For å kunne påvirke en organisasjons funksjonsevne slik at den enten kan opprettholde eller gjenopprette idealtilstanden, må enhver respons både skje til rett tid (tidsnok) og på rett måte (kunne oppnå ønsket effekt).

Det er dette Hollnagel (2011) beskriver som evnen til å adressere det som faktisk utfolder seg i sann- eller nåtid.

En respons kan være forberedt og planlagt på forhånd, eller utvikles i løpet av en hendelse, selv om det riktignok er vanskelig å forberede respons på skjeldne eller uregelmessige hendelser på en realistisk måte. Organisasjonen bør derfor alltid være i beredskap og klar for å kunne iverksette tiltak (Hollnagel, 2018, s. 30). I følge Hollnagel (2018, s. 29) ligger altså nøkkelen til effektiv respons i å kunne vite *når* man skal respondere og *hvordan*. Responsen må komme som følge av en tilstand eller varsel, men det er også viktig å forstå når responsen skal opphøre. Responsen må hverken opphøre for tidlig (før ønsket effekt er oppnådd) eller for seint (når responsen ikke lenger har noen virkning – og dermed er bortkastet).

En organisasjons evne til å respondere har altså liten verdi dersom organisasjonen ikke også evner å drive effektiv overvåking. Det vil si å overvåke eller å innhente data regelmessig for å gjøre det mulig å både forstå hvordan organisasjonen fungerer og forstå miljøet den fungerer i, samt å eventuelt avgjøre hvorvidt endringer eller avvik krever en respons (Hollnagel, 2018, s. 58). Å respondere tidlig på en forventet utvikling kan ha den fordelen at mindre eller færre

tiltak er nødvendig for å korrigere en uønsket utvikling. Men det er selvfølgelig en risiko knyttet til en slik forebyggende respons, da en ikke kan vite med sikkerhet om responsen er riktig eller i det hele tatt nødvendig (Hollnagel, 2018, s. 35).

Å kunne forholde seg til det som har hendt: en lærende organisasjon

En organisasjon som har evnen til å effektivt overvåke sine aktiviteter og til å kunne respondere når det er nødvendig kan fungere rimelig bra så lenge de underliggende forholdene og betingelsene er stabile (Hollnagel, 2018, s. 61). Men hvis disse skulle endre seg må også organisasjonen endre seg for å kunne fungere like effektivt, noe som betyr at organisasjonen også må ha evnen til å kunne lære. Hollnagel (2018, s. 61) beskriver nemlig læring som «aktiv og tilsiktet modifisering av hvordan en organisasjon håndterer normale eller hverdagslige situasjoner», og betrakter dermed læring i et Resilience Engineering-perspektiv som en organisasjons evne til å endre hvordan den overvåker, responderer og er forutseende, samt evnen til å endre hvordan den faktisk lærer. Evnen til å lære er altså avgjørende for en organisasjons evne til å fungere på en resilient måte (Hollnagel, 2018, s. 36).

En organisasjons evne til både å kunne monitorere en tilstand og å kunne reagere ved avvik er avhengig av at den både vet hva som er normaltilstanden og hva som fører til avvik fra denne. Uten å vite hvorfor en hendelse inntreffer – eller hvorfor den ikke inntreffer – er det vanskelig å kunne reagere og innføre eventuelle tiltak for å forhindre eller avgrense hendelsen. For at en organisasjon skal kunne lære må den derfor vite hva som har betydning, eller med andre ord: hvilke erfaringer som det gir mening å lære fra.

Evnen til å kunne lære fra erfaringer, eller som Hollnagel (2011b) presiserer: evnen til å hente den riktige lærdomen fra de riktige erfaringene, er essensielt for evnen til å kunne forbedre en virksomhets aktiviteter i fremtiden. Hollnagel (2011b, s. 287) viser til en definisjon av læring som «endring i adferd som et resultat av erfaring», men presiserer videre at læring ikke er en *tilfeldig* endring i adferd, men en systematisk endring som medfører at visse utfall [av en aktivitet] er mer sansynlig enn andre.

En mer formell definisjon på læring uttrykkes i Hollnagel (2018, s. 36) som «på hvilke måter en organisasjon endrer eller tilegner seg ny kunnskap, kompetanse og ferdigheter», og Hollnagel peker her videre på hvordan læringen skjer gradvis; den bygger på og formes av tidligere tilegnet kunnskap. Læringsprosessen kan dermed forstås bedre som en pågående utviklingsprosess enn som passiv innsamling av kunnskap, informasjon og fakta.

En organisasjon som ikke evner å lære fra erfaring, enten fra hvordan den selv fungerer eller fra det omkringliggende miljøet den opererer i, vil begrense seg til å alltid overvåke de samme indikatorer, og eventuelle responser vil alltid være de samme (Hollnagel, 2018, s. 36). En slik organisasjon vil bli hengende fast de samme etablerte arbeidsmønstrene, og vil ha vanskelig for å tilpasse seg endringer i både funksjonsevne og i det omkringliggende miljøet.

Læringsprosessen kan enten være uregelmessig eller regelmessig, eller for den saks skyld kontinuerlig (Hollnagel, 2018, s. 37). Uregelmessig læring er knyttet til uvanlige situasjoner eller hendelser, for eksempel når en ulykke inntreffer, og kan derfor betraktes som reaktiv eller hendelsesdrevet. Hollnagel (2018, s. 37) peker på at et slikt perspektiv på læring også antyder at det ikke er noe å lære så lenge det ikke skjer noen uvanlige eller uventede hendelser. Dette står i kontrast til regelmessig eller kontinuerlig læring som er mer basert på organisasjonens normale ytelsesmønstre enn på unike hendelser.

Hollnagel (2018, s. 37) viser til at dersom læringsprosessen er kontinuerlig, fokuserer den på hendelser som normalt inntreffer ofte, for eksempel som del av hverdagslige aktiviteter og rutiner, og ikke knyttet til de enkelte mer alvorlige hendelsene. En god læringskultur er ut fra dette basert på at organisasjonen både kan identifisere og skille mellom aktiviteter som utføres godt eller gir gode resultater og tilsvarende dårlig utførelse av aktiviteter, samt forstå og ta inn over seg konsekvensene av disse. Dette vektlegger dermed breddeforståelse fremfor dybdeforståelse, og skiller seg fra en læringskultur som fokuserer på målrettede analyser av spesifike hendelser (Hollnagel, 2018, s. 37).

Hollnagel (2018, s. 39) peker på noen konkrete forutsetninger som må ligge til grunn for at effektiv læring skal finne sted: Det er behov for kompetente ressurser, både i form av mennesker og materiell, til å samle inn relevante data og informasjon, samt til å analysere og tolke disse, før en kan konkludere og formulere hvordan lærdommen kan best operasjonaliseres og implementeres i organisasjonen. I tillegg har det grunnleggende betydning *hvordan* læringen foregår og hvordan den kontrolleres eller holdes i hevd, med andre ord hvor viktig organisasjonen anser læringsprosessen for å være. Er læringsprosessen for eksempel en kontinuerlig del av det daglige arbeidet, eller er den begrenset til de tilfellene der det er et «opplagt og uunngåelig behov – normalt etter at noe har gått alvorlig galt» (Hollnagel, 2018, s. 39)?

Et annet viktig grunnlag for læringsprosessen er selve forholdet mellom tiltak (respons) og effekten eller resultatet av disse, både de som har vært vellykket og de som har mislykkes. Her er det viktig å kunne forstå hvor lang tid en forventer at det skal ta før konsekvensen av responsen vises (Hollnagel, 2018, s. 39). En effektiv læringsprosess er altså avhengig av tid, både fordi læringen i seg selv er tidskrevende og fordi det tar tid å iverksette og å kunne se effekten av tiltak og endringer. Læring kan først finne sted når en respons har fått tid til å fungere, og når effekten av responsen er åpenbar (Hollnagel, 2018, s. 40).

Hollnagel (2018, s. 40-41) peker på tre grunnleggende forhold som må være tilstede for at læring skal finne sted:

a. Organisasjonen må anerkjenne at en aktuell hendelse eller utfallet av en aktivitet skiller seg fra det som er forventet, og at det er nødvendig å forstå hvorfor dette er tilfelle slik at en kan gjøre noe med det. Dette kan ses på som en naturlig konsekvens av eventuelle uheldige eller alvorlige uventede utfall, men Hollnagel (2018, s. 40) peker også på betydningen av å lære av utfall som er akseptable eller bedre enn forventet fordi dette også forteller noe om kvaliteten på aktivitetene. Her ligger evnen til å styrke eller forsterke det som fungerer og gir akseptable utfall, og endre eller justere det som ikke gir de forventede utfallene (Hollnagel, 2018, s. 27).
b. Læring er i utgangspunktet situasjonsspesifik, i betydningen at det at det vil være vanskelig eller umulig å bringe med seg læring, kunnskap og kompetanse mellom situasjoner som er grunnleggende ulike. Derfor er det mer hensiktsmessig å se på hva som er likhetstrekkene mellom forskjellige situasjoner og dermed lære noe som kan ha generell eller universell betydning. Å kunne finne likhetstrekk mellom situasjoner er altså en betingelse for læring, uavhengig av om likhetstrekkene er reelle eller antatte.
c. Det må være mulig å bekrefte eller verifisere at læring faktisk har funnet sted. Med utgangspunkt i at læring medfører en endring i adferd eller funksjonsevne, og ikke bare endring i kunnskapsnivå, må slike endringer være merkbare eller observerbare. Det betyr at den samme eller en tilsvarende situasjon må kunne intreffe igjen, og innebærer at det er vanskelig å verifisere at en har lært noe av skjeldne hendelser som for eksempel alvorlige ulykker eller katastrofer (Hollnagel, 2018, s. 41).

Å kunne forholde seg til det som potensielt kan skje: en forutseende organisasjon

Evnen til å kunne overvåke, respondere og lære er ikke tilstrekkelig for organisasjoners evne til å opptre på en resilient måte. Å kunne være forutseende eller forventende er en forutsetning for at organisasjonen skal kunne forberede seg på fremtidige endringer eller hendelser (Hollnagel, 2018, s. 48). Så selve grunnleget for evnen til å være forutseende ligger i organisasjonens anerkjennelse av behovet for å kunne se forbi den nåværende tilstanden (Hollnagel, 2018, s. 45).

Hensikten med å være forutseende ligger naturligvis i å ha forståelse for potensialet som ligger i mulige fremtidige hendelser, endringer i funksjonsvilkår og/eller trusler som kan skade virksomhetens funksjonsevne (Hollnagel, 2011a, s. xxxvii). Men å kunne identifisere muligheter som kan være gunstige eller til fordel for virksomheten er også viktig.

Dette beskriver Hollnagel (2011a) som evnen til å adressere potensialet som ligger i fremtiden.

Mens overvåking fokuserer på det som ligger innenfor de nåværende eller pågående aktivitetenes omfang, ser forutseenhet lengre. Forutseenhet kan både betrakte hendelser og situasjoner som kan oppstå i fjern fremtid, og situasjoner som ikke umiddelbart kan knyttes til organisasjonens primæraktivitet.

Andre måter organisasjoner betrakter fremtiden er for eksempel gjennom planlegging og risikovurdering. Men Hollnagel (2018, s. 43) argumenterer for at forutseenhet skiller seg fra planlegging, da planleggingen har til hensikt å legge til rette for og gjøre klart for organisasjonens fremtidige aktiviteter basert på forståelsen av den nåværende situasjonen. Hensikten med forutseenhet er derimot *ikke* å støtte opp under nåværende aktiviteter, men å kunne forestille seg alternative scenarier og vurdere hva som må gjøres dersom fremtidens grunnleggende betingelser og forhold er fullstendig annerledes enn de nåværende.

Videre argumenterer Hollnagel (2018, s. 43) for at også risikovurdering skiller seg fra forutseenhet. Hensikten med en risikovurdering er i følge Hollnagel å kunne identifisere hendelser eller forhold som kan true organisasjonen og dens aktiviteter på forhånd. En slik risikovurdering er nyttig så lenge de grunnleggende forholdene og betingelsene for aktiviteten er kjent og enkelt kan beskrives, samt at organisasjonen og det miljøet den opererer i er stabilt slik at forståelsen av disse er gyldig over (lang) tid. I motsetning til forutseenhet er risikovurdering altså begrenset til å måtte forholde seg til hvordan organisasjonens

funksjonsevne uttrykkes, og avhengig av at de grunnleggende betingelsene er kjent (Hollnagel, 2018, s. 44).

Forutseenhet innebærer en forventning om noe som vil eller kan intreffe i fremtiden, og er dermed avhengig av hvordan vi tenker om eller oppfatter fremtiden. Dette henger igjen sammen med hvordan vi oppfatter både nåtiden og fortiden, eller med andre ord hvilken ontologisk tilnærming vi har. For eksempel vil ontologiske realister anse at verden, og prinsippene for hvordan den fungerer, eksisterer uavhengig av mennesklig bevissthet – altså at farer og trusler eksisterer enten vi kjenner til dem eller ikke. Et konstruktivistisk ontologisk syn vil derimot se på verden og hvordan den fungerer som et resultat av vår forståelse og tolkning av den (Engen, Kruke, Lindøe, Olsen, Olsen og Pettersen, 2016, s. 89).

Et dilemma som er tydelig når det gjelder å være forutseende, er at det er umulig å vite med sikkerhet hvilke elementer ved et forventet problem eller situasjon som vil kreve en respons, og hvilke som kan ignoreres (Hollnagel, 2018, s. 47). Evnen til å være forutseende kan også hemmes av organisasjonskultur - for eksempel en motvilje mot endring i organisasjonen eller at en tviholder på eksisterende (institusjonaliserte) oppfatninger. Hollnagel (2018, s. 47) viser også til andre forhold som har negativ påvirkning på evnen til å være forutseende, blant annet å overse eksterne signaler til fordel for fokus på tydelige, men uvesentlige eller falske indikatorer, undervurdering av farer som er i ferd med å materialisere seg og manglende evne til å forstå eller etterkomme formelle krav og forventninger.

Formålet med forutseenhet er å kunne forstå hva som er viktig å fokusere på i fremtiden, hvilke områder som må prioriteres og hva de mest kritiske bekymringene er knyttet til (Hollnagel, 2018, s. 46). Dette representerer organisasjonens bilde av hvordan både selve fremtiden, rammevilkår og funksjonsbetingelser vil utvikle seg og påvirke organisasjonens evne til å fungere. Hollnagel (2018, s. 46) påpeker at en forutsetning for forutseenhet er en «konstant uro – en følelse av at situasjonen ikke lenger er stabil, forutsigbar eller sikker». Denne underliggende følelsen kan utløses av hendelser som ikke nødvendigvis kan knyttes til organisasjonens primæraktivitet, og innebærer også en anerkjennelse av at fremtiden er usikker. Dette medfører videre en anerkjennelse av et behov for å kunne være forberedt, og å kunne vurdere hvilke forberedelser som kan bli nødvendige (Hollnagel, 2018, s. 46).

SAFETY-III: Kritikk av selve grunnlaget for Resilience Engineering

I Leveson (2020) retter Nancy Leveson kritikk mot hvordan innholdet som er tillagt begrepene Safety-I og Safety-II danner grunnlag for Resilience Engineering. Hun hevder at det reaktive synet som Safety-I representerer, der sikkerhet utelukkende ses som en tilstand som oppnås gjennom å hindre at uønskede hendelser inntreffer, ikke eksisterer på den måten det er beskrevet i blant annet Hollnagel (2011a, 2014, 2018) og Woods og Hollnagel (2006). Samtidig hevder hun at måten Safety-II presenteres som et alternativt paradigme ikke gir mening, da Safety-II langt på vei ikke representerer noe annet enn det som allerede er etablert praksis. Leveson peker videre på at andre alternative perspektiver allerede finnes og benyttes, og benevner dette som «safety engineering» (Leveson, 2020, s.27).

Safety-I kritiseres primært på bakgrunn av oppfatningen av at sikkerhet er en reaktiv og bakoverskuende prosess, basert utelukkende på analyse og forståelse av tidligere inntrufne hendelser. Leveson (2020) peker på at det ikke er noe som indikerer at dette er et utbredt perspektiv, selv om erfaringsinnhenting, evaluering og læring fra tidligere hendelser såklart er sett på og gjennomføres som en viktig prosess. Leveson (2020) peker videre på at slik Safety-II er beskrevet, er fokus primært på den menneskelige faktoren, eller operatørgrensesnittet, og utelater dermed hvordan systemene er designet som en faktor. *System* betegner i denne sammenhengen hvordan en samling komponenter fungerer sammen for å oppnå et felles mål (Leveson, 2020, s. 40). I dette legger Leveson (2020) at Safety-II representerer en motpol til en sosioteknisk- eller system-tilnærming, der det overordnede systemdesignet i virkeligheten alltid vil være en begrensende eller kontrollerende faktor på spillerommet for menneskelig fleksibilitet – eller resiliens. Slik sosio-tekniske systemer beskrives, innebærer det en gjensidig avhengighet mellom den menneskelige operatøren og systemets tekniske funksjonalitet. Leveson (2020) hevder at det vil være urealistisk å forvente at mennesker eller organisasjoner skal fungere på en resilient måte uten å også vurdere hvordan systemet de opererer i fungerer som en faktor.

Leveson (2020) introduserer videre begrepet Safety-III, som baseres på systemteori og spesielt hvordan systemer utformes med fokus på sikkerhet. Målet for et system er i følge dette perspektivet å fungere som forventet gjennom å unngå tap som følge av utilstrekkelig kontroll med farer eller trusler. I dette ligger at et resilient system må designes fra grunnen av med fokus på å forhindre eller unngå farer, og inkluderer mennesket eller operatøren som en kritisk komponent i systemet. Her skiller Safety-III seg fra Safety-II, da Safety-II i følge

Leveson (2020) kun har fokus på operatøren, ikke på systemet. Safety-III anerkjenner at det vil være et behov for fleksibilitet og evne til å tilpasse seg endringer i systemets levetid, men det påpekes at eventuelle endringer i systemet må analyseres nøye for å forhindre at det introduseres ny risiko eller fare som systemet i utgangspunktet ikke var designet for å håndtere. En forutsetning for Safety-III er at systemdesignet altså innebærer en overordnet holistisk tilnærming til sikkerhet allerede fra man begynner utformingen av systemet, i tillegg til systematisk og kontinuerlig risikostyring som også tar inn over seg hvordan sikkerhetskultur utvikles og pleies i organisasjonen.

Slik Safety-III presenteres, ligger det en forventning om at dette perspektivet på sikt kan bidra til et mer kvalitativt beslutningsgrunnlag, på bekostning av probabilistiske metoder som ikke gir et tilstrekkelig nøyaktig beslutningsgrunnlag i komplekse systemer (Leveson, 2020, s. 105). Dette synet understøttes av Aven (2022), som peker på at sikkerhet – slik det defineres i både Safety-I, Safety-II og Safety-III – ikke gir mening uten å også vurdere risikoperspektivet. Aven betrakter her sikkerhet som det motsatte av risiko gjennom betydningen «sikkerhet oppnås gjennom fravær av uakseptabel risiko». Aven hevder videre at moderne tilnærming og forståelse av risiko inkluderer og bygger på forståelse av usikkerheter, mulige overraskelser og systemers robusthet og resiliens, i motsetning til tradisjonelle probabilistiske tilnærminger (Aven, 2022, s. 9).

Både Safety-II og Safety-III kan oppfattes som tilnærminger eller modeller som supplerer lineære kausale modeller (se for eksempel Hollnagel, 2014, 2018, og Young og Leveson, 2014) – som igjen har betydning for hvordan uhåndterlige eller komplekse systemer vurderes (Aven, 2022). Lineær kausalitet kan her forstås som at et hendelsesforløp har et årsak/virkning-forhold som er både forutsigbart og repeterbart, altså at like hendelser som opptrer på samme måte under de samme betingelsene alltid har samme årsak og alltid vil gi samme virkning. Aven (2022) viser til hvordan en slik tilnærming kan forbedres ytterligere ved å innlemme betraktninger om usikkerhet og kunnskapsstyrke, og at risikovurderinger og fokus på risikoforståelse gir forbedret grunnlag for å håndtere fremtidige hendelser – både ventede og uventede.

Roller og rolleforståelse

Resilience Engineering fokuserer altså på hvordan organisasjoner utfører sine aktiviteter, og at organisasjonene skal kunne utføre sine aktiviteter under både forventede og uventede

betingelser. Resilience Engineering har altså tatt til seg et funksjonelt perspektiv, og fokuserer på hva organisasjonene gjør fremfor hva de er (Hollnagel, 2018, s.24). Hva en organisasjon gjør styres gjennom å tildele forskjellige roller eller funksjoner til ulike grupperinger eller sammensetninger i organisasjonen (Hollnagel, 2018, s.17). Implisitt i dette ligger at en del av organisasjonen har ansvaret for å styre og planlegge hva andre deler av organisasjonen må gjøre for at organisasjonen skal oppnå sine mål og forventninger. Antagelser eller forventninger til hva andre må gjøre for at arbeidet skal gi det forventede resultatet kaller Hollnagel «Work-as-imagined», eller arbeid slik det er forestilt, mens arbeidet som faktisk utføres kalles «Work-as-done» (arbeid som det utføres) (Hollnagel, 2018, s.17).

Ordet rolle kan i følge Store norske leksikon defineres som de forventninger og normer som til sammen er knyttet til en bestemt oppgave, stilling eller relasjon (Store norske leksikon, 2021). Dette kan forstås som at en rolle er tillagt ansvar for at visse bidrag, funksjoner eller oppgaver utføres i samsvar med forventede reaksjonsmønstre. Slike forventninger eller normer kan være både formelle og uformelle, der formelle normer typisk er nedskrevet og dokumentert, for eksempel i form av lovverk, retningslinjer, klassifiseringskrav osv. mens uformelle normer ofte er rene sosiale konvensjoner.

Begrepet *rolleforståelse* peker videre på hvordan ansvaret i en gitt rolle oppfattes og forstås, og innebærer dermed at det kan være ulike oppfatninger knyttet til hva som til enhver tid er forventet av en gitt rolle. Rolleforståelsen kan også variere gjennom ulike faser i en aktivitet eller hendelse, noe som kan kreve videre avklaring.

Det er også ulike deler av organisasjonen som enten tar på seg eller tildeler forskjellige roller og ansvar, derfor vil Work-as-imagined aldri være helt sammenfallende med Work-as-done. I følge Hollnagel reagerer mennesker i forhold til hva de oppfatter, hva de [velger å] fokusere på og hva de husker. Hva mennesker gjør gjenspeiler altså deres situasjonsforståelse, tidshorisont og interesse (Hollnagel, 2018, s.21). Men hva mennesker gjør er også avhengig av påvirkning fra omgivelsene, og de krav, forventninger, normer og verdier som omgivelsene har. Hva mennesker gjør er altså avhengig av deres sosiale og organisatoriske miljø i samme grad som av hvordan de selv tenker og føler (Hollnagel, 2018, s.21).

Roller i en organisasjon

Her kan det være interessant å se hvordan forutsetningene for Resilience Engineering-perspektivet kan beskrives med utgangspunkt i organisasjonsteori. Spesielt hvordan

rolleforståelse og roller kan beskrives gjennom formelle og uformelle strukturer i en organisasjon. Nedenfor presenteres de to organisasjonsteoretiske perspektivene *det instrumentelle perspektivet* og *det institusjonelle perspektivet* for å beskrive hvordan en organisasjons handlings- og reaksjonsmønster i møte med en trussel kan påvirkes av formelle og uformelle strukturer, og hvordan ulike roller kan oppfattes og tillegges innhold. Dette knyttes videre til Resilience Engineering-perspektivet gjennom hvilke forutsetninger som må ligge til grunn for at organisasjoner skal kunne fungere på en resilient måte.

En forståelse for organisasjonenes strukturer gir muligheten til å analysere i hvor stor grad organisasjonene er satt i stand til å handle og organisere seg effektivt og koordinert, mens forståelse for deres kulturelle og symbolske egenskaper muliggjør analyse av hva slags tillit, forventninger og oppfatninger organisasjonene selv og omgivelsene har til både virkemiddelbruken og handlingenes formål og effekt.

Det instrumentelle perspektivet

Det instrumentelle perspektivet beskriver hvordan formelle organisasjonsstrukturer kan bidra til at hendelser håndteres effektivt (Andreassen og Bjørkelo, 2020). Et instrumentelt perspektiv peker altså på at selve organisasjonen kan betraktes som et hjelpemiddel, eller instrument, for å oppnå et gitt mål. Ladegård og Vabo (2010, s. 17) peker på at det instrumentelle perspektivet innebærer at det ligger et rasjonelt pespektiv på ledelse og styring til grunn for bevisst koordinering og påvirkning av adferd i organisasjonen. Dette betyr at intensjoner og mål bak organisasjonens handlinger er entydige og forståelige, og at konsekvensene av disse er forutsigbare. Dette er i tråd med Tvetbråten og Knutsen (2019) sin beskrivelse: «Instrumentelle teorier forteller at aktørene handler formålsrasjonelt etter en konsekvenslogikk» (Tvetbråten og Knutsen, 2019, s. 398).

En formålsrasjonell handling betyr at en velger det alternativet som vurderes som best egnet for å oppnå målsetningen. Konsekvenslogikk, slik Tvetbråten og Knutsen (2019) beskriver det, baseres på at organisasjonens målsetninger er definert ut fra det som anses som en idealtilstand eller ønsket tilstand, og at visse handlinger må utføres for å oppnå denne. Konsekvenslogikken innebærer dermed at ulike handlingsalternativer må vurderes ut fra sine respektive forventede konsekvenser. Dette er altså i tråd med hvordan Hollnagel (2018) beskriver betydningen av både overvåking og evnen til å respondere. En kan derfor argumentere for at formålsrasjonaliteten og konsekvenslogikken som ligger til grunn for det

instrumentelle perspektivet også er en forutsetning for evnen til å kunne respondere til riktig tid og på riktig måte.

Forventningen om at handlinger er formålsrasjonelle og følger en konsekvenslogikk medfører altså at organisasjonen velger handlinger og aksjoner ut fra hva som er best egnet til å oppnå det definerte målet, eller best egnet til å oppnå en ønsket idealtilstand.

Endringer i omgivelsene vil påvirke hva som kan betraktes som formålsrasjonelle handlinger, og i følge konsekvenslogikken vil aktørene tilpasse seg «sitt nære handlingsmiljø» slik at de fremdeles er i stand til å oppnå sine definerte mål (Christensen, Egeberg, Lægreid, Roness og Røvik, 2015, s. 45). Det ligger altså en forutsetning om at organisasjonene må kunne overvåke omgivelsene de opererer i for å kunne opptre formålsrasjonelt.

Tverbråten og Knutsen (2019) beskriver hvordan det er en forventning i et instrumentelt perspektiv at organisasjonen utfører beslutningsprosesser systematisk, der målsetningen ved aktivitetene defineres først, før alternative fremgangsmåter for å oppnå målet vurderes. Å definere en målsetning innebærer at organisasjonen må bestemme hva som er den ønskede tilstanden, og hvor langt unna en er fra å oppnå denne, som også er en forutsetning for overvåking av organisasjonens funksjonsevne og -tilstand i Resilience Engineering-perspektivet.

Men i organisasjoner kan det være flytende, uklare eller direkte motstridende målsetninger, og tilhørighet eller plassering i organisasjonen har også betydning for aktørenes interesser og kapasitet til å gjennomføre beslutningsprosessen (Tvetbråten og Knutsen, 2019). Videre kan aktørene ha ulik eller begrenset evne til å innhente relevant informasjon om forskjellige alternativer og deres medfølgende konsekvenser. «Det betyr at aktørenes informasjonstilgang påvirker deres beslutningsgrunnlag» (Tvetbråten og Knutsen, 2019, s. 401). Begrensninger i evnen til å kontrollere alle tilhørende faktorer og til å gjøre en rasjonell beregning betyr at ut fra det instrumentelle perspektivet må man i realiteten peke på *begrenset* rasjonalitet for å kunne forstå og forklare organisasjoners handlinger (Tvetbråten og Knutsen, 2019).

For å forklare olje- og gasselskapers rolle i forhold til hybride trusler ut fra et instrumentelt perspektiv må en altså forvente at virksomhetene:

a. Styrer sin adferd og handlinger etter rasjonelle regler, det vil si at intensjonene og konsekvensene bak handlingene er forståelige og forutsigbare.

b. Baserer intensjoner og målsetninger ut fra en definert ønsket tilstand, og vurderer og analyserer hvilke virkemidler som er best egnet for å oppnå denne tilstanden.

c. Velger de virkemidlene som gir best effekt for å opprettholde virksomhetens normale drift og for å minimere faren for tap av verdier.

Det institusjonelle perspektivet

I det institusjonelle perspektivet ligger det en forventning om at organisasjoner enten vil handle i tråd med den kulturen som er etablert i organisasjonen eller i tråd med de forventningene som omgivelsene har. Det institusjonelle perspektivet kan altså inndeles i kulturelle og symbolske handlinger i organisasjonene (Andreassen og Bjørkelo, 2020).

Det kulturelle institusjonelle perspektivet

Det kulturelle institusjonelle perspektivet legger vekt på de uformelle reglene, normene og verdiene som eksisterer og er etablert i en organisasjon (*«slik fungerer det i denne organisasjonen»*). Dette innebærer at handlinger ikke nødvendigvis følger formelle eller offisielle styringssignaler (Tvetbråten og Knutsen, 2019). Ledelsens betydning vil derfor variere avhengig av situasjonen, og være påvirket av hvordan organisasjonens identitet, verdier og antagelser har utviklet seg og blitt en del av organisasjonen over tid (Andreassen og Bjørkelo, 2020). I det kulturelle institusjonelle perspektivet kan ulike subkulturer innad i organisasjonen altså gjøre avstanden mellom Work-as-imagined og Work-as-done (Hollnagel, 2018) større. I tillegg etableres og utvikles organisasjonens kultur og eventuelle subkulturer seg gradvis, og endringer kan derfor være svært vanskelig og ta lang tid.

I organisasjonene vil beslutningstakerne påvirkes av de uformelle reglene, normene og verdiene som er etablert, og disse vil altså ikke kunne endres og tilpasses nye omgivelser og vilkår like lett som det for eksempel forutsettes i et instrumentelt perspektiv (Tvetbråten og Knutsen, 2019). Det vil si at den erfaringen organisasjonen har med eksisterende virkemiddelbruk og handlingsmønster påvirker organisasjonens adferd og beslutningsprosess (Tvetbråten og Knutsen, 2019). For organisasjoner som har en veldig sterk kulturell identitet og styring kan det derfor være utfordrende å kunne raskt endre seg og tilpasse seg nye funksjonsbetingelser slik Resilience Engineering-perspektivet forutsetter, med andre ord være utfordrende i forhold til å opptre på en resilient måte.

For å forklare olje- og gasselskapers rolle i forhold til hybride trusler ut fra et kulturelt institusjonelt perspektiv må en altså forvente at virksomhetene:

a. Handler i tråd med og holder fast ved rutiner og praksis som er etablert internt.
b. Har en avventende holdning til endringer i omgivelsene.

Det symbolske institusjonelle perspektivet

Det symbolske institusjonelle perspektivet, eller myteperspektivet, tar utgangspunkt i hvordan eksterne normer påvirker organisasjonens utforming og funksjon, og hvordan organisasjonen tilpasser seg omgivelsenes forventninger («*slik forventer andre at vår organisasjon fungerer*»).

Sentralt i dette perspektivet er hvordan handlingsmønsteret i organisasjonen utgjør et system av normer, basert på omverdenens eller samfunnets forventninger og oppfatninger. Dette kan forstås som at organisasjonen tilpasser seg forventninger fra omgivelsene, og at handlinger derfor må være akseptable for organisasjonens omgivelser (Tvetbråten og Knutsen, 2019). I følge det symbolske institusjonelle perspektivet vil organisasjonene søke utover mot samfunnets og omgivelsenes etablerte normer for å få aksept for sine handlinger, uavhengig av om handlingene vil være effektive eller ikke (Tvetbråten og Knutsen, 2019). Dette skiller seg med andre ord fra den konsekvenslogikken og formålsrasjonaliteten som ligger til grunn for handlinger i både det instrumentelle perspektivet, og i følge Resilience Engineering-perspektivet.

I det symbolske institusjonelle perspektivet vil altså en organisasjon følge og tilpasse seg sosialt etablerte og aksepterte normer og verdier. Når flere organisasjoner gjør dette, vil det gradvis etableres en organisatorisk likhet (Tvetbråten og Knutsen, 2019). Her skiller det symbolske institusjonelle perspektivet seg fra det kulturelle institusjonelle perspektivet, da det sistnevnte fører til at organisasjonene vil søke innover og utføre handlinger i tråd med sin egen internt etablerte kultur.

For å forklare olje- og gasselskapers rolle i forhold til hybride trusler ut fra et symbolsk institusjonelt perspektiv må en altså forvente at virksomhetene:

a. Tilpasser seg krav og forventninger som omgivelsene stiller.
b. Vil velge virkemidler og tilpasse seg i tråd med endringer i omgivelsenes normer og forventninger.

3. Metode

I dette kapitlet presenterer og forklarer jeg hvilket forskningsdesign og metode jeg har valgt for å kunne besvare spørsmålet stilt i problemstillingen, som introdusert i kapittel 1. I tillegg vurderes forskningsdesign og metode i forhold til reliabilitet og validitet. Hvilke utfordringer jeg har hatt i arbeidet med denne masteroppgaven, hvilke konsekvenser utfordringene har medført og hvordan de kan ha påvirket resultatet redegjøres også for.

Metodevalg og metodiske svakheter

Problemstillingen og oppgavens tematikk dreier seg om hybride trusler, som er et begrep som mangler en entydig og omforent definisjon (Reichborn-Kjennerud og Cullen, 2016, Cullen og Wegge, 2019). Samtidig oppfattes og beskrives ofte hybride trusler som komplekse og sammensatte problemer, preget av flere ulike og kanskje ukjente eller vanskelig detekterbare elementer. Jeg har derfor valgt en kvalitativ metode som tilnærming til å besvare og utdype problemstillingen i denne oppgaven. En kvalitativ metode kjennetegnes ved en tilnærming som har til hensikt å forstå, beskrive eller forklare fenomener sett fra et bestemt utgangspunkt, for eksempel fra informanters perspektiv (Nilssen, 2012, s. 13). En kvalitativ metode er derfor en egnet tilnærming til å forstå og analysere hvilken betydning det kan ha at det eksisterer ulike oppfatninger relatert til hvordan begrepet hybride trusler gis mening og innhold. En kvalitativ metode gir også mulighet til å fordype seg i tematikken og gi en større forståelse for hvilke faktorer som påvirker og har betydning for å besvare problemstillingen.

I oppgaven ønsker jeg å finne svar på og danne en dypere forståelse for hvordan olje- og gasselskaper oppfatter sin egen rolle i forhold til hybride trusler, og hvordan de oppfatter at hybride trusler påvirker deres evne til å opprettholde normal funksjon og drift. Det krever at jeg har måttet samle inn empiriske data fra ulike informanter i virksomheter tilknyttet petroleumssektoren for å forstå deres perspektiver, og analysere hvordan de beskriver sitt forhold til og forståelse av sin egen rolle i et hybrid trusselscenario.

I metodevalget ligger altså et premiss om at de ulike informantenes subjektive oppfatninger og meninger er representative som empirisk grunnlag, det vil si at de kan generaliseres videre som generelle oppfatninger og meninger som er representative for deres respektive organisasjoner og for petroleumssektoren. Dette er selvfølgelig et svakt premiss, da informantene bare representerer et begrenset utvalg personer, som i tillegg er valgt bevisst på

bakgrunn av at de har en funksjon eller arbeidsoppgave knyttet til oppgavens tematikk i sine respektive virksomheter.

Det empiriske datagrunnlaget er samlet inn gjennom en serie informantintervjuer, og representerer og baseres altså på informantenes egne meninger, opplevelser og erfaringer. I tillegg vil mine egne perspektiver og tolkninger kunne påvirke hvordan de empiriske dataene analyseres og presenteres. Datagrunnlaget representerer et «informantsubjektivt empirisk grunnlag» (Tjora, 2021, s. 37), og må også forstås ut fra den helhetlige konteksten, eller rådende forhold i omgivelsene. I denne oppgaven har kontekst spesielt betydning i forhold til hvordan hybride trusler har fått svært økt eksponering og medieomtale i forbindelse med Russlands angrep og krigføring mot Ukraina. Intervjuene ble gjennomført i perioden februar-mars 2022, og dette tidsintervallet dekker både opptakten og forløpet til invasjonen og den første fasen av krigen. Det vil derfor være naturlig å anta at informantene har reflektert og satt seg mer inn i tematikken enn det som kanskje ville vært naturlig under andre omstendigheter. Leseren må altså være oppmerksom på at både informantenes og min egen virkelighetsoppfatning er preget av kontekst, og at denne i større eller mindre grad vil ha innvirkning på måten empirien presenteres, analyseres og drøftes.

Forskningsdesign og -strategi

Forskningsdesign peker på hvordan et forskningsprosjekt utformes og hvilken fremgangsmåte som velges for gjennomføringen av forskningsprosjektet. Forskningsdesign innebærer altså synliggjøring og begrunnelse for alle valg som gjøres når forskningsprosjektet planlegges og utformes, og hvordan forskningsprosessen videre knytter sammen problemstilling, forskningsspørsmål, innsamling og analyse av empiriske data før en er i stand til å konkludere. Altså hvordan forskeren har tenkt å komme frem til sine konklusjoner. Forskningsdesignet danner et rammeverk for hva som vil bli studert, samt hvorfor og hvordan dette vil bli studert, og fungerer som en guide eller ledetråd gjennom forskningsprosessen.

Abduktiv forskningsstrategi

Forskningsstrategi følger av forskningsdesign og kan beskrives som hvorvidt den fremgangsmåten og resonneringen som benyttes for å kunne besvare problemstillingen og forskningsspørsmålene er gyldig og følger alminnelig logikk. Det finnes flere ulike forskningsstrategier, blant annet deskriptiv, induktiv, deduktiv og abduktiv, som hver for seg beskriver og representerer ulike tilnærminger til å finne svar på problemstillingen og

forskningsspørsmålene. I et forskningsprosjekt kan en eller flere forskningsstrategier anvendes, så lenge de er relevante for å kunne svare på problemstillingen.

I denne oppgaven har jeg valgt å benytte meg av en abduktiv forskningsstrategi. Denne tar utgangspunkt i empirien, men tar også hensyn til betydningen av ulike teorier og perspektiver, både i forkant og i løpet av forskningsprosessen (Tjora, 2021). Empiriske data samles altså inn, analyseres og drøftes innenfor et teoretisk rammeverk. Denne koblingen mellom empiri og teori kommer spesielt til uttrykk i tre områder i oppgaven: For det første er forskningsspørsmålene utformet som både empirisk og som teoriutforskende (henholdsvis forskningsspørsmål nummer 1 og 2-3). Videre er intervjuspørsmålene som er stilt til informantene utformet på bakgrunn av det teoretiske rammeverket, og i tillegg er de empiriske dataene klassifisert og analysert på bakgrunn av det teoretiske rammeverket.

Gjennom en abduktiv forskningsstrategi har jeg hatt som mål å forstå og beskrive olje- og gasselskapenes oppfatning og forståelse av egen rolle i forhold til hybride trusselscenarier, og hvordan denne eventuelt påvirker deres oppfatning av selskapenes evne til å opprettholde normal funksjon og drift. Dette er gjort gjennom å analysere informantenes oppfatninger, forklaringer og meninger i forhold til problemstilling, forskningsspørsmål og det teoretiske grunnlaget. Gjennom å intervjue et utvalg informanter søker jeg å få en bedre forståelse for hvordan de ser tematikken og problemstillingen fra deres ståsted, eller med andre ord å forstå deres syn ut fra deres «ontologiske tilnærming» (Engen, et al., 2016). Dette danner grunnlag for hvordan det empiriske datagrunnlager kan forstås.

Gjennom denne prosessen ønsker jeg å utlede eller oppnå ny og dypere forståelse for tematikken, og anvendelse av teorien i forhold til denne. En abduktiv forskningsstrategi er altså ikke nødvendigvis ute etter en unik logisk slutning, men søker å gi en plausibel tolkning som kan testes, kritiseres og eventuelt bekreftes gjennom andre forskningsprosjekter (Dey, 2004, s. 91).

Datakilder og innsamling av datamateriale

Det empiriske datamaterialet i denne oppgaven er samlet inn gjennom en serie intervjuer, og kan beskrives som primærdata. Primærdata defineres typisk som data forskeren selv har samlet inn, analysert, beskrevet og presentert. Dette er altså førstehåndsinformasjon som forskeren deler og bygger sin forskning på, i motsetning til for eksempel sekundærdata som er

innsamlet av andre enn forskeren selv, gjerne i form av publiserte rådata og statistikk. Bruk av primærdata innebærer at det er liten avstand mellom forskeren og den originale datakilden.

Intervjuer

Som beskrevet over, er hovedkilden til empiriske data i denne oppgaven intervjuer med nøkkelinformanter innenfor petroleumssektoren. Andersen (2006) beskriver nøkkelinformanter som «personer som antas å ha særlig god oversikt over og innsikt i et spørsmål forskeren ønsker å få belyst» (Andersen, 2006, s. 279). Dette vurderer jeg som en hensiktsmessig tilnærming, da informantenes bakgrunn, erfaring, funksjon og arbeidsoppgaver bringer både kunnskap og informasjon som kan gi en bredere og dypere forståelse for tematikken og danne bedre grunnlag for å kunne besvare problemstilingen og forskningsspørsmålene. I en slik setting gjøres mye av den utforskende og kreative delen av forskningen i selve intervjusituasjonen (Tjora, 2021, s. 144).

Valg av informanter

Som Tjora (2021, s. 145) beskriver, er det i et kvalitativt studie en hovedregel å velge ut informanter basert på hvorvidt de kan uttale seg på en reflektert måte om tematikken, eller med andre ord at informantene representerer et strategisk utvalg.

Til denne oppgaven startet jeg med en liten gruppe potensielle informanter som jeg kjente på forhånd og som jeg visste hadde kunnskap om temaet gjennom sine arbeidsoppgaver og ansvarsområder. Disse «førstekontaktene» satte meg i kontakt med andre potensielle informanter, slik at utvalget gradvis vokste etter hvert som jeg fikk flere tips om nye potensielle kandidater. En slik rekruttering av informanter kalles gjerne for «snøballmetoden» (for eksempel Tjora, 2021, s. 150). En ulempe med metoden er at den kan begrense variasjonen i informantenes oppfatninger, bakgrunn og erfaring, samt at det kan være vanskelig å få «snøballen til å slutte å rulle» (Tjora, 2021, s. 151).

Det siste opplevde jeg, og det gjenstod fremdeles flere potensielle informanter som ikke ble kontaktet og intervjuet da jeg bestemte meg for å avslutte datainnsamlingen. Jeg valgte hovedsakelig å avslutte datainnsamlingen for å gi tilstrekkelig tid til dataanalyse og videre sammenstilling og arbeid. Samtidig var mitt inntrykk at datagrunnlaget som allerede var samlet inn var tilstrekkelig, og at det ikke syntes å komme så mange nye synspunkter og avvikende perspektiver i forhold til de eksisterende. Men som Tjora (2021, s. 158) beskriver, kan dette også skyldes at det eksisterende informantutvalget representerer en relativt homogen

gruppe. Det kan med andre ord argumenteres for at informantene jeg har intervjuet ikke er utvalgt på bakgrunn av representativitet – altså at de representerer et tverrsnitt av ansatte i norsk petroleumssektor, men på bakgrunn av deres hensiktsmessighet til oppgavens formål. Altså at de er valgt fordi de kan bidra med kunnskap, oppfatninger og erfaringer som i større grad vil utdype og bidra til å forstå kunnskapsgrunnlaget for tematikken og problemstillingen bedre. Dette kan være en utfordring i forhold til å kunne generalisere og trekke konklusjoner på vegne av hele sektoren, og påvirker dermed forskningsresultatenes validitet.

Til slutt endte jeg opp med ti informanter, som alle har sine primære arbeidsoppgaver knyttet til prosjektstyring, sikring og/eller tilsyn innen petroleumssektoren og nært tilgrensende sektorer. Informantene kommer fra tre ulike operatørselskaper og to ulike tilsynsmyndigheter. De tre operatørselskapene har ulik størrelse. To av disse opererer flere produserende felt, og har en aktiv rolle innen leting og utforskning av nye ressurser på norsk sokkel. Det siste operatørselskapet har ikke selv operatøransvar for produserende felt, men er en aktiv operatør for både letelisenser og for et utbyggingsprosjekt som vil bli satt i produksjon i nær fremtid. Alle disse tre operatørselskapene er selvstendige norske juridiske enheter, men har i større eller mindre grad utenlandske eierinteresser og/eller hovedkontor i utlandet.

De tre operatørselskapene representerer bare et lite utvalg av selskapene som er aktive på norsk sokkel, men jeg vurderer at de tre operatørselskapene som er valgt gir et representativt tverrsnitt eller bilde av norske olje- og gasselskapers oppfatning av hybride truslers betydning. I tillegg valgte jeg å inkludere informanter fra ulike tilsynsmyndigheter. Disse fører tilsyn med virksomheter på tvers av sektoren, og har derfor en annen oversikt og perspektiv, eller et mer overodnet helhetsinntrykk enn det en kan forvente av informanter fra enkeltstående virksomheter. Tabell 1 gir en oversikt over informantene, deres organisatoriske tilknytning og en kort beskrivelse av deres rolle og funksjon i de respektive virksomhetene.

Informant	Virksomhet	Beskrivelse av funksjon/rolle	Type intervju
Informant #1	*Operatørselskap A*	*Rådgivning innen virksomheten. Skape forståelse for sikringsrisiko og gi beslutningsgrunnlag i form av trussel- og risikobilde*	*Individuelt*
Informant #2	*Operatørselskap B*	*Hovedsakelig en rolle innen beredskap, men utarbeider også sikringsrisikoanalyser*	*Individuelt*
Informant #3	*Operatørselskap C*	*Representant for selskapet i driftslisenser og som myndighets-kontakt*	*Individuelt*
Informant #4	*Tilsynsmyndighet A*	*Avdelingsleder med faglig og administrativt ansvar for sikring*	*Individuelt*
Informant #5	*Operatørselskap B*	*Primært ansvar knyttet til sikringsrisiko/risikostyring og utarbeidelse av trusselanalyser*	*Individuelt*
Informant #6	*Operatørselskap C*	*Ansvar for IT-drift, spesielt i forhold til cybersecurity og fysisk tilgang til enheter*	*Individuelt*
Informant #7	*Operatørselskap C*	*Lederrolle, med blant annet ansvar for sikring i virksomheten, samt i beredskapsorganisasjonen*	*Individuelt*
Informant #8	*Tilsynsmyndighet B*	*Rådgivning innen sikring og tilstøtene fagområder*	*Gruppe*
Informant #9	*Tilsynsmyndighet B*	*Rådgivning innen sikring og tilstøtene fagområder*	*Gruppe*
Informant #10	*Tilsynsmyndighet B*	*Rådgivning innen sikring og tilstøtene fagområder*	*Gruppe*

Tabell 1 *Oversikt over informanter*

På bakgrunn av sine roller og funksjoner var det flere informanter som uttrykte et ønske om anonymisering i oppgaven. Jeg har derfor valgt å ikke identifisere noen informanter eller virksomhetene informantene representerer.

Gjennomføring av intervju

Forberedelser; intervjuguide og informasjonsskriv

I forkant av intervjuene ble det utarbeidet en intervjuguide med spørsmål som jeg ønsket å stille til informantene, både fordi svar på enkelte konkrete spørsmål ville gi dypere forståelse og innsikt i tematikken, men også for å kunne strukturere intervjuene og styre samtalene. Spørsmålene er til en viss grad utformet på bakgrunn av teorien, og bidrar på denne måten til å knytte empiri og teori sammen. Spørsmålene er strukturert på en sånn måte at intervjuet kunne starte med innledene spørsmål knyttet til den overordnede tematikken og informantenes generelle oppfatning av begrepet «hybride trusler». Deretter følger spørsmål knytttet mer direkte til informantenes egen rolleforståelse og deres oppfatning av rolleforståelsen i sine respektive virksomheter og sektoren generelt. Videre følger spørsmål knyttet til informantenes oppfatning av hvilken evne virksomhetene har til å oppfatte, forstå og forutsi videre utvikling av et trusselscenario. Avslutningsvis ville jeg gi informantene mulighet til å komme med utfyllende kommentarer og refleksjoner om temaet, altså å «snakke fritt» dersom de skulle ha mer informasjon de følte var relevant og ikke allerede dekket av spørsmålene, samt gi de mulighet til å foreslå andre potensielle informantkandidater. Dette kan beskrives som oppvarmings-, refleksjons- og avslutningsspørsmål (Tjora, 2021).

At intervjuene følger den samme strukturen er en styrke for oppgavens reliabilitet, da det empiriske datagrunnlaget som kommer fra intervjuene vil være mer konsistent og repeterbart. Intervjuene ble gjennomført over en tidsperiode på ca. en måned, og at intervjuene fulgte den samme strukturen bidrar til å gjøre dataene mindre kontekstavhengig – siden konteksten endret seg gjennom denne perioden, blant annet ved Russlands angrep i Ukraina. I tillegg bidrar en felles struktur for alle intervjuene til å gjøre det lettere for meg som forsker når jeg i neste fase skal sammenstille, sammenligne og analysere datagrunnlaget.

Spørsmålene i intervjuguiden ble utformet litt ulikt for intervju med informanter fra tilsynsmyndigheter sammenlignet med intervju med informanter fra de ulike operatørselskapene. Dette reflekterer forutsetningen om at tilsynsmyndighetene har større anledning til å se på tvers av sektoren, og det var derfor interessant å stille spørsmålene på en slik måte at disse informantene kunne fokusere mer på helhetsbildet og -inntrykkene. Intervjuguidene til informanter fra operatørselskap og tilsynsmyndigheter er lagt ved denne oppgaven som henholdsvis Vedlegg A og Vedlegg B.

For å demonstrere problemstillingens relevans og for å gjøre det lettere for informantene å konkretisere sine oppfatninger og meninger valgte jeg å introdusere et case som utgangspunkt for noen av spørsmålene. Dette caset omhandler utforskning av olje- og gassresurser i Barentshavet.

Relevansen til caset i forhold til oppgavens tematikk og problemstilling er gitt blant annet ved Politiets sikkerhetstjeneste (2020), som peker på at informasjon om utforskning og eventuelt fremtidig utvinning av olje og gass har interesse for flere andre lands myndigheter. Det kan også være i andre lands interesse å så tvil om norsk troverdighet som en sikker og forutsigbar petroleumsleverandør, for eksempel ved å forstyrre norsk gassleveranse til Europa (Politiets sikkerhetstjeneste, 2020). Nettopp Barentshavet er vurdert til å ha potensiale for store gjennværende gassressurser (Oljedirektoratet, 2020), og påvisning og fremtidig utbygging av gassfelt her kan bidra til å sikre fortsatt stabil og økt norsk gasseksport til Europa (Gassco, 2020). Men økt petroleumsvirksomhet i Barentshavet er omdiskutert og kan åpne for konflikter. Økt norsk gasseksport til Europa kan komme i konflikt med både Russlands betydning og rolle som gassleverandør til Europa, og tilsvarende påvirke Europas avhengighet av Russland som gassleverandør. I tillegg kan økt petroleumsvirksomhet i Barentshavet også komme i konflikt med politiske partiers og miljøorganisasjoners interesser. Barentshavet har også strategisk betydning, og norsk aktivitet i dette området har betydning for utenriks- og sikkerhetspolitiske forhold, spesielt i den nåværende sikkerhetssituasjonen i Europa. Dette gjelder ikke bare forholdet til Russland, men også i økende grad forholdet til andre land og organisasjoner, for eksempel EU og NATO. En ytterligere faktor ved å velge et case knyttet til utforskning av olje- og gassresurser i Barentshavet er at eventuelle sårbarheter kan være mer tydelige, og dermed lettere for informantene å forholde seg til. Det gjelder spesielt geografiske forhold, som for eksempel store avstander mellom forsyningsbaser og forhåndslagre for oljevernutstyr (NOFO, u.å.). Alle de tre operatørselskapene som er representert med informanter har operert og vært aktive i Barentshavet, og har derfor i utgangspunktet inngående forståelse for utfordringene som caset viser til.

I tillegg til intervjuguide ble det utformet informasjonsskriv for å gi informantene bakgrunnsinformasjon for mitt valg av tema og hvilken kontekst data fra intervjuet vil bli benyttet i. Dette informasjonsskrivet forklarer hvorfor jeg ønsker å intervjue de forskjellige informantene, hvilken tematikk jeg utforsker, hvordan intervjuet er tenkt gjennomført, og ikke minst hvilke rettigheter informantene har i forhold til deltagelse og personvern.

Informasjonsskrivet inneholder også en samtykkeerklæring, der informantene bekrefter at de vil delta og at de har mottatt informasjon om sine rettigheter. Informasjonsskrivet er lagt ved denne oppgaven som Vedlegg C.

Alle informantene fikk tilsendt intervjuguide og informasjonsskriv med bakgrunnsinformasjon i god tid forut for intervjuene. Dette gjorde at informantene kunne stille forberedt og at de hadde reflektert noe over tema og problemstilling før intervjuet. Jeg kunne dermed forvente nyanserte og gjennomtenkte svar og innspill. En risiko ved denne fremgangsmåten er at informanter som ikke føler at de har nok kunnskap om temaet på forhånd benytter anledningen til å «lese seg opp» og henter informasjon fra andre kilder. I slike tilfeller vil ikke svarene informantene gir i samme grad reflektere dere egne meninger og oppfatninger, men heller referere andre kilder.

Semistrukturerte intervju

Jeg har valgt å benytte en semi-strukturert intervjuform, det vil si at intervjuene bærer preg av en relativt fri samtale mellom informanten og intervjueren, der samtalen «kretser rundt noen spesifike temaer som forskeren har bestemt på forhånd» (Tjora, 2021, s. 127). Hensikten med å gjennomføre datainnsamling ved semi-strukturerte intervjuer er å få informantene til å reflektere over egne erfaringer og oppfatninger knyttet til temaet for oppgaven. Intervjuformen følger en struktur og dynamikk preget av åpne spørsmål der informantens respons i stor grad styrer samtalen (Andersen, 2006, s. 279). Samtidig peker Andersen (2006) på at i samtaler med informanter som sitter på stor kunnskap og forståelse for problemstillingen vil en mer aktiv og bevisst intervjuer- eller forskerrolle kunne gi bedre analytisk kontroll. Dette benevner Andersen som «aktiv samtalebasert intervjuing», og kan bidra til å øke forskningens validitet og reliabilitet.

Til sammen ble det gjennomført åtte intervjuer med ti informanter. Syv av disse intervjuene ble gjort individuelt og ett som gruppeintervju med tre informanter. Selv om jeg var bevisst på at informantene kunne påvirke hverandres svar og uttrykksform i en gruppeintervjusetting, opplevde jeg ikke at gruppeintervjuet la noen demper på informantenes vilje til å dele sine egne subjektive meninger eller erfaringer. Halvparten av intervjuene ble gjennomført virtuelt som video- eller telefonintervjuer, mens de resterende intervjuene ble gjennomført fysisk. Disse ble holdt på informantenes arbeidssted. At noen intervjuer ble gjennomført virtuelt kan i noen tilfeller være en svakhet, da uttrykksformer som for eksempel kroppsspråk ikke blir like tydelig oppfattet (Tjora, 2021, s. 183). Jeg var bevisst på dette, og forsøkte å kompensere for

denne utfordringen ved å bygge en viss relasjon til de aktuelle informantene gjennom korte møter eller telefonsamtaler i forkant av intervjuene. Jeg oppfatter ikke at datagrunnlaget ville endret seg i større grad dersom også disse intervjuene hadde blitt gjennomført fysisk.

Hvert intervju varte mellom 50 og 90 minutter og opplevdes som en relativt åpen samtale, men styrt ut fra spørsmålene som var forberedt i intervjuguiden. Intervjuformen, og at intervjuene langt på vei bar preg av å være en åpen samtale, gjorde det lett å kunne stille oppklarende- og oppfølgingsspørsmål for å belyse tematikken fra ulike vinkler og få en bredere forståelse for informantenes syn. Dette bidro også til å oppklare eventuelle misforståelser underveis, og flere ganger ledet informantenes svar naturlig til videre diskusjon og nye oppfølgingsspørsmål der jeg kunne gå i dybden i forhold til det aktuelle temaet spørsmålene var knyttet til. Denne fleksibiliteten som et semi-strukturert intervju gir er viktig for å kunne få fram og utdype eventuelle nyanser og forskjeller i informantenes rolle- og begrepsforståelse, men kan også gjøre det vanskeligere å etterprøve og sammenstille de innsamlede dataene.

Jeg var bevisst på at informantene skulle forstå hva jeg var ute etter i forhold til tematikk og bakgrunn, så hvis informantene oppfattet eller opplevde spørsmålene som upresise eller uklare prøvde jeg så langt som mulig å forklare eller omformulere spørsmålene.

I flere av intervjuene opplevde jeg at samtalen og informantenes svar dekket flere av spørsmålene som var formulert i intervjuguiden samtidig, eller at svarene overlappet. I tillegg ble noen spørsmål ikke besvart i alle intervjuene, enten fordi de ikke ble ansett som relevant i forhold til informantens bakgrunn og erfaring, eller fordi tiden ikke strakk til.

Jeg valgte å hverken gjøre lyd- eller bildeopptak av intervjuene, men i stedet skrive fortløpende notater i stikkordsform. Dette valget gjorde jeg delvis på grunn av personvernhensyn og delvis for å senke tempoet i intervjusituasjonen, for å dermed gi informantene mer tid til å tenke og reflektere over spørsmålene underveis. En sideeffekt var at jeg selv også fikk mer tid til å reflektere, og kunne stille bedre oppfølgings- og oppklarende spørsmål. En svakhet ved dette valget er at notatene ikke nødvendigvis alltid er presise og nøyaktige i forhold til alle utsagn, og at sitater derfor kan miste noe av sin kontekst. Videre kan det være utsagn eller svar som jeg har gått glipp av eller ikke fanget opp i notatene, og som derfor ikke er inkludert i det empiriske datagrunnlaget. Dette er svakheter som kunne vært unngått ved å i stedet gjøre lydopptak av intervjuene, men samtidig peker Andersen

(2006, s. 291) på at lydopptak også kan skape en viss ufrihet i samtalen. For å kompensere for svakhetene som valget mitt om å skrive notater innebar, var jeg var veldig bevisst på og benyttet ofte anledningen til å stille oppklarende spørsmål for å sikre at jeg hadde forstått informantenes utsagn riktig.

Etterarbeid, transkribering av intervjuer og finskriving av notater

Umiddelbart etter at intervjuene var gjennomført sørget jeg for å renskrive notatene og gå fra stikkordsform til å gjengi en fullstendig samtale slik jeg oppfattet den. Jeg anså det som svært viktig å gjøre dette umiddelbart etter intervjuene, slik at jeg hadde samtalen «friskt i minne» og fremdeles kunne forstå både utsagnenes kontekst og meningsinnhold. Ved ett tilfelle ble de transkriberte notatene korrigert noe av informanten i ettertid, og dette gjaldt særlig i forhold til å gi korrekte henvisninger til publikasjoner og regulativer.

Transkribering eller omforming fra muntlig til skriftlig form er ikke mulig å gjøre på en helt objektiv måte (Tjora, 2021, s. 185). For eksempel vil kroppsspråk, og om informanten er usikker og nøler eller leter etter ord, være vanskelig å synliggjøre i transkribert form. Samtidig betyr min rolle, der det er jeg som både leder intervjuet, står for transkripsjon i ettertid og bearbeiding og analyse av dataene, at jeg dermed har bedre anledning til å fange opp og inkludere subtile signaler og meninger fra informantene. Dette peker på styrken ved å bruke primærdata som det viktigste datagrunnlaget.

Datareduksjon og analyse

Uansett hvilken metode som er valgt og anvendt for å samle inn data, kreves det en passende kategorisering, sortering og registrering, eller omstilling, av dataene før de kan analyseres og behandles videre. Å bryte ned og kategorisere data omtales ofte som koding (Nilssen, 2012). Det neste steget er å finne sammenhenger og sammenstille kodene, og etter hvert redusere datamengden til man sitter igjen med noen få kategorier som «fanger opp essensen av datamaterialet» (Nilssen, 2012, s.78), og er relevant for videre analyse og drøfting i forhold til problemstillingen.

Datarelevans, analyse og tolkning

For å avgjøre hvilke data som var relevante, eller hvilke data som var nødvendig for å svare på problemstillingen, valgte jeg å ta utgangspunkt i både måten intervjuguidene var utformet og i teorigrunnlaget. Dette er i tråd med en abduktivt forskningsstrategi, som beskrevet tidligere, og er en måte å knytte empiri og teori sammen.

Intervjuguidene er grovt sett inndelt etter tre hovedtema. Første del handler om informantenes oppfatning av begrepet «hybride trusler» og hvordan det benyttes i virksomhetene. Neste del omhandler hvordan informantene oppfatter rolleforståelse, før siste del peker på hvilken oppfatning informantene har av virksomhetenes evne til å oppfatte, forstå og forutse en videre utvikling av et hybrid trusselscenario. Første del støtter seg på teorien og betraktningene rundt hybride trusler presentert i kapittel 2, mens de to neste delene i stor grad peker tilbake på teorien rundt både rolleforståelse og Resilience Engineering-perspektivet.

Det empiriske datagrunnlaget er relativt omfattende. Gjennom reduksjon og utvelgelse i forhold til hvilken relevans dataene har med tanke på informantenes begrepsforståelse, oppfatning av egen rolle og ikke minst relevans i forhold til de fire grunnelementene i Resilience Engineering-perspektivet, ble datamengden både mer håndterbar og ga meg et godt grunnlag for å besvare forskningsspørsmålene og spørsmålet som stilles i problemstillingen.

Gjennom analysen er dataene altså kategorisert ut fra min forståelse av det teoretiske grunnlaget. Hver del er analysert adskilt, og enkelte utsagn kan ha relevans og være inkludert i flere kategorier. Samtidig har det vært viktig for meg å forstå og bevare helheten i informantenes utsagn, noe som kommer til uttrykk i både presentasjonen av det empiriske datagrunnlaget i kapittel 4, og i videre drøfting i kapittel 5.

Betraktninger rundt validitet og reliabilitet

Begrepene validitet og reliabilitet viser i grove trekk til henholdsvis i hvilken grad resultatene fra et studie er gyldige, og i hvilken grad studiet kan etterprøves. Med andre ord uttrykker et studies validitet hvorvidt de konklusjoner som gjøres stemmer med det som forskningen har avdekket. Reliabilitet derimot peker på om de resultatene som forskningen har avdekket er avdekket på en slik måte at de er pålitelige, altså at det er en sammenheng mellom empiri, analyse og resultat (Tjora, 2021). Dette innebærer også at forskningen må kunne gjentas og oppnå et tilsvarende resultat.

Det er en generell utfordring ved et kvalitativt studie at kontekst og subjektive oppfatninger preger forskningen fra start til slutt. Denne trenger heller ikke å være den samme gjennom hele forskningsprosessen, men kan godt endre seg i takt med omgivelsene eller etter hvert som forskeren oppnår en dypere innsikt og forståelse for temaet. Min egen forforståelse av tematikken har også vært med å prege og forme oppgaven, og hvordan problemstillingen er utformet. Som Nilssen (2012, s. 68) uttrykker, omfatter ikke forforståelse bare det teoretiske

grunnlaget eller rammeverket, men også de erfaringer, verdier, holdninger og meninger forskeren bringer med seg inn i studiet. Dette kan også påvirke studiens begrepsvaliditet, eller med andre ord hvorvidt de empiriske dataene som samles inn faktisk er objektivt sett relevante i forhold til intensjonen om å besvare oppgavens problemstilling.

Jeg har mitt daglige arbeid i et operatørselskap på norsk sokkel, og har i perioder blitt eksponert for tilsvarende problemstillinger som den jeg har formulert i denne oppgaven. Dette preger og påvirker selvsagt min forforståelse, og kan komme til uttrykk i måten de empiriske dataene er behandlet, analysert og drøftet. I tillegg har også informantene en tilknytning til petroleumssektoren, noe som automatisk gir en relasjon mellom forsker og informant. Til sammen kan dette påvirke studiets reliabilitet, da det ikke er gitt at en annen forsker uten tilsvarende bakgrunn eller tilknytning til petroleumssektoren ville utformet studiet likt og dermed kommet til samme konklusjoner.

I tillegg har så godt som alle informantene i en eller annen form sine primære arbeidsoppgaver og ansvar knyttet til sikringsrisiko og vurdering av trusselbilder. Det betyr at en kan forvente at de har relativt lik bakgrunn og forforståelse, i hvert fall grovt sett. Dette kan medføre at bredden i datamaterialet er begrenset, og at et bredere utvalg av informanter fra sektoren kunne påvirket forskningsresultatene i en annen retning. Dette påvirker studiens ytre validitet, altså hvorvidt resultatene og data fra et begrenset utvalg informanter kan generaliseres og gjelde for et større utvalg enn det som er representert her. Dette er også en effekt av «snøballmetoden» ved rekruttering av informanter, som beskrevet tidligere.

At alle intervjuene er utført etter og følger samme intervjuguide bidrar til å styrke reliabiliteten, da andre forskere også vil ha mulighet til å repetere intervjuene. Selvfølgelig ligger det en svakhet eller utfordring i at informantene er anonymisert, så å repetere intervjuene med de eksakt samme informantene vil vanskelig la seg gjøre.

At informantene er anonymisert kan betraktes som både en styrke og en svakhet for oppgaven. Anonymisering tillater at informantene i større grad kan uttale seg fritt, uten å bekymre seg for å senere bli gjenkjent og/eller konfrontert med sine uttalelser. Det er også grunn til å tro at informantene kunne ha vært mer restriktive i forhold til å dele informasjon og oppfatninger dersom de eller deres virksomheter kunne bli identifisert. I tillegg tillater anonymisering at informantene deler mer av sine egne subjektive oppfatninger, da de ikke risikerer at det i samme grad oppfattes som om de uttaler seg på vegne av sine respektive

virksomheter. Dette er med å styrke studiets validitet. Samtidig gjør anonymiseringen av informantene det ekstra utfordrende, om ikke umulig, for andre forskere å repetere intervjuene. Det kan argumenteres for at dette påvirker og svekker studiets reliabilitet.

Etiske hensyn og vurderinger

Datasikkerhet og personvern

Før datainnsamlingen kunne starte var det nødvendig å innhente tillatelse fra Norsk senter for forskningsdata (NSD). Dette skyldes at personopplysninger fra informantene ville bli behandlet i arbeidet med oppgaven, og gjelder opplysninger som navn, arbeidssted og stilling eller arbeidsfunksjon, samt kontaktinformasjon som telefonnummer og e-postadresser. Det kunne dermed være mulig for utenforstående å identifisere informantene, og godkjenning fra NSD var derfor nødvendig. NSDs vurdering av forskningsprosjektet er lagt ved oppgaven som Vedlegg D.

Flere informanter ønsket at hverken de selv eller deres virksomheter skulle kunne identifiseres. En slik anonymisering innebærer at datamaterialet blir bearbeidet og presentert på en slik måte at ingen enkeltpersoner eller virksomheter kan gjennkjennes, og gjelder både de som konkret har bedt om å bli anonymisert og andre. Jeg har gjort dette ved å sikre at informantenes personopplysninger ikke knyttes direkte til de enkelte intervjuene eller utsagn og sitater, hverken i notater, transkriberte gjengivelser av intervjuene eller presentasjon av datamaterialet i oppgaven.

Andre etiske hensyn

Som diskutert tidligere, representerer rekruttering av informanter ved hjelp av «snøballmetoden» en ulempe, og som beskrevet av Tjora (2021, s. 151) kan det være vanskelig å opprettholde forskningsetiske krav når informanter «angir» hverandre. Dette skyldes at opplysninger om andre informanters deltagelse kan gjøres kjent ved at de «nomineres» av deltakere som allerede er en del av forskningsstudiet. I ytterste konsekvens kan dette komme i konflikt med personvernforhold og krav som stilles i forhold til anonymisering.

Et annet moment er at hybride trusler mot Norge både er og oppfattes som reelt. Det kan være utfordrende for informanter å peke på eller avsløre sårbarheter i egen virksomhet, sektor eller for den saks skyld i samfunnet som helhet. Dette gjelder spesielt i den nåværende konteksten med krigen i Ukraina og energikrise i Europa som bakteppe. Jeg har derfor vært tydelig i

intervjuene på at jeg er ute etter generelle betrakninger, ikke etter konkrete objekter eller forhold. Jeg har også informert om at det er helt greit dersom informantene ikke kan eller ønsker å svare på enkelte spørsmål. Dette var også tilfelle ved et par anledninger ved spørsmål informantene ga klart uttrykk for at de ikke ville eller kunne kommentere og svare på.

Det er en utfordring å kunne vise til at transkriberte notater og skriftlig gjengivelse av samtalene representerer en korrekt gjengivelse av informantenes egentlige utsagn og meninger. Andersen (2006, s. 291) uttrykker det på denne måten: «Noen ganger brukes informantintervjuer kun som bakgrunn for å tolke og forstå, mens fakta kan dokumenteres uavhengig av samtalen. Andre ganger er det viktig å kunne dokumentere hva som faktisk er blitt sagt. Informanter kan i etterhånd huske samtalen på en annen måte, eller forandre mening på en måte som har betydning for forskerens beskrivelse og analyse». Som det også er diskutert og vist til tidligere kan datamaterialet bli påvirket av mine egne subjektive oppfatninger og ikke minst av konteksten intervjuet foregikk i. For eksempel kan jeg ha blitt påvirket av meninger og refleksjoner som har kommet frem i tidligere intervjuer, og dermed ubevisst tillagt nye informanter tilsvarende meninger. Dette gjelder både under intervjuene, ved transkribering og finskriving av notater, samt ved bearbeiding, analyse og presentasjon av endelige data, og er noe leseren må være oppmerksom på når oppgaven skal forstås.

4. Presentasjon av empiri

I dette kapittelet sammenstilles og presenteres det empiriske datagrunnlaget, innhentet gjennom intervjuer med representanter fra ulike deler av norsk petroleumsvirksomhet. For å kunne benytte og drøfte dette materialet videre i forhold til problemstilling og forskningsspørsmål, er det først nødvendig å kartlegge hvordan informantene selv beskriver begrepet «hybride trusler», noe som gir en indikasjon på hvorvidt sektoren har en felles oppfatning og forståelse av begrepet, eller om det er avvik. Videre presenteres informantenes oppfatning av sine egne og petroleumssektorens roller i et hybrid trusselscenario, før datamaterialet brytes ned og kategoriseres i henhold til de fire grunnelementene som påvirker virksomhetenes evne til å fungere på en resilient måte (Hollnagel, 2011).

Informantenes forståelse av begrepet «hybride trusler»

Generelt viser intervjuene at det er en relativt samsvarende forståelse blant informantene for hva begrepet hybride trusler innebærer. Alle informantene peker på hybride trusler som sammensatte og komplekse hendelser, og at de representerer hendelser som man ikke nødvendigvis umiddelbart forstår hensikten bak – det vil si at fra informantenes perspektiv kan det være uklart hva en trusselaktør egentlig ønsker å oppnå. Videre utdyper informantene at hybride trusler innebærer at trusselbildet er uklart og sammensatt av mange elementer, der alt kan inkluderes. Men også virkemiddelbruken er sammensatt, over et bredt spekter, og kan inneholde kombinasjoner av både åpne og skjulte virkemidler. Selve virkemiddelbruken beskrives som at den kan ha forskjellig karakter sett fra ulike sektorer, men søker å oppnå ett bestemt mål eller resultat.

I et intervju påpeker informantene det at det er viktig å kunne skille mellom hva som ligger i en trussel, og når trusselen eventuelt utarter seg til en hendelse eller et angrep. Altså at begrepet «trussel» peker på noe som ikke er manifestert ennå, i motsetning til et faktisk angrep.

Noen av informantene mener at hybride trusler først og fremst må betraktes fra et samfunnsperspektiv eller «makroperspektiv», som for eksempel illustrert ved dette sitatet fra intervju nummer åtte:

> *«Begrepet peker nok først og fremst på trusler som ikke primært er rettet mot objekter, men mot samfunnet».*

I flere av intervjuene påpekes det at hybride trusler ikke er noe nytt. Sammensatte og komplekse trusselscenarier har alltid forekommet, selv om begrepsbruken kanskje er ny. Riktignok vises det til at hybride eller sammensatte trusler i dag kanskje innebærer bruk av nye virkemidler, eller at virkemidler brukes på en annen måte. For eksempel sosiale medier, der kommunikasjon og informasjonsdeling er mye mer direkte og vanskeligere å kontrollere eller verifisere enn i tradisjonelle redaktørstyrte medier.

Slik en av informantene formulerer det, kan begrepet hybride trusler betraktes fra to synsvinkler. Sammensatt virkemiddelbruk er en vinkel, men begrepet kan også betraktes i forhold til hva som er det bakenforliggende formålet eller hensikten med trusselen. Denne kan kan være skjult eller uklar, men ofte knyttet til et større bakteppe, for eksempel hvordan trusselbildet lokalt i Norge kan forstås ut fra den pågående krigen mellom Russland og Ukraina. «Det handler om å forstå et helhetsbilde».

Informantene viser til flere ulike eksempler på hva slags virkemiddelbruk de normalt ser på som del av hybride trusler. Trusler i cyberdomenet er typisk, og nevnes av de fleste. Andre peker spesielt på påvirkningsoperasjoner og uklare hendelser i et lavkonfliktscenario. For eksempel vises det til hvordan lavintensive angrep kan ha langsiktig fokus, der sårbarheter som avdekkes kan utnyttes lenge etterpå. Etterretningsvirksomhet, som industrispionasje og kartlegging, brukes av de fleste informantene som et eksempel. De viser her til hvordan etterretningsvirksomhet kan danne grunnlag for senere bruk av maktmidler, og at den derfor må inkluderes som en del av begrepet. I tillegg viser flere til hvordan strategiske oppkjøp og endrede eierstrukturer har potensiale for å føre til sårbarheter som ikke er umiddelbart åpenbare, men som kan utnyttes på et senere tidspunkt.

I et av intervjuene nevnes det at informantens virksomhet har opplevd GPS-jamming under boreoperasjoner i Barentshavet. Det er også rapportert om dette i media i ulike sammenhenger (for eksempel Johansen, 2019 og NRK, 2019), og kan være et eksempel på en hendelse man ikke umiddelbart forstår hensikten med. Kanskje var formålet å teste norsk beredskap eller avdekke sårbarheter ved petroleumsvirksomheten i Barentshavet? Også mulige avledningsmanøvre nevnes som et eksempel, i betydningen at disse kan tvinge oss til å fokusere og rette oppmerksomheten mot «feil» område.

Flere informanter viser også til hvordan innsiderproblematikken alltid eksisterer. Det kan i denne sammenhengen bety at ansatte enkelt- eller nøkkelpersoner kan trues eller påvirkes til å

gjøre skade på innsiden. Faren for at noen kan komme seg innenfor skallsikring eller få tilgang til skjermede områder der de ikke normalt skal ha tilgang nevnes også.

Betydningen av begrepet «hybride trusler» innebærer også en forståelse for hvem de mulige trusselaktørene kan være. I intervjuene pekes det først og fremst på fremmede nasjonalstater, Russland og Kina nevnes spesielt, Iran og Pakistan i mindre grad. Dette er i tråd med de siste åpne trusselvurderingene publisert av Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet (henholdsvis Forsvaret, 2022, Politiets sikkerhetstjeneste, 2022 og Nasjonal sikkerhetsmyndighet, 2022). Bildet på fremmede nasjonalstater som trusselaktører kan illustreres ved sitatet nedenfor fra intervju nummer fem:

> *«De mest sansynlige trusselaktørene her vil nok være Russland og Kina. De er flinke til å legge aktivitetene veldig tett opp til det som må oppfattes som lovlig eller legitim aktivitet, noe som gir de en «plausible deniability»».*

Men informantene viser også til hvordan andre og mer utradisjonelle aktører kan utgjøre en trussel, for eksempel kan de opptre på vegne av fremmede nasjonalstater med sammenfallende mål. Det beskrives som at disse opptrer som «stedfortredere». Dette gjelder typisk aktører og miljøer som kan være vanskelig å forholde seg til, som for eksempel kriminelle grupperinger, noen NGO'er[2] og mer uorganiserte, ytterliggående eller militante miljøbevegelser, som etter hvert også kan tenkes å utgjøre en selvstendig trussel. Disse aktørene kan være multinasjonale og uten åpenbar politisk eller ideologisk forankring.

I intervjuene kommer det frem at informantene og virksomhetene av ulike årsaker i veldig liten grad fokuserer på et sammensatt helhetlig trusselbilde, slik de beskriver at et hybrid trusselbilde er. I stedet fokuserer de på enkelthendelser. Så lenge fokuset er på enkelthendelser, påpeker de at det har begrenset betydning hvem som står bak hendelsen. Den initielle håndteringen av enhver hendelse vil være lik. Det vil fort bare bli spekulasjoner om hva hensikten med en trussel egentlig er, og dermed lite konkret for virksomhetene å forholde seg til og bygge videre på. Samtidig påpekes det at det kan være viktig å forstå rasjonalet bak truslene for å kunne forberede seg og forebygge trusselen på best mulig måte. Andre

[2] NGO er en forkortelse for det engelske «Non-Governmental Organization». Store norske leksikon (u.å.) definerer dette som «en samlebetegnelse på ikke-statlige, frivillige organisasjoner, inkludert nærings- og fagorganisasjoner.»

informanter peker også på at kunnskap om hvem trusselaktøren er har betydning i forhold til hvem man vil kontakte og varsle, for eksempel av myndighetsorganer eller andre samarbeidspartnere.

Videre nevnes det at forståelse for hvem som står bak en trussel har betydning for å forstå trusselaktørens evne og kapasitet til å kunne påføre skade, hvor lenge trusselaktøren kan utføre en aksjon, og dermed hva skadepotensialet egentlig kan være. For et oljeselskap kan det også ha betydning for omdømmet hvem trusselaktøren er. Det vil for eksempel være en forskjell om trusselaktøren er en fremmed nasjonalstat enn om den er en miljøorganisasjon. Likevel påpekes det at omdømmerisiko primært har betydning for petroleumssektoren som helhet, ikke for enkeltselskaper.

På spørsmål om hvilken betydning hybride trusler egentlig har for informantene og deres respektive virksomheter svarer flere at det har liten betydning, i hvert fall på kort sikt. De ser relativt små konsekvenser for virksomhetene isolert sett.

De største sårbarhetene, slik det fremkommer i intervjuene, ligger i cyberdomenet og i virksomhetenes avhengighet av digitale verktøy og nettverksløsninger. De påpeker at det ligger en åpenbar sårbarhet i digitaliseringen av virksomhetene og deres respektive aktiviteter, så lenge de er avhengige av at disse fungerer. Det ligger også en bekymring for kompleksiteten i forholdet til leverandørkjeden, samarbeidspartnere og kontraktører til grunn for denne vurderingen. Sitatet nedenfor fra intervju nummer syv uttrykker denne sårbarheten gjennom informantens retoriske spørsmål:

> *«Vi vet egentlig ikke om vi har kontroll på alle kanalene inn i våre it-systemer. [Vet vi] For eksempel om riggselskapene har alt under kontroll?»*

Det er enighet blant informantene om at skadepotensialet er størst ved felt i drift, og da for eksempel gjennom dataangrep eller insidere med tilgang til styringssystemer som kan stoppe eller forstyrre driften av installasjoner. Dette nevnes spesielt ved ubemannede installasjoner som driftes fra og har sine kontrollrom på land. Generelt er det enighet om at alt som kan ramme «business continuity» og ha negativ påvirkning på den daglige driften har skadepotensiale, fordi det involverer en stor økonomisk faktor. Dersom produserende felt må stenge ned rammer det inntjeningen direkte.

En informant viser til hvordan ulike nettverksløsninger gjør virksomheten sårbar, og bruker skytjenester og ulike hjemmekontorløsninger som eksempel. Samtidig viser sitatet nedenfor fra intervju nummer syv hvordan en annen informant anser at nettopp dette samtidig kan bidra til å gjøre virksomheten mer robust:

> «*Litt ubevisst eller tilfeldig egentlig, men vi har blitt langt mer robuste de siste årene fordi blant annet IT-løsningene nå er sky-basert, med gode backuprutiner. I tillegg er det også den fysiske dimensjonen, etter noen år med hjemmekontor er vi ikke avhengig av å møte på kontoret. Vi kan jobbe og sørge for å opprettholde drift fra hvor som helst.*»

Petroleumssektoren som helhet anses som et attraktivt mål på grunn av sin strategiske betydning, både politisk og økonomisk. Dette illustreres under ved sitatet fra intervju nummer fire:

> «*Spesielt i forhold til krigen i Ukraina, og forløpet til denne, er det synlig at energi er et virkemiddel. At en trusselaktør kan ha noe å vinne på å forstyrre vår energiproduksjon og -leveranse er tydelig.*»

I tillegg peker flere på at virksomhetenes aktiviteter i nordområdene og Barentshavet kan gjøre dem til attraktive mål for trusselaktører, slik dette sitatet fra intervju nummer en viser:

> «*På grunn av dette selskapets operasjoner i nordområdene er det tenkelig at påvirkingsoperasjoner kan rettes mot enkeltpersoner eller mindre deler av organisasjonen lokalt.*»

Av andre sårbarheter som påpekes i intervjuene nevnes verdi- og leverandørkjedene spesielt. Dette skyldes at det er vanskelig å ha oversikt over hele verdikjeden; det vil si at det kan ligge sårbarheter langt nede i verdikjeden, så kunnskap om denne er viktig. Slik presiseres det blant annet i intervju nummer fire:

> «*Dette handler om «known unknowns» - det er sårbarheter som kan være kjent for noen, men ukjent for andre.*»

Som en annen informant påpeker er dette spesielt utfordrende fordi virksomhetene bare har begrenset mulighet til å kunne påvirke sårbarheter i verdi- og leverandørkjedene, for eksempel kun gjennom ulike bransjeforum. Videre påpekes det i ett intervju at verdikjeden ikke er

sektorspesifik, men har elementer som dekker mange sektorer. Den kan blant annet inneholde elementer fra e-komm, luftfart, maritim sektor og/eller kraftleverandører. Slik som illustrert i sitatet fra intervju nummer åtte:

> *«Alt henger sammen med alt. […] vi kjenner ikke alle sammenhengene og hvordan det vil påvirke oss til slutt.»*

I intervjuene blir det også uttrykt at hybride trusler på lengre sikt kanskje kan påvirke norsk forsvarsevne. Det er i hvert fall potensiale for at norsk politikk og det politiske rammeverket kan påvirkes. Sitatet fra intervju nummer fem viser betydningen av dette for norsk petroleumssektor:

> *«I et mer overordnet eller strategisk perspektiv vil påvirkning av politiske beslutningstakere og beslutningsprosesser, eller folkeoponionen for den del, ha stort skadepotensiale for virksomheten og petroleumssektoren, da selve vilkårene for vår aktivitet kan bli endret.»*

Men hva er det egentlig i virksomhetene selv som gjør dem sårbare? Flere av informantene peker på at de er sårbare på grunn av manglende bevissthet knyttet til trusselbildet. Virksomhetene, spesielt beslutningstakere, forholder seg til risiko som de allerede er kjent med, og ukjente trusler kan lett havne i en blindsone. Spesielt nevnes det at innsikt og kompetanse mangler for å kunne forstå og vurdere betydningen av et hybrid trusselscenario; det blir fort oppfattet som «konspiratorisk» og urealistisk. Grunnen til dette kan kanskje forklares ved at hybride trusler er vanskelig å kvantifisere, og dermed vanskelig å sammenligne med annen risiko, slik det uttrykkes i dette sitatet fra intervju nummer en:

> «*Sikringsrisiko baserer seg på en kunnskapsbasert tilnærming til risiko, noe som gjør det vanskelig for beslutningstakere og andre å forholde seg til – spesielt sammenlignet med mer kvantifiserbar risiko. […] Det kan føre til at annen risiko får mer oppmerksomhet.»*

Mangel på bevissthet og forståelse for hybride trusler blir også pekt på i intervju nummer fem:

> *«NSM poengterte i sin åpne trusselvurdering RISIKO 2021* (Nasjonal sikkerhetsmyndighet, 2021) *at virksomhetene har liten bevissthet i forhold til trusselbildet, og pekte blant annet på manglende implementering av sikkerhetsloven.»*

Som en av informantene påpeker har vi også en tendens til å overvurdere våre egne evner, spesielt når det kommer til å ha oversikt og forstå trusselbildet. Dette vises i sitatet fra intervju nummer fem:

> «*Selv om vi liker å tro det, har vi ikke i stor nok grad evnen til å drive kritisk tenkning, noe som igjen kan utnyttes av en trusselaktør.*»

Generelt er inntrykket blant informantene at begrepet hybride trusler er lite brukt og i hvert fall dårlig forstått blant de aller fleste ansatte i de ulike virksomhetene. Det er hovedsakelig kun i spesielle miljøer, som i sikringsmiljøene og IT-/informasjonssikringsmiljøene, at begrepet benyttes. Ut over disse miljøene, som jobber aktivt med å overvåke og forstå trusler, har begrepet svært lite fokus. Det eksisterer liten eller ingen generell forståelse for at enkelthendelser kan og bør ses i sammenheng med et større trusselbilde. Det påpekes riktignok av en informant at folk flest nok har en grunnleggende forståelse for begrepet «hybride trusler», men at de samtidig vil ha vanskeligheter med å kjenne igjen en reell trussel og forstå hva et slikt trusselbilde egentlig innebærer. Bare en virksomhet forklarer at begrepet er introdusert bredt i organisasjonen, som vist i dette sitatet fra intervju nummer åtte:

> «*Så lenge sikkerhetsmyndighetene benytter begrepet er det naturlig at vi også har adoptert bruken av det. Men forståelsen vil variere i forhold til arbeidsfunksjonene, for eksempel vil det være ulikt fokus blant de som jobber med beredskap og sikring.*»

Rolleforståelse i et hybrid trusselscenario

På spørsmål om hvilken oppfatning informantene har om sin egen og sin virksomhets rolle og ansvar i et hybrid trusselscenario svarer de fleste at de kun fokuserer på «angrep på oss selv». De har med andre ord kun fokus på sitt eget selskap og det som kan ha negativ påvirkning på egen drift og inntjening. Likevel anerkjenner informantene at dette gjør det utfordrende å skape en bred og overordnet situasjonsforståelse.

Selv om virksomhetene først og fremst ser sin rolle i forhold til å identifisere trusler rettet mot seg selv, er det altså også en anerkjennelse blant enkelte informanter at det er en verdi eller egeninterresse knyttet til å ha et så komplett trusselbilde som mulig. Sitatet fra intervju nummer fem antyder dette:

> «*I forhold til strategiske beslutninger har jeg inntrykk av at organisasjonen til en viss grad tar hensyn til hybride trusler, og da spesielt cybertrusler*.»

Noen informanter påpeker at dette også handler om virksomhetsstyring, der betydningen av å vurdere et helhetsbilde blir mer tydelig. Riktignok beskriver informantene at hybride trusler lett blir veldig abstrakt for beslutningstakerne, og at det er vanskelig for dem å se relevansen («dette treffer ikke oss»).

Som det påpekes i to av intervjuene kan det argumenteres for at norske selskaper også har et slags ansvar for samfunnssikkerheten i Norge, men at denne rollen er nok mer indirekte og ikke formelt definert. Det blir mer et spørsmål om hva samfunnet kan kreve av virksomhetene i et «totalforsvarsperspektiv». Sitater nedenfor fra intervju nummer åtte viser til dette:

> *«Generelt er selskapenes fokus på økonomi og inntjening. Det legger begrensninger på hva en tar på seg av ansvar. Men i et totalforsvarsperspektiv kan selskapene nok ha et ansvar, selv om det ikke er formelt definert. Hvem kan la være å bidra i en krise?»*

En informant peker på at petroleumssektoren fra utsiden oppfattes som relativt moden i forhold til sikringsrisiko, og at det er noe som har fått stadig større fokus og blitt mer og mer tydelig over tid. Informanten beskriver at det for eksempel kan skyldes hvordan angrepet på In Amenas-anlegget (Statoil, 2013) har ført til endret adferd i sektoren, men også som resultat av av det økende fokuset i samfunnet og i media.

Selskapenes størrelse har betydning. Informantene oppfatter det som at mindre selskaper ser et langt mer begrenset ansvarsområde enn de større. Sitatet fra intervju nummer åtte uttrykker hvordan selskapsstørrelsen har betydning:

> «*Her må man skille mellom de store driftsoperatørene og mindre selskaper med aktivitet i mindre skala. De store er nok veldig bevisst på sin egen rolle i forhold til forsyningssikkerhet og har en stor vilje til å opprettholde dette fokuset. De mindre selskapene vil typisk peke på andre, for eksempel på Gassco, i forhold til infrastruktur og leveranse-/forsyningssikkerhet.»*

Men hvem har egentlig ansvaret i et hybrid trusselscenario? Informantene peker først og fremst på at hybride trusler forekommer på et samfunns- eller makronivå, samt at truslene er sektoroverskridende, så det er og må være myndighetene som har ansvaret. Selv om noen informanter tydelig også peker på betydningen for virksomhetene i å se hendelser ut fra et helhetsperspektiv, er de like tydelig på at myndighetene har det endelige ansvaret. Som en

informant uttrykte det: «Dette havner fort hos politiet uansett». Disse to sitatene fra intervju nummer åtte viser også til denne problemstillingen:

> «V*i er veldig opptatt av å ikke ta på oss ansvar som ligger utenfor vårt klart definerte ansvarsområde.»*

> «*Når man snakker om hybride trusler tenker man fort på statssikkerhet og samfunnssikkerhet og hvordan disse overlapper.»*

Hvorfor vil ikke olje- og gasselskapene ta på seg et ansvar for sikring i forhold til et hybrid trusselscenario? Primært peker informantene på at virksomhetene deres ikke kan pålegges ansvar for å se et sektoroverskridende helhetsbilde. De har i beste fall kun et ansvar innenfor egen sektor. Alt ut over det blir vanskelig eller umulig å forholde seg til.

Som en informant utrykte det, har ikke selskapene et selvstendig ansvar for å bidra til samfunnssikkerhet – i så fall må det komme som et konkret krav fra myndighetene. I tillegg vises det til at det mangler koordinering på et overordnet nivå, som her sitert fra intervju nummer fem:

> *«Selv myndighetene vet jo ikke helt hvordan de skal håndtere et hybrid trusselbilde.»*

Av andre faktorer som informantene peker på er organisasjonenes modenhet viktig. Modenhet i organisasjonen påvirker evnen til å kunne se og analysere et helhetsbilde, og er dermed viktig for å forstå et hybrid trusselscenario. En informant uttrykker at evne til å vurdere et helhetsbilde krever mye ressurser og analysekapasitet for å kunne gi et brukbart beslutningsgrunnlag. Virksomhetene er derfor avhengig av å motta gode analyser og informasjon fra myndighetene, i tillegg til en stor intern kapasitet for å operasjonalisere og gjøre nytte av disse analysene og informasjonen.

Organisasjonskultur er også viktig. Som informantene fra ett selskap uttrykker det sitter virksomheten deres fast i en statisk selskapskultur, der det er vanskelig å utfordre eller stille kritiske spørsmål til det eksisterende. Det gjør det krevende å endre eller tilpasse virksomhetene til endringer i verden omkring, for eksempel til et dynamisk trusselbilde og arbeids- eller rammebetingelser i stadig endring. Det påpekes også at organisasjonene er veldig fragmentert i sine ansvarsområder. Dette kan både være litt tilfeldig og skyldes at organisasjonsstrukturen er lite gjennomtenkt. Eller som en informant uttrykte det: «fordi vi er veldig konservative og holder fast i gamle løsninger og strukturer».

På spørsmål om det finnes noen *formelle* krav eller forventninger til at olje- og gasselskaper også skal vurdere og ta stilling til hybride trusselscenarier er det litt delte meninger blant informantene. De fleste enige i at formelle krav, slik de for eksempel er uttrykt i lovverket, også kan dekke et hybrid trusselscenario. Som flere informanter påpeker er riktignok lovverket dekkende i en normalsituasjon eller -tilstand, men det blir mer uklart i et hybrid trusselbilde. Informantene kjenner heller ikke til at lovverk og myndighetskrav ikke har vært dekkende ved hendelser i et hybrid trusselscenario. Dette kan konkretiseres videre, slik det uttrykkes i dette sitatet fra intervju nummer fire:

> *«Det er ikke mangel på tiltak eller krav som er problemet i forhold til å kunne oppnå et tilstrekkelig sikringsnivå. Det skyldes mer mangel på kunnskap og forståelse.»*

Sitatet nedenfor fra intervju nummer fem viser også at det ikke er en grunnleggende oppfatning at myndighetene er i stand til å stille konkrete krav til at virksomhetene skal kunne fange opp alle typer risiko, for eksempel knyttet til en hybrid trussel:

> *«Selv myndighetene vet jo ikke helt hvordan de skal håndtere et hybrid trusselbilde. Ut fra det bakteppet kan en si at kravene ikke er dekkende.»*

Det pekes samtidig også på at de eksisterende kravene kanskje har «for stor maskevidde», er for generelle og ikke tilpasset dagens situasjon og teknologiske utvikling, som illustrert i de to sitatene nedenfor fra intervju nummer fire:

> *«For eksempel fører man personkontroll ved havneanlegg, men ikke kontroll med kjøretøy. Dette selv om dagens kjøretøy kan betraktes som rullende sensorer og potensielt kan brukes i kartleggingsøyemed.»*

> *«Regelverksimplementering er i hovedsak reaktiv, ikke proaktiv. Og det er regelverk myndighetene forvalter.»*

I forhold til hvorvidt myndighetene kan forvente at olje- og gasselskaper inkluderer hybride trusler i sine trusselvurderinger, peker informantene på at det allerede ligger en forventning fra myndighetene om at virksomhetene generelt skal ha en analytisk tilnærming til risiko, gjøre trusselvurderinger og tilpasse sin virksomhet og operasjoner til disse. Hvis trusselvurderingene gjøres godt nok, mener informantene at et hybrid trusselscenario også vil fanges opp. I følge en informant ligger begrensningene mer hos de som utarbeider trusselvurderingene og hvordan disse vurderingene påvirker organisasjonen, ikke i hva

regelverket sier. En annen informant påpeker også at regelverket representerer en minimumsstandard. Det er i mange tilfeller nødvendig å legge listen høyere enn det regelverket krever.

Generelt uttrykker informantene at hybride trusler nok er «indirekte regulert». For eksempel nevnes rammeforskriften (2010) som snakker om «beskyttelse av verdier», styringsforskriften (2010, §4) som peker på «risikoreduserende effekt» og petroleumsloven (1996, §9-3) som sier at sikringstiltak som kan *bidra til* å hindre bevisste anslag skal iverksettes.

Resilience Engineering i et hybrid trusselscenario

Slik det beskrives i kapittel 2, presenterer Hollnagel (2011) i Resilience Engineering-perspektivet fire elementer som påvirker og muliggjør organisasjoners evne til å kunne fungere på en resilient måte. Nedenfor er data fra intervjuene samlet og sortert i henhold til disse fire elementene; evnen til å kunne respondere, evnen til å kunne overvåke, evnen til å kunne lære og evnen til å være forutseende.

Evnen til å kunne respondere

En viktig faktor i organisasjonenes evne til å kunne respondere, er hvor raskt og effektivt en respons kan iverksettes. Informantene uttrykker at dette varierer, for eksempel sier en informant at det må være veldig tydelige signaler eller ligge en konkret trussel til grunn. Virksomhetene ser ikke eller fokuserer ikke på et overordnet (politisk) nivå, og vil ikke nødvendigvis respondere på hendelser eller vage signaler fra andre sektorer. En annen informant peker på selskapets størrelse som en faktor, som dette sitatet fra intervju nummer tre viser:

> *«At vi er en liten og transparent organisasjon med korte linjer er positivt. Vi kan potensielt reagere eller respondere raskt, deling og formidling av informasjon (for eksempel varsler om mistenkelige hendelser) er lett.»*

Dette sitatet antyder likevel en reaktiv holdning, der virksomheten først evner å respondere raskt hvis det vurderes som nødvendig etter en hendelse eller etter at en trussel er identifisert. En tredje informant viser til at de kun vil respondere på enkelthendelser eller -trusler, men nok samtidig vil vurdere om det virksomheten utsettes for kan være en del av en større kampanje. Det pekes her på betydningen av å ha forståelse for om en hendelse kan være en del av et sammensatt trusselbilde og/eller representere sammensatt virkemiddelbruk. Dette

kan i følge informanten ha betydning i forhold til å varsle andre deler av organisasjonen og få de til å forstå trusselbildet, samt for varsling til myndigheter, andre selskaper og samarbeidspartnere. Det vises også til at det kan ha betydning i tilfelle virksomheten må samhandle med andre – både myndigheter og/eller andre aktører.

Informantene utrykker altså at de ser at hendelser mot deres virksomhet også kan ha betydning for andre, og peker på at det er viktig å kunne dele mest mulig informasjon så tidlig som mulig. Riktignok, som en informant viser til, vil de ha større tillit til og tro på varsler som kommer fra noen man allerede har en relasjon til.

I forhold til *hvordan* virksomhetene vil respondere er det lite som er forberedt eller forhåndsdefinert. Dette kan også relateres til forståelsen av hybride trusler, da de kan innebære fullstendig ukjent eller uklar virkemiddelbruk. I intervju nummer seks uttrykkes denne problemstillingen slik:

> *«Det er anerkjent i organisasjonen at vi ikke kan sikre oss mot alt. [Vi] Har derfor større fokus på hvor raskt vi kan få systemer opp og gå igjen, og sikre så lite tap eller nedetid som mulig.»*

Informanten fortsetter å beskrive hvordan de vil ha ganske lav terskel for å iverksette tiltak. Det første tiltaket vil typisk være på «raised awareness» i organisasjonen, altså å formidle informasjon om trusselen eller hendelsen man står overfor.

Betydningen av manglende bevissthet i forhold til at virksomheten kan stå overfor en trussel eller hendelse påpekes også av andre informanter. Som for eksempel uttrykt i sitatet nedenfor fra intervju nummer syv:

> *«Det hele handler om manglende awareness i organisasjonen. Beslutningstakerne ser ikke og/eller har ikke eierskap til hele bildet […] vi har ingen scenariotankegang. Igjen mangler den strukturerte tilnærmingen.»*

Informanten fortsetter med å peke på hvordan ansvarsforhold i organisasjonen er veldig fraksjonert, og antyder at strukturen er lite gjennomtenkt, og at manglende forberedelser og organisering påvirker evnen til å respondere effektivt. Sitatet fra intervju nummer syv oppsummerer problemet ved virksomhetenens organisering slik:

> *«Vi har ikke noe fokus på en systematisk tilnærming, mangler helt ytelseskrav osv. […] Vi mangler mye på systematikk og planmessighet ved denne type hendelser og trusler. Vi vet ikke hvilke roller i organisasjonen som bør være involvert eller hvem dette kan ha betydning for. Her må vi bare improvisere!»*

Evnen til å kunne overvåke

Informantenes virksomheter driver i veldig begrenset grad selvstendig innhenting av data og overvåking av trender og indikatorer på et overordnet sektor- eller samfunnsnivå. De forklarer hvordan de er avhengig av å bruke informasjon fra eksterne kilder, og nevner for eksempel sikkerhetsmyndighetenes åpne trusselvurderinger, andre offentlige rapporter og beskrivelser av kjente hendelser, spesielt fra media. Videre nevnes også hvordan informantene i noen tilfeller mottar informasjon direkte fra relevante myndigheter, som for eksempel PST og NSM, gjennom bransjesamarbeid og nettverk, samt fra andre samarbeidspartnere og konsulenter. En informant peker spesielt på betydningen av å dele mest mulig informasjon mellom selskapene og samarbeidspartnere, og uttrykker at «å danne en felles situasjonsforståelse i industrien er et mål».

En informant peker på en forutsetning for å kunne overvåke og danne seg et godt bilde av virksomhetens funksjonsevne og -tilstand. Han viser til hvordan en god dialog med innretningene danner grunnlag for økt forståelse for hvor sårbarhetene ligger, mulige konsekvenser av hendelser, hvilke avhengigheter som er til stede og så videre. Dette peker også på et gjensidig forhold, der personell ute i organisasjonen eller på installasjonene får økt forståelse for betydningen av å overvåke funksjonstilstanden, og hva eventuelle avvik kan indikere. Ansvaret for overvåkingen flyttes dermed ut i organisasjonen, i stedet for at det kun legges på de som har som fagfelt å vurdere sikring og trusler.

Samtidig påpeker informantene fra ett selskap at ledelsen og virksomheten generelt har forventninger til at de skal kunne identifisere et bredt spekter av trusler og utarbeide helhetlige trusselvurderinger. Spesielt har dette fått fokus i forbindelse med nye store utbyggingsprosjekter.

Til tross for at alle informantene viser forståelse for betydningen av å kunne overvåke virksomhetenes tilstand, både internt og i forhold til omgivelsene, uttrykkes det at overvåking av indikatorer skjer tilfeldig – ikke systematisk. Det må være en spesiell grunn for at det skal gjennomføres, for eksempel at en konkret trussel er identifisert. Mye tilskrives mangel på

intern kapasitet og evne til å være forberedt og forutseende, slik sitatet fra intervju nummer en indikerer:

> *«I en ideell verden vil vi på forhånd ha utarbeidet en innhentingsplan og kartlagt hva som er indikatorene.»*

Som en annen informant uttrykker det, er indikatorer situasjonsbetinget. De må være basert på et spesifikt informasjonsbehov. Han påpeker videre at indikatorer har størst verdi i sanntid – på samme måte som at etterretning er ferskvare. Det blir da mye opp til virksomhetene selv å avgjøre hva de anser som viktig. Dette illustreres ved sitatet fra intervju nummer åtte:

> *«Enhver petroleumsaktivitet skal forholde seg til det aktuelle trusselbildet. Hvilket trusselbilde de skal forholde seg til må de selv vurdere.»*

Det kan altså være utfordrende å avgjøre hvor man skal fokusere. Det er opp til de ulike virksomhetene å selv identifisere risiko og avgjøre betydningen av denne. Kontekst er derfor viktig, slik dette sitatet fra intervju nummer åtte viser:

> *«I Norge er kanskje etterretningstrusselen viktigere enn sikring mot fysiske angrep, mens i andre land er det omvendt. Man må evne å skille mellom ulike trusselbilder.»*

Men hvilke momenter er det som gjør det vanskelig for olje- og gasselskaper å overvåke sin egen funksjonstilstand og det omkringliggende miljøet de opererer i? Informantene peker på en rekke utfordringer.

En informant peker på at det kan være vanskelig å bygge (de rette) relasjonene, for eksempel ved operasjoner i Nordnorge og Barentshavet, da det er langt unna informantens egen organisasjon. Dette kan utfordre evnen til å oppdage og forstå hybride trusler. Sitatet nedenfor fra intervju nummer to peker nettopp på utfordringene knyttet til relasjonsbygging:

> *«Det vil gjerne være nye folk som ikke kjenner lokale forhold, så nye relasjoner kan være utfordrende. Relasjonsbygging tar tid.»*

Informantene peker videre på at virksomhetene sliter med å se sammenhenger og det fremtidige potensialet i eventuelle hendelser. Verden betraktes ofte som statisk, og virksomhetene vurderer kun hendelser i et nå-perspektiv. Det vises også til hvordan den generelle manglende forståelsen og bevisstheten i virksomhetene gjør at de ikke nødvendigvis vil forstå at de utsettes for en hendelse i et hybrid trusselscenario, for eksempel en

påvirkningsoperasjon eller etterretning/spionasje. Informantene peker på at dette primært skyldes manglende erfaring, trening og kunnskap.

Slik en informant uttrykker det, kan det i utgangspunktet være nødvendig å stille spørsmål ved alle mulige avvik fra en normalsituasjon. Han utdyper videre hvordan alle avvik i utgangspunktet kan være mistenkelige, men at det er vanskelig å ta inn over seg hva betydningen av avviket er. Det gjelder både hva avviket skyldes og hva det kan føre til.

Oppfatningen av hvilken betydning det har å kunne innhente eller motta informasjon fra hendelser i andre sektorer eller andre land spriker blant informantene. En informant uttrykker at han tviler på at man umiddelbart vil tenke på sammenhenger, og forklarer det med at virksomheten nok fokuserer mest på operasjonell sikkerhet fra et teknisk perspektiv. Eksempelet i sitatet fra intervju nummer tre viser dette:

> *«For eksempel hvis vi mister kommunikasjon mellom land og rigg ville vi ikke umiddelbart tenkt på jamming[3], selv om vi vet at det forekommer.»*

Videre påpeker informantene at virksomhetene ikke sitter med all informasjon og oversikt over alle mulige hendelser, og dermed ikke vet hva som eventuelt kan være relevant. Virksomhetene vil ikke nødvendigvis fange opp hendelser som rammer andre sektorer, og de er derfor avhengig av å få konkret beskjed fra for eksempel myndighetene om at dette har betydning også for dem. At dette også gjelder evnen til å overvåke virksomhetenes egen funksjonsevne og -tilstand illustreres ved sitatet fra intervju nummer syv, der informanten også peker på effekten av virksomhetens interne organisering:

> *«Som organisasjon er vi veldig fragmentert, og det er vanskelig å ha et oversiktsbilde. Det er heller ingen vet hvem som eventuelt skal ha et oversiktsbilde.»*

Samtidig understreker flere informanter at hendelser og trusler mot andre virksomheter og sektorer kan ha stor betydning for dem. Dette gjelder spesielt på et mer overordnet eller strategisk nivå, for eksempel i forhold til verdikjede og underleverandører. Det vises også til hvordan det kan ha positiv betydning for virksomhetenes omdømme at de er oppmerksom på hva som skjer i andre sektorer. Men en bekymring luftes likevel av noen informanter. De har

[3] Jamming betyr i denne sammenhengen blokkering eller forstyrrelse av signal, for eksempel radiokommunikasjon eller datatrafikk.

inntrykk av at mye informasjon og detaljer deles i lukkede fora, som gjør at de dermed kan gå glipp av «essensielle biter i puslespillet».

Når det gjelder myndighetenes rolle i forhold til virksomhetenes evne til å overvåke egen tilstand og forholdet til omgivelsene, er informantene samstemte: *Myndighetene kan ikke vurdere de enkelte virksomheters evne til å overvåke og vurdere indikatorer på mulige trusler!* Informantene er tydelige på at myndighetene i utgangspunktet bare fører tilsyn med hvordan virksomhetene bruker lovverket, og hvordan virksomhetenes egne trusselvurderinger operasjonaliseres. Myndighetene kan altså ikke føre tilsyn med noe som ikke er forankret i lovverket.

Evnen til å kunne lære

Det er interessant å se på om eller eventuelt hvordan økt fokus og kunnskap fører til endringer i de ulike virksomhetene. Dette er selve essensen i læringsprosessen, slik det er beskrevet tidligere i kapittel 2. I forhold til organisasjonskultur og holdninger uttrykker en informant at toppledelsen i virksomheten hans har klare forventer at hans avdeling, som primært har ansvar for sikring og trusselanalyse, også skal bidra til å bygge og forbedre sikringskultur og sikringsbevissthet i organisasjonen. Dette er blant annet formalisert gjennom obligatoriske kurs for alle ansatte. Flere informanter gjentar hvordan økt bevissthet i organisasjonene virker forebyggende. Det gjelder også bevissthet om egne sårbarheter, ikke bare om potensielle trusler.

En annen informant forklarer at i hans virksomhet har de fokusert på å bygge et fagmiljø som har utviklet seg fra å være regelfokusert til å også ha et bredere og mer tverrfaglig kunnskapsområde, slik sitatet fra intervju nummer fire viser:

> *«Dette handler igjen om «kjente ukjente», altså at ulike miljøer sitter på ulik kunnskap og ulik forståelse for å kunne se sammenhengene. I forhold til sikringshendelser er det vanskelig å ha et forhold til noe når det ikke finnes noen empiri. Alt kan i prinsippet brukes som våpen eller virkemiddel for å oppnå et mål.»*

Samtidig peker flere informanter på at virksomhetene bare trener på håndtering av enkelthendelser, ikke på sammensatte og komplekse scenarier. De mangler derfor erfaring, trening og kunnskap i organisasjonene for å kunne drive effektiv læring i forhold til et hybrid trusselscenario. Likevel er det et forbehold, slik informanten i intervju nummer fem uttrykker det:

> *«På den annen side kan vi si at vi egentlig har trent på det uten å være klar over det. For eksempel ved covid har vi trent på scenarier som går over flere dimensjoner – der sikring har vært en av mange. Her har vi sett på konsekvenser langs mange forskjellige akser.»*

For virksomhetene er det vanskelig å kunne verifisere at læring faktisk har funnet sted så lenge det ikke finnes noe empiri eller datagrunnlag å sammenligne med. Sitatet nedenfor fra intervju nummer seks viser dette:

> *«Vi er forberedt på å møte trusler, men vet ikke hvordan vi faktisk hadde håndtert et større angrep.»*

En måte noen virksomheter adresserer dette dilemmaet vises i dette sitatet fra intervju nummer fem:

> *«Vi «sparrer» med andre analysemiljøer og -fora, både innenfor vår sektor og utenfor. […] Kunnskap fra noen andre sektorer vil være svært relevant, for eksempel luftfart, maritim sektor og e-komm, og selvfølgelig også finanssektoren.»*

Her benytter informantens virksomhet seg av et utvidet nettverk for å øke datagrunnlaget over mulige trusler og hendelser, og dermed hva som faktisk kan være relevant å lære fra.

Evnen til å kunne være forutseende

Når det kommer til virksomhetenes evne til å kunne være forutseende og tenke langsiktig, også i forhold til hybride trusselscenarier, indikerer de fleste informantene at de har et vanskelig utgangspunkt. Det pekes blant annet på at de bare har en generell forståelse og oversikt over trender og endringer i samfunnet. Videre, som en informant viser til, skjer langsiktige beslutninger – typisk store investeringsbeslutninger – kun basert på tekniske vurderinger og forretningsrisiko, som for eksempel prosjektøkonomi. Fremoverskuende og langsiktige trusselvurderinger og -scenarier inkluderes bare i veldig liten grad på norsk sokkel.

Samtidig pekes det på at hybride trusler nok har et større fokus og står noe høyere på agendaen blant beslutningstakerne nå. Som en informant uttrykker det bygger dette forventninger til sikringsmiljøene i virksomheten, og gir samtidig spillerom og mulighet for å kunne gå mer i dybden og være fremoverskuende. Informanten viser til at trusselvurderinger fokuserer mest på isolerte trusler, men at virksomheten også må ta stilling til hvordan det

overordnede trusselbildet presenteres. Dette viser riktignok hvordan virksomhetenes evne til å være fremoverskuende langt på vei er opp til enkeltpersoner eller mindre miljøer. Sitatet fra intervju nummer fem underbygger dette:

> *«Dette innebærer at det er mye opp til analytikeren som utformer trusselvurderingen hva som inkluderes i vurderingene.»*

Det er vanskelig for virksomhetene å vurdere hva som er fremtidens trusler, hvor de kommer fra og hvordan en skal forholde seg til disse. Som en informant påpeker, må det typisk en hendelse til for å eksponere sårbarheter, men informantene anerkjenner likevel behovet for å tenke langsiktig og være forutseende. Sitatet nedenfor fra intervju nummer åtte oppsummerer dette:

> *«Her kan man sammenligne virksomhetsstyring og etterretningsdoktrine, da begge handler om å innhente beslutningsgrunnlag. Vi må vite hva som kan utgjøre et problem i fremtiden og hva vi trenger å innhente mer informasjon om.»*

Oppsummering

Det empiriske datagrunnlaget som er presentert i dette kapittelet oppsummerer informantenes forståelse for begrepet «hybride trusler», hvilket innhold begrepet gis og hvilken betydning det har for informantenes virksomheter og sektor. Videre er informantenes syn på sine virksomheters roller og ansvar i et hybrid trusselscenario presentert, og til slutt er datamaterialet analysert og kategorisert i forhold til virksomhetenes evne til å legge til rette for å opptre på en resilient måte. Dette er gjort ved å samle og kategorisere data i forhold til de fire grunnelementene i Resilience Engineering-perspektivet, som introdusert i kapittel 2.

Datamaterialet bringes videre inn i neste kapittel, der det drøftes i forhold til teorigrunnlaget for å gi svar på forskningsspørsmålene og problemstillingen, som er presentert i kapittel 1.

5. Drøfting

Formålet med dette kapitlet er å drøfte funn som er gjort under datainnsamlingen og presentert i kapittel 4 i forhold til det teoretiske grunnlaget presentert i kapittel 2. Drøftingen tar utgangspunkt i problemstillingen, slik den ble formulert i kapittel 1:

> *Hvilken betydning har rolleforståelse for hvordan norske olje- og gasselskaper kan legge til rette for å fungere på en resilient måte i et hybrid trusselscenario?*

For å kunne svare på spørsmålet som stilles i problemstillingen er det først viktig å beskrive om norske olje- og gasselskapers oppfatning av hybride trusler er i tråd med den generelle beskrivelsen av hybride trusler presentert i kapittel 2. Her er det også viktig å vurdere hvorvidt det er en felles oppfatning blant informantene, eller om det er tydelige avvik. Dette vil gi en indikasjon på sektorens nåværende situasjonsforståelse i forhold til hybride trusler, og danne grunnlag for videre drøfting av hva et hybrid trusselscenario betyr for norske olje- og gasselskaper.

Drøfting av det empiriske datagrunnlaget sett i lys av teorien tar utgangspunkt i følgende tre forskningsspørsmål, slik de ble formulert i kapittel 1:

1. *Hvilke utfordringer oppfatter olje- og gasselskapene at hybride trusler representerer, både for dem selv spesielt og for sektoren generelt?*
2. *Er utfordringene av en slik art at Resilience Engineering-perspektivet kan være en hensiktsmessig tilnærming?*
3. *Kan olje- og gasselskapers eventuelle utfordringer i forhold til å kunne fungere på en resilient måte i et hybrid trusselscenario forklares ut fra hvordan deres rolleforståelse kan beskrives?*

Det første forskningsspørsmålet er av empirisk art. For å besvare dette tas det utgangspunkt i hvilke utfordringer som kommer frem i det empiriske datagrunnlaget presentert i kapittel 4. I forskningsspørsmål 2 utforskes hvordan Resilience Engineering-perspektivet kan beskrive og adressere utfordringene som norske olje- og gasselskaper oppfatter at hybride trusler representerer. For å besvare dette forskningsspørsmålet tas det utgangspunkt i teorigrunnlaget presentert i kapittel 2, og de fire grunnelementene som i følge Resilience Engineering-perspektivet har betydning for en organisasjons evne til å kunne fungere på en resilient måte.

Disse faktorene er: evnen til å kunne overvåke, evnen til å kunne respondere, evnen til å kunne lære og evnen til å være forutseende.

Teorien danner også grunnlag for å besvare forskningsspørsmål 3, der norske olje- og gasselskapers rolleforståelse i forhold til hybride trusler drøftes opp mot hvilken nåværende tilstand olje- og gasselskaper har og kan utvikle i forhold til sin egen evne til å fungere på en resilient måte. Hvilken betydning rolleforståelsen har for Resilience Engineering-perspektivet drøftes også i forhold til de organisasjonsteoretiske perspektivene introdusert i kapittel 2.

Norske olje- og gasselskapers oppfatning av hybride trusler

Intervjuene viser at hybride trusler er et begrep alle informantene har kjennskap til, og at det langt på vei er samsvar mellom informantene i forhold til å gi begrepet innhold og mening. Informantene beskriver et hybrid trusselbilde som sammensatt og komplekst, preget av mange ulike og kanskje ukjente elementer, samt at trusselbildet også kan knyttes til en større bakenforliggende kontekst. Flere informanter peker på at det kan være vanskelig å forstå hensikten bak konkrete trusler eller enkelthendelser i et hybrid trusselscenario, og at omfanget av den eventuelle trusselen ikke er åpenbart. Dette er noe som bidrar til å gjøre det ytterligere krevende å forstå og beskrive det faktiske trusselbildet, og ligger nært opp til hvordan hybride trusler beskrives som «wicked problem» i kapittel 2.

I et intervju kommer det frem at informanten betrakter begrepet hybrid *trussel* som at det innebærer at eventuell maktbruk ikke er manifestert ennå, i motsetning til et faktisk angrep. Det pekes altså på at det er et skille mellom en aktør som opptrer truende og en som faktisk går til angrep. I kapittel 2 refereres det til hvordan Society for Risk Analysis (2018) definerer trussel som en «varslet eller oppfattet intensjon om å angripe eller ramme en gitt verdi». I forhold til denne definisjonen kan hybride trusler altså betraktes som en foranledning og/eller varsel om at en trusselaktør har til hensikt å angripe og forsøke å ramme en verdi. Informantens argument om at hybride trusler ikke nødvendigvis innebærer manifestert maktanvendelse kan altså støttes ut fra denne definisjonen.

Likevel er det mulig å argumentere for at hybride trusler også kan inkludere aktiv bruk av virke- og maktmidler, ikke bare et varsel om fremtidig bruk. Det hele er avhengig av hvilket perspektiv man har. For eksempel kan trusler betraktes fra et individ-, virksomhets- og samfunnsperspektiv, og/eller fra et kort eller langt tidsperspektiv. Eksempelet nedenfor viser dette:

Dersom en forestiller seg at en trusselaktør har som mål å ramme Norges troverdighet som en stabil gassleverandør til Europa, en verdi som både er viktig for det norske samfunnet og for enkeltvirksomheter i norsk petroleumssektor, kan dette oppnås ved å angripe og ramme konkrete mål eller objekter. For eksempel ved å påvirke enkeltvirksomheters leveransekapasitet, ved å påvirke nøkkelpersoner i politiske beslutningsprosesser og/eller ved å blokkere knutepunkter i leverandørkjeden. Fra deres individuelle perspektiver kan slike virkemidler gjerne oppfattes som enkeltstående hendelser eller angrep, altså som «manifestert» maktbruk. Men fra et mer overordnet samfunnsperspektiv kan derimot slik virkemiddelbruk anses som en trussel eller intensjon om å ramme en overordnet samfunnsverdi – Norges troverdighet som gassleverandør. Makt- og virkemiddelbruken er altså ikke manifestert på samme måte når man betrakter det fra et samfunnsperspektiv som fra et individ- eller virksomhetsperspektiv. Det vil si at et direkte angrep på for eksempel et knutepunkt i leverandørkjeden ikke nødvendigvis betraktes som klart definert maktanvendelse rettet mot samfunnsverdien «Norges troverdighet som gassleverandør», men at angrepet likevel bidrar til å true denne samfunnsverdien.

Konsekvensene av virkemiddelbruken kan også ligge langt frem i tid, og det egentlige formålet – som i dette eksempelet var å ramme Norges troverdighet som gassleverandør – kan være skjult eller vanskelig å oppfatte. I et hybrid trusselbilde vil også trusselaktøren ønske å skjule hvem som faktisk står bak virkemiddelbruken. Dette synet er mer i tråd med hvordan Malerud et al. (2021) beskriver en trussel. I kapittel 2 er dette referert til som «hvordan en trusselaktørs mål, metode, fremgangsmåte og virkemiddel er satt sammen for å ramme et angrepsmål», og videre at det er måten ulike trusler kombineres som gjør det til en hybrid trussel. Her pekes det altså også på en underliggende hensikt om å ramme en verdi.

Et annet eksempel som illustrerer dette kommer fra informanten som fortalte at de hadde opplevd GPS-jamming under operasjoner i Barentshavet. Isolert sett er en slik hendelse i høyeste grad «manifestert maktbruk», men hva som egentlig var formålet med å benytte GPS-jamming som virkemiddel, altså hvilken verdi trusselaktøren faktisk truer, er fortsatt uklart.

Det er flere informanter som peker på at hybride trusler primært må betraktes fra et overordnet samfunns- eller makroperspektiv, slik sitatet nedenfor som også er referert til i kapittel 4 viser:

> «Begrepet peker nok først og fremst på trusler som ikke primært er rettet mot objekter, men mot samfunnet».

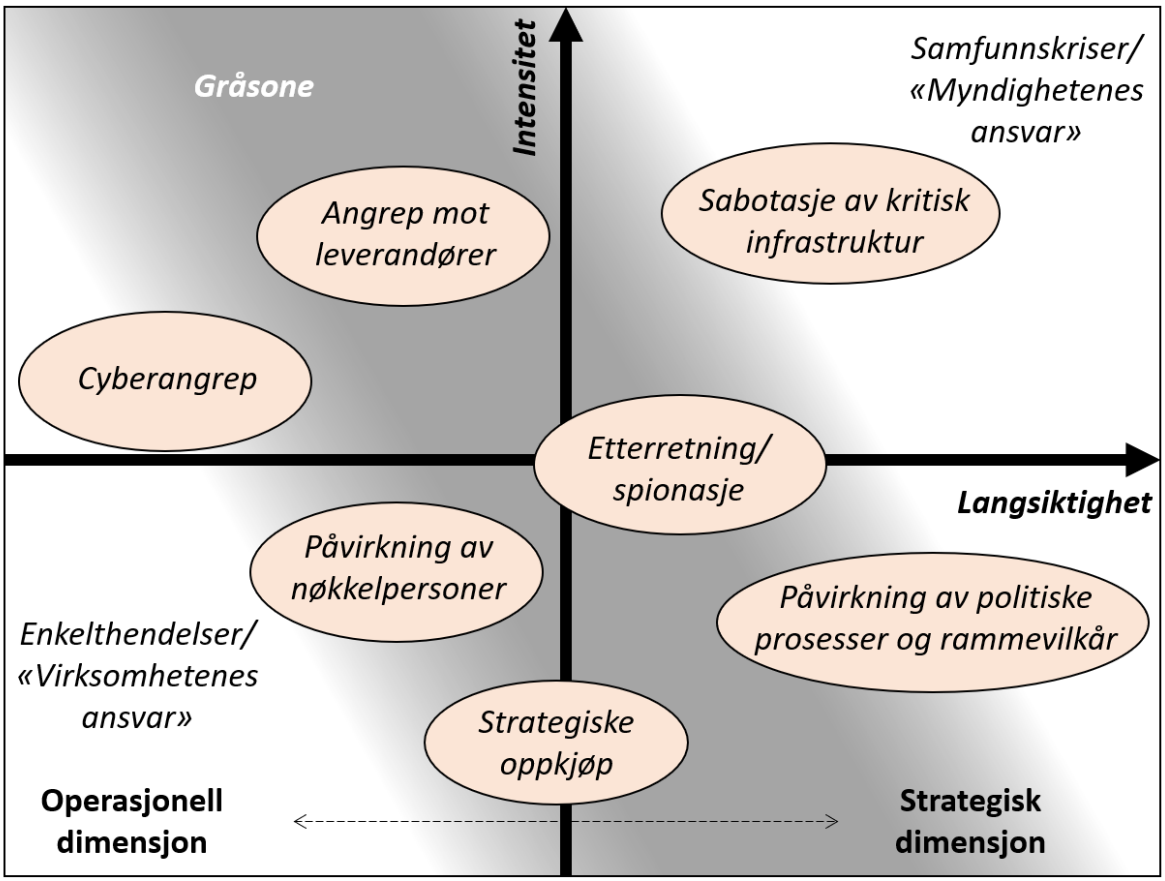
Dette argumentet understrekes også ved at informantene i stor grad peker på at hybride trusler har begrenset betydning for virksomhetene, i hvert fall på kort sikt. Virksomhetene retter fokuset innover, og fokuserer primært på enkelthendelser og angrep rettet mot dem selv. De vurderer ikke i særlig grad hvilken betydning disse hendelsene kan ha ut over egen sektor og for samfunnet som helhet. Samtidig blir det likevel nevnt at hybride trusler kan ha betydning for virksomhetene på lengre sikt, for eksempel dersom rammebetingelsene for norsk olje- og gassvirksomhet trues eller påvirkes.

At informantene generelt har lite fokus på samfunnssikkerhetsdimensjonen samsvarer også med inntrykket informantene etterlater om at de har lite fokus på sektoroverskridende trusler. Siden informantene faktisk beskriver dette av som et av kjennetegnene ved hybride trusler, underbygger det dermed deres oppfatning av at hybride trusler primært er et problem på samfunnsnivå - ikke på virksomhetsnivå. At samfunnsdimensjonen og betydningen av sektoroverskridende trusler bare nevnes av noen få informanter kan riktignok også skyldes at intervjusettingen og bakgrunnen for oppgaven retter spesielt fokus på petroleumssektoren. Men samtidig bekrefter flere informanter at de ikke ser langt utenfor egen sektor når det kommer til å vurdere et trusselbilde. Dette kan derfor tolkes som en generell utfordring i virksomhetene når det kommer til å forstå hybride trusler.

Det er mulig å skille informantenes oppfatning av hvilken betydning hybride trusler har i to dimensjoner: en kortsiktig operasjonell dimensjon, som fokuserer på virksomhetenes evne til å håndtere enkelthendelser og vurdere konkrete trusler rettet mot dem selv, og en mer langsiktig strategisk dimensjon, der betydningen av de store trendene i sektoren og samfunnet blir mer tydelig.

Dette er illustrert i Figur 3, som viser at jo mer intensiv og langsiktig eller langvarig virkemiddelbruken i et hybrid trusselscenario er, desto mer peker informantene på at det er myndighetene som har en rolle og et ansvar for å håndtere disse. Inntrykket er altså at jo mer langsiktig eller «fjernt» trusselbildet og hybride trusselscenarier er, desto mer pekes det på at myndighetene har det primære ansvaret. Holdningen «vi har kun ansvar for oss selv og vår virksomhet» er gjennomgående. Dette er i tråd med at virksomhetene anser sitt ansvarsområde som begrenset til å håndtere enkelthendelser og trusler rettet mot dem selv, mens

myndighetene har ansvar for håndtering av komplekse, sektoroverskridende kriser som kommer til uttrykk på samfunnsnivå.



Figur 3 *Trusseltypologi og klassifisering av hybride trusler i forhold til rolle og ansvar*

Figuren viser eksempler på ulike hendelser i et hybrid trusselscenario klassifisert ut fra intensitet og langsiktighet, altså hendelsens varighet og hvor lenge effekten eller resultatet av hendelsen har betydning. En klassifisering basert på intensitet og langsiktighet illustrerer også hvordan virksomhetene oppfatter en operasjonell og en strategisk dimensjon. I forhold til betydning og ansvar for håndtering av hendelser peker virksomhetene i petroleumssektoren i økende grad på myndighetene når hendelser klassifiseres i høyre del av figuren, og tilsvarende oppfatter virksomhetene at sitt ansvarsområde er begrenset til venstre del, eller den operasjonelle dimensjonen. Det oppfattes ikke noe tydelig skille mellom når ansvar går fra virksomhet til myndigheter, som illustrert ved gråsonen.

I intervjuene trekkes hovedsaklig fremmede nasjonalstater frem som mulige trusselaktører, først og fremst Russland og Kina. Dette er er i tråd med de åpne trusselvurderingene fra sikkerhetsmyndighetene, og er derfor forventet. Men det er interessant at flere informanter også trekker frem ikke-statlige organisasjoner og grupperinger som mulige trusselaktører i et

hybrid trusselscenario. I intervjuene kommer det riktignok frem at virksomhetene legger begrenset vekt på hvem de eventuelle trusselaktørene er. Dette skyldes igjen i stor grad at virksomhetene fokuserer på håndtering av enkelthendelser, og at disse sansynligvis vil håndteres likt uavhengig av trusselaktør.

Samtidig er det en utbredt oppfatning blant informantene at petroleumssektoren er et attraktivt mål i et hybrid trusselscenario, spesielt med tanke på å ramme produksjons- og leveransekapasiteten. I den konteksten blir det påpekt at det faktisk kan ha stor betydning å forstå hvem trusselaktøren er, da eventuelle hendelser også kan ha betydning ut over deres egen virksomhet. En informant understreker dette ved å vise til hvordan felles situasjonsforståelse og samarbeid i sektoren må være et ideal i et hybrid trusselscenario. Det er med andre ord avvikende oppfatninger av hvilken betydning det har for informantene å forstå hvem trusselaktørene er. Dette kan igjen tolkes som en indikasjon på at det er et skille mellom en operasjonell og en strategisk dimensjon, da informantene indikerer at fremmede nasjonalstater i et hybrid trusselscenario har langt større evne og kapasitet på strategisk nivå. Det gjelder både hvor lenge trusselaktørene er i stand til å drive sine aksjoner, hvor intensive virkemidler de er i stand til å mobilisere og hvilken kapasitet de har til å opptre skjult eller fordekt.

Informantene peker videre på at hybride trusler innebærer sammensatt virkemiddelbruk; at både åpenlyse og skjulte virkemidler kan benyttes over et bredt spekter. At cyberdomenet anses som mest utsatt er i tråd med norsk næringsliv generelt. I Hybridundersøkelsen (Næringslivets sikkerhetsråd, 2019) peker omtrent en tredjedel av respondentene på dette som den største sårbarheten. Det er riktignok interessant at informantene tilsynelatende legger større vekt på påvirkningsoperasjoner rettet mot enkeltpersoner enn det som kommer frem i Hybridundersøkelsen. Der peker bare en av ti respondenter på påvirkning av enkeltpersoner som en sårbarhet. Informantene som er intervjuet for denne masteroppgaven beskriver at påvirkningsoperasjoner både kan være rettet mot enkeltpersoner i de ulike virksomhetene, gjerne enkeltpersoner i nøkkelroller, og/eller rettet mot politiske beslutningstakere og folkeopinionen som helhet. Dette indikerer at individperspektivet også spiller en rolle i et hybrid trusselscenario.

I tillegg trekker noen informanter frem hvordan trusselaktører kan utnytte posisjonering i ulike maktposisjoner, for eksempel gjennom strategiske oppkjøp av virksomheter, som et

mulig strategisk virkemiddel i et hybrid trusselscenario. Dette kan være spesielt interessant for petroleumssektoren, som er en internasjonal industri med mange utenlandske aktører og eierinteresser. At skjulte eierskapsstrukturer kan utnyttes til å påvirke håndtering av hybride trusler er ikke utenkelig. Det er et paradoks at dersom det pekes på at petroleumssektoren har en rolle og et ansvar i forhold til norsk stats- og samfunnssikkerhet, kan dette innebære at mye av ansvaret legges på internasjonale selskaper med utenlandske eiere.

Igjen trekker informantene frem den strategiske og langsiktige dimensjonen når hybride trusler diskuteres. Ulike former for posisjonering, strategiske oppkjøp og bruk av økonomiske virkemidler for å oppnå strategiske mål er klassiske eksempler på virkemidler som har en langsiktig horisont, og oppfattes ikke som primære fokusområder for informantene og deres respektive virksomheter når et trusselbilde vurderes.

Også ulike former for avlendningsmanøvre er nevnt som virkemidler, i betydningen at de kan påvirke både situasjonsforståelsen og hvor enkeltvirksomheter, petroleumssektoren og samfunnet for øvrig retter sin oppmerksomhet. Som beskrevet i kapittel 1, viser blant annet Stian Schnelle (2018) til hvordan det å påvirke eller ramme motstanderens situasjonsforståelse kan være et mål for en trusselaktør i et hybrid trusselscenario, med hensikt å gjøre det enda vanskeligere å oppfatte trusselen og/eller identifisere hvem som står bak denne.

Når det gjelder hvor sårbarhetene er mest åpenbare for olje- og gasselskapene, trekker informantene spesielt frem at de er sårbare fordi de har manglende forståelse og trusselbevissthet knyttet til hybride trusler. Dette er i høyeste grad i tråd med norsk næringslivs generelle oppfatning. Som det vises til i kapittel 2 sier faktisk at hele 70% av respondentene i Hybridundersøkelsen at manglende evne til å gjenkjenne hybride trusler gjør dem sårbare, mens 63% også viser til at sårbarhet skyldes manglende situasjonsbevissthet i forhold til å oppfatte hvordan hybride trusler rettes mot virksomhetene (Næringslivets sikkerhetsråd, 2019, s. 5).

Dette kan også ses i sammenheng med informantenes uttalelser om at verdikjeden og de ulike forsyningskjedene er uoversiktlige, og at det derfor er vanskelig å vite hvor sårbarhetene egentlig ligger og hvor de er størst. Her trekkes det i tillegg frem at det kan være utfordrende og vanskelig for informantenes virksomheter å påvirke sårbarheter langt ute i verdi- og forsyningskjedene, blant annet fordi disse kjedene også er sektoroverskridende.

Informantene fra ett selskap påpeker at organiseringen og ansvarsforholdene i deres virksomhet er fragmentert, og at det derfor kan være uklart hvem som har det egentlige ansvaret for å identifisere trusler og iverksette respons ved eventuelle hendelser i et hybrid trusselscenario. Informantene gir inntrykk av at denne organisasjonen er motvillig til å endre seg og tilpasse seg nye trusselbilder. Her er det tydelig forskjell mellom selskapene og deres grad av modenhet i forhold til å kunne vurdere, utarbeide og presentere et trusselbilde for beslutningstakerne, da informantene fra et annet selskap viser til hvordan de er tildelt både ansvar og økte ressurser for å dekke dette, og hvordan deres vurderinger er anerkjent i hele virksomheten – også i toppledelsen.

I forhold til hvilke verdier som trues, er det interessant at informantene i første rekke peker på driftforstyrrelser, eller som det spesifiseres: «hendelser som kan ha negativ innvirkning på virksomhetenes daglige drift og inntjening». Det er interessant at hverken tap av konfidensiell informasjon, tap av fremtidige forretningsmuligheter eller tap av utenlandske partnere og kunder nevnes spesielt av informantene, selv om disse verdiene rangeres høyt i Hybridundersøkelsen (Næringslivets sikkerhetsråd, 2019, og referert til i kapittel 2). Her er det riktignok mulig å tolke at informantene inkluderer «tap av konfidensiell informasjon» som en verdi som trues av både cyber- og etterretningvirksomhet.

At disse verdiene ikke nevnes spesifikt av informantene kan også forklares ut fra informantutvalgets størrelse; til denne oppgaven er det utført åtte intervjuer med til sammen ti informanter, mens Hybridundersøkelsen er en kvantitativ undersøkelse basert på 354 intervjuer (Næringslivets sikkerhetsråd, 2019, s. 6). Et større datagrunnlag kan tenkes å utvide spekteret av verdier som trues i et hybrid trusselscenario. Men alt i alt avviker ikke bildet informantene gir sett fra deres respektive posisjoner i norske olje- og gasselskaper i særlig grad fra det generelle bildet av norsk næringslivs oppfatning av hybride trusler, slik det presenteres i Hybridundersøkelsen.

Påvirkning av politiske beslutningsprosesser nevnes bare i mindre grad som en verdi av betydning for informantene fra olje- og gasselskapene, og tap av omdømme anses å ha minimal betydning for enkeltvirksomheter, kun for petroleumssektoren som helhet. Dette viser igjen at informantene primært har fokus på det operasjonelle nivået, og ser lite på langsiktige og strategiske trusler og utfordringer, slik det tidligere er illustrert i Figur 3. At respondentene i Hybridundersøkelsen også peker på *tap av fremtidige forretningsmuligheter*

og *tap av utenlandske partnere og kunder* som verdier som trues i et hybrid trusselscenario, kan indikere at det er et høyere stratetegisk fokus blant norsk næringsliv generelt enn det som kommer frem fra informantene i olje- og gasselskapene. Dette kan igjen skyldes at utvalget som informantene representerer bare i mindre grad inkluderer beslutningstakere og ledere i virksomhetene.

Hvilke utfordringer representerer hybride trusler for olje- og gasselskaper?

Bildet som kommer frem i intervjuene er at norske olje- og gasselskaper primært møter tre utfordringer i et hybrid trusselscenario. Det første er at det er en generell manglende bevissthet og forståelse for hybride trusselbilder i virksomhetene. Dette gjelder tilsynelatende på tvers av virksomhetene, og inkluderer i stor grad også ledelse og beslutningstakere. Dette innebærer både en generell forståelse for hva et hybrid trusselbilde er og bevissthet knyttet til å fortå at man eventuelt er utsatt for hybrid virkemiddelbruk. Den neste utfordringen det pekes på er komplekse verdi- og leverandørkjeder. Det er vanskelig for informantene og deres respektive virksomheter å ha oversikt over disse, og fullt ut forstå hvilke sårbarheter disse representerer eller hvor sårbarhetene eventuelt er størst. At verdi- og leverandørkjeder ofte er sektoroverskridende er en ytteligere kompliserende faktor, som utfordrer virksomhetenes evne til å danne seg et helhetsbilde og -forståelse. Den siste og kanskje vanskeligste utfordringen som kommer frem i intervjuene er knyttet til informantenes oppfatning av at hybride trusler forekommer og er et problem på stats- og samfunnsnivå, ikke på virksomhets- eller sektornivå. Denne oppfatningen utfordrer også virksomhetenes evne til å se og tenke helhetlig, og forstå hvilken betydning et hybrid trusselbilde kan ha for deres egne virksomheter.

Som diskutert tidligere, kan hybride trusler betraktes fra to dimensjoner: en operasjonell dimensjon som fokuserer på håndtering av enkelthendelser og deres betydning for egen virksomhet, og en strategisk dimensjon som har en mer langsiktig og helhetlig tilnærming.

Når det gjelder utfordringer ved virksomhetenes manglende forståelse og bevissthet knyttet til et hybrid trusselbilde, pekes det på at spesielt beslutningstakere ofte forholder seg til risiko de er kjent med og vant til å vurdere. Som også en informant uttrykte er kunnskapsbasert risiko vanskelig å formidle, og det blir dermed en krevende øvelse for beslutningstakerne å vurdere denne opp mot annen og mer kvantifiserbar risiko. Så lenge virksomhetene primært fokuserer på seg selv, og hendelser eller angrep rettet mot sin egen virksomhet, er det lettere å forstå at

det er selve håndteringen av enkelthendelser som står i fokus – ikke hvorvidt disse representerer eller er del av en sammensatt virkemiddelbruk og trussel rettet mot et overordnet samfunnsnivå eller -verdi. Ut fra dette perspektivet vil de individuelle virksomhetene sansynligvis betrakte hendelser i et hybrid trusselscenario på lik linje med alle andre sikringshendelser.

Utfordringen er kanskje mer synlig når man går fra den operasjonelle dimensjonen, der håndtering av enkelthendelser står i fokus, til den mer langsiktige og strategiske dimensjonen. Hvordan hybride trusler kan forekomme og hvilken betydning de kan ha i fremtiden, gjerne i et tidsperspektiv på tiår, vil være spesielt utfordrende å forholde seg til dersom man ikke har innsikt i hva slike trusler innebærer. Det er lett for at trusselbildet kan oppfattes som urealistisk og «konspiratorisk» når det presenteres, slik en informant beskriver.

Det er heller ikke vanskelig å forstå at lange og uoversiktlige verdi- og leverandørkjeder representerer en utfordring for virksomhetene. Dette henger også sammen med utfordringen representert ved manglende forståelse og bevissthet knyttet til et hybrid trusselbilde. Forståelse for hvor eventuelle sårbarheter ligger i verdi- og leverandørkjedene forutsetter kunnskap om hvilke verdier en gitt trusselaktør ønsker å ramme, og hvilken kapasitet og hvilke virkemidler trusselaktøren råder over. Dette er såklart krevende for virksomhetene, da de hverken har oversikt over alle mulige trusselaktører og de eventuelle verdiene disse kan ønske å ramme, eller kapasitet til å overvåke og analysere indikatorer knyttet til et slikt trusselbilde. Det gjelder både for trusler som rettes mot egen sektor, men også i enda større grad når truslene går på tvers av sektorer og er rettet mot en eller flere samfunnsverdier. At verdi- og leverandørkjedene ofte er sektoroverskridende er en del av dette, og gjør som tidligere nevnt bildet ytterligere komplisert. Flere informanter nevner at petroleumssektoren kan være et attraktivt mål for eventuelle trusselaktører. At petroleumssektoren faktisk kan rammes gjennom å rette trusler mot andre sektorer og dermed påvirke for eksempel leverandørkjeden gjør det såklart vanskelig å vurdere og forstå et helhetlig trusselbilde for enkeltvirksomheter.

Her har det igjen betydning å vurdere hvilken dimensjon utfordringen betraktes fra; operasjonell eller strategisk. Fra en operasjonell dimensjon vil hybride trusler rettet mot verdi- og leverandørkjeden fremdeles kunne oppfattes som enkeltstående hendelser, som først og fremst håndteres lokalt og har betydning i nåtid. Samtidig vil svikt i ett eller flere ledd også

kunne påvirke kapasiteter på lengre sikt, og må derfor også vurderes ut fra den strategiske dimensjonen. Dette leder videre til det som kanskje er den vanskeligste utfordringen olje- og gasselskaper står overfor i et hybrid trusselscenario: skal hybride trusler kun skal betraktes fra et stats- og samfunnssikkerhetsperspektiv eller må de også vurderes fra et virksomhetsperspektiv?

Det er en gjennomgående oppfatning blant informantene at hybride trusler må betraktes og forstås fra et samfunnsperspektiv. På samme måte påpekes det at virksomhetene ikke kan pålegges ansvar for å se og håndtere samfunnssikkerhetsdimensjonen. Men det kan være like interessant for virksomhetene å snu spørsmålet andre veien; hvordan vil en hybrid trussel rettet mot samfunnet påvirke vår virksomhet? Dette spørsmålet utfordrer igjen virksomhetenes evne til å se og vurdere et helhetsbilde, og å se på tvers av sektorene.

Her kan virksomhetenes organisatoriske modenhet i forhold til å forstå, vurdere og benytte et helhetlig trusselbilde som del av et beslutningsgrunnlag ha stor betydning. Slik informantene fra ett selskap beskriver det, har trusselvurderinger fått større fokus i deres organisasjon på grunn av nye store utbyggingsprosjekter, og at organisasjonen på grunn av dette er utvidet og har fått større kapasitet til å vurdere et helhetlig trusselbilde. Dette står i kontrast til hvordan informanter fra andre virksomheter beskriver sine organisasjoner, der manglende kapasitet blir beskrevet som et resultat av at hele organisasjonen har mindre fokus og forståelse for betydningen av mulige fremtidige trusselscenarier – eller med andre ord at organisasjonen viser en lavere grad av modenhet i forhold til et hybrid trusselscenario.

I et hybrid trusselscenario er det altså tydelig at manglende kapasitet er en utfordring for olje- og gasselskapene, både i forhold til å analysere og vurdere trusselbildet på et operasjonelt nivå og på et strategisk eller langsiktig nivå. Det er også like tydelig at det er sammenheng mellom kapasitet og organisasjonens modenhet – eller hvilken forståelse og bevissthet organisasjonen som helhet har i forhold til et hybrid trusselbilde. Her er selskapenes størrelse også en faktor. Som vist i kapittel 4 oppfatter informantene at mindre selskaper ser et langt mer begrenset ansvarsområde enn de større, og vil i større grad peke på myndighetenes rolle og ansvar.

Varsling av andre virksomheter, samarbeidspartnere og myndigheter er en viktig respons på en trussel eller et angrep, men samtidig kan det være vanskelig å avgjøre hvem som skal varsles. Effektiv varsling krever altså at virksomhetene har en bred forståelse, for eksempel for hvem trusselaktøren er og hvilken målsetning trusselaktøren kan ha, men også forståelse

for at man faktisk er utsatt for en hybrid trussel. En trusselaktør kan nemlig i mange tilfeller ønske å skjule virkemiddelbruken, og hvem som egentlig står bak. De fleste informantene peker på at myndighetene har ansvaret for hybride trusler, og at hendelser og trusler uansett vil havne hos politiet. Men hvem har ansvaret for de mer lavintensive truslene, for eksempel påvirkning av nøkkelpersoner eller kartlegging av selskapsstrukturer? Dette er noe som i utgangspunktet kan være lovlig og legitimt, og ikke noe som politiet vil kunne ta tak i.

Hva som til syvende og sist oppfattes som en trussel, enten det materialiseres i nåtid eller fremtid, er avhengig av kunnskap og forståelse for trusselbildet. Det kan derfor argumenteres for at evnen til å kunne oppfatte og forstå en trussel i et hybrid trusselscenario har betydning for virksomhetene i både den operasjonelle og den strategiske dimensjonen.

Er Resilience Engineering en hensiktsmessig tilnærming?

De fire grunnelementene som i følge Resilience Engineering-perspektivet er nødvendig for at virksomheter skal kunne fungere på en resilient måte er beskrevet nærmere i kapittel 2. Disse danner grunnlag for å drøfte om Resilience Engineering-perspektivet er en hensiktsmessig tilnærming til de utfordringene som norske olje- og gasselskaper oppfatter at hybride trusler representerer.

Evnen til å kunne overvåke

I forhold til Resilience Engineering-perspektivet har det grunnleggende betydning for virksomhetenes evne til å kunne fungere på en resilient måte at de er i stand til å overvåke den nåværende funksjonstilstanden og -evnen, og sammenligne denne med den ønskede idealtilstanden for å identifisere eventuelle avvik. Det er evnen til å fange opp og se avviket mellom den faktiske tilstanden og idealtilstanden som danner grunnlag for både å kunne være forberedt og å kunne respondere på eventuelle hendelser. Her er det tydelig at både manglende evne til å forstå hva et hybrid trusselbilde innebærer og manglende evne til å gjenkjenne og forstå at en er utsatt for hybride trusler har stor betydning.

Det er påpekt at det er utfordrende å vite hva man skal fokusere på i forhold til hybride trusler; «de kan være overalt og inkludere alt». Som beskrevet i kapittel 2, peker Hollnagel (2011a) på at evnen til å fokusere på de faktorene som har kritisk betydning krever at en er bevisst på hva en skal overvåke. For å kunne fange opp at endringer eller avvik i virksomhetens tilstand er i ferd med å oppstå, kan effektiv overvåking være basert på indikatorer. Men som en informant uttrykte det, er indikatorer situasjonsbetinget og må være

basert på et spesifikt informasjonsbehov. Så da blir spørsmålet: hvilket informasjonsbehov har egentlig virksomhetene i et hybrid trusselscenario og hvilke indikatorer kan dekke dette?

I forhold til å vurdere og forstå et hybrid trusselbilde antyder informantene at det foregår veldig begrenset overvåking av indikatorer, at det skjer på en tilfeldig og lite systematisk måte, og ikke er forberedt i særlig grad. De er avhengig av å motta data og analyser fra myndighetene for å kunne forstå helhetsbildet, og det faktum at virksomhetene bare i begrenset grad ser utenfor sin egen virksomhet og sektor betyr at de derfor ikke nødvendigvis vil fange opp betydningen av eventuelle sektoroverskridende trusler. Myndighetenes åpne trusselvurderinger er generelle og adresserer ikke enkeltsektorer eller konkrete deler av samfunnet i særlig grad. Når disse danner grunnlag for virksomhetenes egne trusselvurderinger innebærer det en fare for at viktige detaljer overses, og kan dermed hemme virksomhetenes evne til å oppfatte små nyanser og endringer i egen funksjonstilstand eller i trender av betydning i samfunnet. Dersom virksomhetene skal kunne fokusere sin overvåking på «de rette» indikatorene, må myndighetene bidra med spesifik informasjon og peke på konkrete indikatorer eller trender. Som referert til i kapittel 2 viser Hollnagel (2018, s. 34) til at det også er viktig å forklare hvorfor disse spesifike indikatorene har betydning, fordi indikatorer som ikke kan forstås eller tolkes har liten verdi samtidig som de er ressurskrevende å overvåke. Myndighetene må altså peke på spesifike indikatorer som både er grundige og effektive, eller med andre ord meningsfulle.

En informant viser til hvordan dialog og samarbeid med innretningene og å bygge relasjoner ut over sin nærmeste organisasjon har betydning. Dette er et eksempel på hvordan hele organisasjonen kan involveres i å overvåke virksomhetens tilstand, men det forutsetter likevel kunnskap om hva normaltilstanden er og hva man skal se etter. Samtidig kan man argumentere for at virksomhetenes egen funksjonsevne allerede overvåkes – i hvert fall på et teknisk operasjonelt nivå. Så utfordringen ligger igjen mer på å kunne formidle et hybrid trusselbilde på tvers av hele organisasjonen og danne en felles forståelse for hva dette innebærer, slik at den overvåkingen som foregår også inkluderer og oppfatter hybride trusler. Dette peker i retning av evnen organisasjonen har til å kunne lære, som vil bli drøftet videre nedenfor.

Men overvåking av indikatorer er ikke bare begrenset til virksomhetenes egen funksjonsevne og -tilstand. Det omkringliggende miljøet som virksomhetene fungerer i må også overvåkes.

Her er det allerede nevnt virksomhetenes utfordringer med å oppfatte og forstå betydningen av sektoroverskridende trusler, og selvfølgelig spiller komplekse verdi- og leverandørkjeder også en rolle her. Men fra et strategisk perspektiv er det tydelig at spesielt politiske prosesser og eventuelle endringer i sektorens rammevilkår har stor betydning. Samtidig har ikke virksomhetene samme muligheter til å påvirke disse prosessene, og inntar derfor en mer passiv eller reaktiv rolle.

Dette peker igjen på hvordan virksomhetene oppfatter sin rolle som reaktiv i forhold til samfunnssikkerhetsdimensjonen. Samtidig vil det også være viktig at virksomhetene oppfatter hvordan endringer i samfunnssikkerhet kan påvirke deres egen funksjonsevne og fremtidige muligheter. Dette peker på deres evne og kapasitet til å drive virksomhetsstyring på et strategisk nivå, eller med andre ord i hvilken grad virksomhetene er i stand til å styre sine aktiviteter på en systematisk måte for å sikre at et sikringsnivå som samsvarer med de mål og krav virksomheten stiller til seg selv kan opprettholdes. En reaktiv holdning til den strategiske dimensjonen kan beskrives som hendelsesbasert, altså at endringer og tiltak først iverksettes når uønskede hendelser og trusler er identifisert. Dette står i kontrast til en risikobasert styringsmodell, som har en mer proaktiv tilnærming og gjør det mulig å iverksette tiltak før en hendelse eller trussel får betydning for virksomhetens funksjonsevne.

Evnen til å kunne respondere

Når virksomhetene vurderer trusselbildet, kommer det tydelig frem i intervjuene at et overordnet eller politisk nivå ikke inkluderes i særlig grad. Virksomhetenes trusselbilde danner grunnlag for deres risikovurderinger og eventuelt hvilke tiltak eller responser som forberedes i forhold til trusler eller hendelser som er identifisert. Det er vanskelig å både fange opp og å respondere på vage signaler, både signaler som eventuelt kommer fra andre sektorer eller fra et mer overordnet samfunnsnivå. Respons i forhold til hybride trusler kan derfor lett bli reaktiv, og som tidligere diskutert, fokusert mot håndtering av enkelthendelser fremfor å se større eller bakenforliggende sammenhenger. Som en informant uttrykker det, vil det ved en hendelse ofte være fokus på å sørge for å få systemer i gang igjen, med så lite nedetid som mulig, fremfor å være proaktiv og hindre at hendelsen i det hele tatt inntreffer. Dette strider tilsynelatende mot barriæreprinsippet, men innebærer samtidig en erkjennelse av at det ikke er mulig å være forberedt på enhver tenkelig eller utenkelig hendelse til enhver tid.

Den første responsen er ofte å varsle andre deler av virksomheten og sektoren, samt relevante myndigheter. Det kan argumenteres for at første respons dermed er knyttet til å heve bevissthet og årvåkenhet i organisasjonen, eller med andre ord styrke evnen til å kunne overvåke, som diskutert over. En slik hendelsesbasert respons er grunnleggende reaktiv, og med utgangspunkt i Resilience Engineering-perspektivet kan det da sies at virksomhetenes første respons på en hendelse eller trussel er å ha en ambisjon om å øke sin evne til å fungere på en resilient måte, selv om det da allerede kan være for sent.

Som en informant uttrykker det er respons på hybride trusler lite forberedt, og i stor grad basert på at virksomheten må improvisere. Det kan argumenteres for at dette langt på vei kan skyldes en uoversiktlig organisasjonsstruktur, der det er uklart hvem som egentlig har ansvaret for å initiere eller iverksette en respons. Og igjen kan mangel på kunnskap og forståelse føre til at man ikke en gang forstår at man er utsatt for en hendelse, for eksempel en påvirkningsoperasjon, og at det dermed ikke iverksettes noen tiltak i det hele tatt.

Evnen til å kunne lære

Som diskutert over, peker informantene på manglende kunnskap og bevissthet i organisasjonene som en vesentlig sårbarhet i forhold til hybride trusler. Det er naturligvis ønskelig å rette på dette. Enkelte virksomheter har tatt dette innover seg og for eksempel fokusert på å sette sammen mer tverrfaglig kompetanse i organisasjonen. Dette kan bidra til å gjøre det lettere å se ut over egen sektor når trusselbildet vurderes, og dermed kunne hente erfaring og læring fra et bredere samfunnsspekter.

En annen informant beskriver hvordan virksomheten har innført obligatoriske kurs for alle ansatte, og hvordan trusselbildet formidles og deles med hele organisasjonen. I denne virksomheten stiller også toppledelsen tydelige krav til at bevisstheten skal økes i organisasjonen, noe som viser at problemstillingen har forankring i hele organisasjonen – også i toppledelsen. Dette er i tydelig kontrast til hvordan andre informanter beskriver fokus i sine virksomheter, og kan forklares ut fra at virksomhetene har både ulik grad av modenhet og ulik kultur for å vurdere og ta inn over seg nye og tidligere ukjente trusselbilder og -faktorer.

Det er helt grunnleggende for virksomhetenes evne til å både oppfatte signaler (overvåke) og å respondere på disse at de har erfart og lært hva som har betydning og hvilken effekt ulike responser kan forventes å gi. Dette kan for eksempel være gjennom evaluering av hvordan tidligere hendelser er håndtert, både innenfor egen virksomhet eller fra andre virksomheter i

egen eller andre sektorer. Som det poengteres i kapittel 2, er evnen til å trekke den rette lærdomen fra de riktige erfaringene essensielt. Informantene gir ikke inntrykk av at dette gjøres i særlig grad, selv om en informant beskriver at de også bruker andre virksomheter og andre sektorer som sparringpartnere når trusselvurderinger utarbeides. Som det også blir pekt på i ett intervju må det ofte en konkret hendelse til for at en trussel skal få fokus i virksomheten, selv om hendelsen riktignok ikke nødvendigvis trenger å ramme denne virksomheten.

Men selv om det innhentes kunnskap fra et bredt spekter av sektorer og virksomheter, er det likevel vanskelig å kunne verifisere at læring faktisk har funnet sted. Som Hollnagel (2011b) siteres på i kapittel 2 innebærer læring ikke bare passiv tilegnelse av kunnskap, men også en endring i adferd og handlingsmønster. Som det kommer frem av intervjuene, øver ikke virksomhetene i særlig grad på håndtering av sammensatte og komplekse hendelser, og det er derfor vanskelig å vurdere hvorvidt de faktisk er i stand til å kunne håndtere hendelser i et hybrid trusselscenario og hva som eventuelt må forbedres. Riktignok påpeker en informant at de kanskje likevel har øvd på dette uten at det er gjort bevisst, da de i forbindelse med Covid-19 øvde på komplekse scenarier som foregikk langs flere akser samtidig. Dette indikerer at læring knyttet til sammensatte og komplekse trusler, slik et hybrid trusselscenario er, også kan være generaliserbar og anvendelig over et bredt spekter av andre situasjoner.

Evnen til å kunne forutse

Som det er påpekt flere ganger over, fokuserer virksomhetene først og fremst på håndtering av enkelthendelser fremfor å vurdere hybride trusler over et bredt sektor- eller samfunnsperspektiv. Her viser de i stedet til at hybride trusler forekommer og må håndteres på samfunnsnivå, og derfor primært er myndighetenes ansvar. Dette peker på et problem som ligger på strategisk nivå, og spørsmålet blir da om virksomhetene og sektoren inkluderer samfunnssikkerhetsdimensjonen når de utformer sine strategier. Som en informant uttrykker er det opp til de enkelte analytikerne å vurdere hva som skal inngå i trusselvurderingene. Da blir trusselvurderingenes relevans i forhold til et langsiktig strategisk bilde avhengig av at analytikeren også er godt kjent med virksomhetens strategi og langsiktige tenkning, og ikke minst hvilken rolle analytikeren selv vurderer at virksomheten og sektoren har i forhold til samfunnssikkerheten.

Riktignok har hybride trusselscenarier større fokus nå enn før, men likevel gir informantene intrykk av at langsiktige trusselvurderinger har liten plass som beslutningsgrunnlag for store investeringer. En informant forklarer hvordan langsiktige investeringsbeslutninger hovedsaklig baseres på tekniske og økonomiske vurderinger, og at trusselscenarier ikke inkluderes i særlig grad. Da må det i så fall komme som følge av krav eller tydelige signaler fra myndighetene. Her er det igjen en tydelig forskell mellom virksomhetene, da andre informanter peker på at i deres virksomhet er det nettopp store nye utbyggingsprosjekter som har ført til økt behov for å styrke kapasiteten til å utarbeide trusselvurderinger.

Generelt etterlater informantene et inntrykk av at et hybrid trusselbilde i liten grad inkluderes på en systematisk måte som grunnlag for strategiske vurderinger av i sektoren. Forutseenhet slik det defineres i Resilience Engineering-perspektivet har blant annet som hensikt å legge til rette for å forstå potensialet i mulige fremtidige hendelser. Dette kan for eksempel være hvordan rammevilkår kan bli påvirket og endret, og økt bevissthet i forhold til dette vil i større grad gjøre virksomhetene i stand til å kunne tilpasse seg nye utfordringer.

Utfordringer ved hybride trusler sett fra Resilience Engineering-perspektivet

Slik det beskrives i kapittel 2, er Resilience Engineering-perspektivet basert på en endring eller utvikling i sikkerhetsoppfatning fra Safety-I til Safety-II. Et syn på sikkerhet som kun er basert på forståelse av tidligere uønskede hendelser, og der målet er å forhindre gjentagelse av disse, peker på en tilnærming i tråd med Safety-I. Det ligger et tydelig årsak/virkning-forhold til grunn for dette synet, det vil si at total sikkerhet kan oppnås ved å identifisere og håndtere alle mulige årsaker til alle kjente uønskede hendelser. Tilsvarende forutsetter dette synet at erfaring og forståelse av tidligere intrufne uønskede hendelser danner grunnlag for hvilke rammer eller grensebetingelser som det er tilstrekkelig å holde seg innenfor for å kunne operere på en sikker måte.

Et hybrid trusselbilde innebærer at en trusselaktør vil kunne opptre fordekt, og bruke nye, skjulte eller lavintensive virkemidler spredt over flere sektorer for å oppnå sine mål. En virksomhet som kun vil sikre seg i forhold til kjente trusler og tidligere anvendte virkemidler, i tråd med oppfatningen representert ved Safety-I, vil derfor ikke nødvendigvis fange opp eller evne å håndtere hybride trusler.

Slik Hollnagel og Woods (2006, s. 357) argumenterer for, representerer Resilience Engineering en tilnærming som gjør virksomhetene mindre avhengige av en reaktiv,

hendelsesbasert og analytisk sikkerhetstilnærming. I stedet representerer Resilience Engineering en mer proaktiv tilnærming som gjør virksomhetene i større grad i stand til å være fleksibel og tilpasningsdyktig i møte med nye og ukjente trusler. Kontrasten mellom en reaktiv og en proaktiv tilnærming beskrives som skillet mellom Safety-I og Safety-II, eller med andre ord at fokus endres fra å *hindre* til å *håndtere* uønskede hendelser. En tilnærming i tråd med Safety-II forutsetter derfor også at organisasjonen ikke bare fokuserer på enkeltfaktorer, men må i større grad også se og forstå helhetsbildet. Dette er mer i tråd med hvordan hybride trusler beskrives, altså som sektoroverskridende og der enkelthendelser kan være vanskelig å forstå i en større kontekst – hvis de oppdages i det hele tatt.

Som det er pekt på tidligere, er hovedutfordringene ved hybride trusler knyttet til manglende kunnskap og bevissthet i organisasjonene, komplekse verdi- og leverandørkjeder, og ikke minst hvorvidt hybride trusler skal betraktes fra et virksomhets- eller et samfunnsperspektiv. En tilnærming til hybride trusler basert på Safety-I vil være spesielt vanskelig gitt disse utfordringene, da Safety-I nettopp innebærer og krever kunnskap om tidligere hendelser, samt oversikt over hva truslene innebærer. Det kan dermed argumenteres for at en tilnærming basert på Safety-II er mer passende, i hvert fall så lenge virksomhetene primært fokuserer på seg selv og ikke samfunnssikkerhetsdimensjonen.

På den annen side dersom hybride trusler kun betraktes som en trussel på samfunnsnivå, ikke mot enkeltvirksomheter eller objekter, blir det vanskelig å betrakte disse med en Safety-II tilnærming. Å kunne legge til rette for funksjonsevnen til alle de faktorene som gjør hele samfunnet i stand til å være trygt er en formidabel oppgave. I et hybrid trusselscenario kan samfunnet rammes på tvers av sektorer, og å håndtere et slikt scenario vil derfor kreve en overordnet innsats og koordinering som ikke eksisterer i dag.

Som sitert i kapittel 1, peker tidligere forsvarssjef Admiral Haakon Bruun-Hanssen også på behovet for å «forbedre evnen til tverrsektoriell situasjonsforståelse, informasjonsflyt og samarbeidsmekanismer» som en av hovedutfordringene i fremtidige hybride trusselscenarier (Forsvaret, 2019, s.83).

I forhold til de fire elementene som uttrykkes i Resilience Engineering-perspektivet som grunnleggende for organisasjoners evne til å fungere på en resilient måte, er det tydelig at overvåking av virksomhetenes tilstand og forståelse av hva som eventuelt er avvikende i forhold til en idealtilstand er utfordrende i et hybrid trusselscenario. Som beskrevet over kan

dette langt på vei forklares ut fra manglende forståelse og kunnskap om hva hybride trusler innebærer, og hvordan en skal kjenne igjen en slik trussel. Og så lenge det ikke foregår en systematisk overvåking av konkrete indikatorer, vil det selvfølgelig være vanskelig å oppfatte signaler eller avvik.

Det er generelt utfordrende for virksomhetene å formulere indikatorer knyttet til hybride trusselbilder, og i den grad de faktisk eksisterer er de både bakoverskuende – det vil si basert på tidligere kjente og rapporterte hendelser, eller fremoverskuende og basert på for eksempel trender presentert i sikkerhetsmyndighetenes åpne trusselvurderinger. Det er krevende å evaluere relevansen til indikatorene så lenge man ikke med sikkerhet vet at man utsettes for hybride trusler. Hvorvidt slike indikatorer er lett å forholde seg til, altså at eventuelle avvik faktisk kan føre til en respons, er også uklart. På den ene siden kommer det frem at det kan være uoversiktlig hvem som har ansvaret for å overvåke indikatorer i virksomhetene, og samtidig er det uklart om indikatorene eksisterer på virksomhets-, sektor- eller samfunnsnivå.

Inntrykket informantene gir er at virksomhetene responderer raskt når de forstår at de utsettes for et konkret angrep, kanskje gjelder dette spesielt IT-domenet. Men i forhold til de mer skjulte, vage eller lavintensive truslene, som kanskje kan tolkes som et varsel om bruk av maktmidler i fjern fremtid, er det ikke klart om de vil respondere i det hele tatt. Her spiller skillet mellom det operasjonelle og det strategiske domenet en rolle, da lavintensive langsiktige trusler fort blir ansett som myndighetenes ansvar. I det hele tatt er det uklart hvor terskelen for å respondere skal legges i et hybrid trusselscenario. Legges den for lavt må virksomhetene respondere ofte og kanskje bruke ressurser unødvendig. For høy terskel innebærer at en respons kan komme for sent – eller ikke i det hele tatt.

I forhold til hybride trusler skjer læring relativt usystematisk i informantenes virksomheter. I den grad hybride trusler har fokus i opplæring og formidling av trusselbilde i organisasjonene, er det som beskrevet tidligere krevende å kunne verifisere at læring faktisk har funnet sted så lenge det ikke øves på å håndtere sammensatte og komplekse hendelser.

Forståelsen av den langsiktige og strategiske dimensjonen i et hybrid trusselscenario peker på virksomhetenes evne til å være forutseende. Her er det et opplagt skille mellom virksomhetene, der en virksomhet skiller seg ut ved at den har investert i økte ressurser og kapasiteter for blant annet å utarbeide trusselvurderinger. Dette åpner dermed også for økt evne til forutseenhet og for å vurdere et større og mer helhetlig trusselbilde. Samtidig er det

fremdeles i stor grad opp til analytikerene å stå for forutseenheten og fremtidsvurderingene, som også vil være avhengig av og påvirket av deres verdensbilde eller -anskuelse.

Kan rolleforståelse påvirke evnen til å fungere på en resilient måte?

Med utgangspunkt i Resilience Engineering-perspektivet er det vist over hvordan manglende bevissthet og kunnskap i virksomhetene påvirker deres evne til å fungere på en resilient måte i et hybrid trusselscenario. Dette kommer primært som et resultat av at virksomhetene ikke nødvendigvis er i stand til å kjenne igjen en hybrid trussel dersom de utsettes for en, og er videre relatert til overvåking av egen tilstand og funksjonsevne, identifisering og forståelse av avvik, evne til å iverksette en respons og å respondere på riktig måte og til riktig tid, samt ikke minst å kunne være forutseende og vurdere ulike scenarier som kan oppstå i fremtiden.

I kapittel 2 beskrives hvordan formålsrasjonalitet og konsekvenslogikk er en forutsetning for virksomhetens handlinger både i et instrumentelt perspektiv og som grunnlag for Resilience Engineering, eller med andre ord at måten virksomheten velger mellom sine virkemidler og handlingsalternativer følger en vurdering av hvilket alternativ som er best egnet i forhold til å opprettholde normal funksjonalitet og drift.

Det instrumentelle perspektivet innebærer at formelle organisasjonsstrukturer legger til rette for å bidra til effektiv håndtering av hendelser. Det kan argumenteres for at dette peker på systemutforming eller -design, der organisasjonsstrukturen er en del av systemet, tilsvarende hvordan Leveson (2020) introduserer systemtenking i en Safety-III tilnærming. I et instrumentelt perspektiv kan altså selve organisasjonens utforming betraktes som et instrument for dens evne til å kunne fungere på en resilient måte.

En tilnærming til sikkerhet basert på enten Safety-II eller Safety-III baseres altså langt på vei på at roller i organisasjonene kan beskrives ut fra et instrumentelt perspektiv. Slik utfordringene i et hybrid trusselscenario er beskrevet av informantene, er det riktignok tydelig at virksomhetene har ulik og begrenset evne til å innhente all relevant informasjon om de forskjellige handlingsalternativene og deres konsekvenser. Det er forklart i kapittel 2 at slike begrensninger i evnen til å kontrollere alle faktorer, og hvordan informasjonstilgang påvirker virksomhetenes beslutningsgrunnlag, i realiteten medfører at et instrumentelt perspektiv må peke på *begrenset* rasjonalitet. Virksomhenenes evne til å fungere på en resilient måte i et hybrid trusselscenario utfordres altså på bakgrunn av muligheten de har til å opptre formålsrasjonelt.

Som beskrevet tidligere påvirker også organisatoriske forhold hvordan virksomhetenes evne til å fungere på en resilient måte varierer i et hybrid trusselscenario. Virksomheter som har et tydelig og uttalt fokus på å utarbeide trusselvurderinger og styre sine aktiviteter i forhold til disse, skiller seg fra virksomheter med uklare og fragmenterte ansvarsforhold og mindre evne og kapasitet til å vurdere et helhetlig trusselbilde. Spesielt der informantene peker på at det er liten vilje eller evne til å endre organisasjonsstrukturene kommer dette klart til syne. Som noen informanter beskriver det, oppfatter de at deres virksomhet har en statisk organisasjonskultur der det er vanskelig å endre på noe, og resultatet blir at de utfører sine aktiviteter på samme måte som de alltid har gjort. Virksomheter som handler i tråd med hvordan interne rutiner er etablert over tid, og viser en motvillighet eller avventende holdning til å endre seg i tråd med endringer i omgivelsene, kan best forstås ut fra et kulturelt institusjonelt perspektiv.

Et kulturelt institusjonelt perspektiv, som legger vekt på hvordan uformelle regler, normer og verdier eksisterer og er etablert i en organisasjon, kan blant annet komme til uttrykk gjennom hvilke antagelser og virkelighetsoppfatninger som ligger til grunn for organisasjonens handlinger (Andreassen og Bjørkelo, 2020). En tydelig oppfatning av at hybride trusler kun er myndighetenes ansvar, og ikke noe som angår virksomhetene, er eksempel på en slik virkelighetsoppfatning - selv om beskyttelse av petroleumsvirksomheten er regnet som en grunnleggende nasjonal funksjon og underlagt sikkerhetsloven. Virksomhetene peker altså bevisst eller ubevisst på myndighetene som ansvarlige for beskyttelse av petroleumsvirksomheten. Denne virkelighetsoppfatningen påvirker igjen virksomhetenes evne til å opptre resilient i et hybrid trusselscenario.

Som det er beskrevet tidligere, varierer virksomhetenes modenhet i forhold til å oppfatte, forstå og tilpasse seg nye trusselbilder, men også i forhold til hvilken vekt beslutningstakerne legger på trusselvurderinger. Spesielt kommer dette til uttrykk ved langsiktige beslutninger og investeringer dersom disse hovedsakelig baseres på tekniske og økonomiske vurderinger og ikke inkluderer mulige fremtidige trusselbilder. Som en informant uttrykte det, er det en fare for at ledelse og beslutningstakere kan oppfatte fremtidige hybride trusselscenarier som urealistiske, vanskelige å forholde seg til eller rett og slett konspiratoriske, og dermed velge å se bort fra disse.

Som beskrevet i kapittel 2, vil virksomheter der beslutninger påvirkes av etablerte uformelle regler, normer og verdier altså ikke kunne endre og tilpasse seg nye trusselbilder og funksjonsvilkår like lett som det for eksempel forutsettes i et instrumentelt perspektiv. Det vil si at virksomheter som i stor grad responderer på hendelser og trusler ved å følge den erfaringen de har med tidligere handlingsmønstre og virkemiddelbruk best kan forstås ut fra et kulturelt institusjonelt perspektiv. Dette ligger også tett opp til hvordan en tilnærming til sikkerhet beskrives som Safety-I.

Hvordan virksomhetenes grad av modenhet i møte med et hybrid trusselscenario varierer, eller med andre ord hvordan deres adferd og beslutningsprosess varierer i forhold til å oppfatte, forstå og tilpasse seg nye trusselbilder, har altså betydning for hvorvidt deres tilnærming og rolleforståelse best kan beskrives fra et instrumentelt eller et kulturelt institusjonelt perspektiv. Dette danner også grunnlag for å vurdere virksomhetenes evne til å fungere på en resilient måte.

Et symbolsk institusjonelt perspektiv tar derimot utgangspunkt i hvordan omverdenens forventninger og oppfatninger påvirker virksomhetenes utforming og funksjon. Dette skiller seg altså fra det kulturelle institusjonelle perspektivet, ved at handlinger tilpasser seg og følger normer og forventninger som er etablert utenfor virksomheten, og altså ikke de som er etablert og eksisterer internt.

Men hvordan oppfatter så informantene sine respektive virksomheters rolle i et hybrid trusselscenario? Som beskrevet tidligere kan det skilles mellom en operasjonell og en strategisk dimensjon i hvordan hybride trusler og tilhørende virkemiddelbruk klassifiseres (Figur 3). Bildet som kommer frem er at virksomhetene fokuserer på og tar ansvar for håndtering av enkelthendelser som er rettet mot dem selv, mens de peker på myndighetenes ansvar og rolle når det kommer til trusler som rammer bredere, for eksempel på tvers av sektoren eller hele samfunnet. Dette indikerer at virksomhetene ikke oppfatter at det eksisterer forventninger i samfunnet til at petroleumssektoren har en spesifik rolle eller ansvar for samfunnssikkerhet og sektoroverskridende trusler i et hybrid trusselscenario.

Som beskrevet i kapittel 2 innebærer et symbolsk institusjonelt perspektiv på virksomhetenes rolle at det over tid vil utvikle seg en organisatorisk likhet mellom virksomhetene. De empiriske dataene viser at det er til dels stor forskjell mellom hvordan ulike virksomheter tilnærmer seg hybride trusler i sine trusselvurderinger og som beslutningsgrunnlag. Det er

med andre ord lite som tyder på en utvikling i retning av organisatorisk likhet i forhold til hvordan virksomhetenes rolle i et hybrid trusselscenario oppfattes. Et symbolsk institusjonelt perspektiv beskriver altså i svært liten grad rolleforståelsen som kommer frem i intervjuene.

Riktignok kommenterer enkelte informanter at det kan være forventninger til virksomhetene, eller at de kan bli tillagt en rolle i et totalforsvarsperspektiv. Samtidig vil dette neppe være aktuelt med mindre det oppstår en krisesituasjon. I et hybrid trusselscenario som innebærer lavintensiv virkemiddelbruk, og der trusselaktørens målsetning er skjult og uklar, er det vanskelig å peke på en klar rollefordeling mellom virksomhetene i petroleumssektoren og myndighetene.

Informantene er tydelige på at virksomhetene deres ikke tar på seg ansvar eller roller som ikke er klart definert. Det gjelder også i forhold til hybride trusler. Her viser de til at det eksisterende lov- og regelverket er dekkende i forhold til hvordan de oppfatter sin rolle. Et funksjonelt reguleringsregime spiller også inn her, da dette innebærer at det er opp til virksomhetene selv å analysere og vurdere hvilket trusselbilde de må forholde seg til. Så lenge lovverket ikke peker konkret på at virksomhetene har et ansvar for å bidra til samfunnssikkerhet, oppfatter informantene altså at sin rolle og ansvarsområde er begrenset til egen virksomhet.

En rolleforståelse der det primære fokuset er på trusler rettet mot ens egen virksomhet, og som er påvirket av organisasjonens manglende evne og kapasitet til å danne seg et helhetlig trusselbilde på tvers av sektor og samfunn, kan altså ikke entydelig beskrives ut fra et instrumentelt perspektiv fordi manglende helhetlig forståelse gjør det vanskelig å opptre formålsrasjonelt. Riktignok vil økende grad av modenhet i organisasjonene danne grunnlag for en utvikling i retning av en mer instrumentell tilnærming og, som vist over, et bedre grunnlag for å fungere på en resilient måte i et hybrid trusselscenario. Informantene etterlater et inntrykk av at den nåværende tilnærmingen virksomhetene har bare unntaksvis kan forstås fra et instrumentelt perspektiv, og i mange tilfeller helt klart best kan uttrykkes ved hjelp av et kulturelt institusjonelt perspektiv. Det er altså klare utfordringer i forhold til å fungere på en resilient måte i et hybrid trusselscenario slik premissene for Resilience Engineering-perspektivet er uttrykt.

6. Konklusjoner

Funn og implikasjoner

Formålet med denne studien har vært å få dypere innsikt i hvordan olje- og gasselskaper på norsk sokkel forstår hybride trusler, og hvordan de oppfatter sin rolle i en større sammenheng i et hybrid trusselscenario. Petroleumssektoren har stor betydning for det norske samfunnet, og det er derfor interessant om sektoren oppfatter at den også har en rolle i forhold til samfunnsikkerhet. Ved analyse av empiriske data samlet inn gjennom intervjuer med relevante informanter tilknyttet petroleumssektoren kommer det frem interessante funn:

- I forhold til hybride trusler anser virksomhetene i petroleumssektoren sin rolle som begrenset. De har fokus på å håndtere enkelthendelser og trusler rettet mot dem selv, mens de peker på myndighetene som ansvarlig for håndtering av mer komplekse, sektoroverskridende trusler.
- Det er mulig å skille virksomhetenes vurdering av hybride trusler gjennom å kategorisere trusselaktørers virkemiddelbruk ut fra intensitet og hvor langsiktig virkemiddelbruken anses å være. Dette indikerer et skille mellom en operasjonell og en strategisk dimensjon, der virksomhetene primært oppfatter sitt ansvar og sin rolle knyttet til den operasjonelle.
- En trusselaktørs eventuelle bruk av virkemidler med en langsiktig horisont, og som typisk kommer til uttrykk på sektor- eller samfunnsnivå, inkluderes bare unntaksvis i virksomhetenes trusselvurderinger og beslutningsgrunnlag.
- Manglende kunnskap, forståelse og trusselbevissthet i forhold til hybride trusler er en vesentlig sårbarhet. Som en konsekvens er det sammenheng mellom virksomhetenes modenhet i forhold til hvilken forståelse og bevissthet organisasjonen har med tanke på et hybrid trusselbilde, og hvilken kapasitet virksomhetene har investert i for å kunne danne seg et selvstendig trusselbilde som beslutningsgrunnlag for operasjonelle og strategiske beslutninger.

Disse funnene er interessante når en skal vurdere hvilken rolle virksomhetene anser at de har i en større sammenheng. Det har blitt pekt på at hybride trusler først og fremst handler om og må betraktes fra en samfunnssikkerhetsdimensjon. I forhold til denne dimensjonen inntar virksomhetene en reaktiv rolle, og fokuserer først og fremst på seg selv og sin egen evne til å opprettholde eller eventuelt gjenopprette normal drift. Å kunne opprettholde normal drift også i et hybrid trusselscenario kan riktignok betraktes som et bidrag til samfunnssikkerheten, og

med utgangspunkt i Resilience Engineering-perspektivet (Hollnagel et al., 2006) er det vurdert hvordan petroleumssektorens nåværende tilstand er i forhold til å kunne fungere på en resilient måte, og også hva som skal til for å kunne utvikle denne evnen videre.

Virksomhetene bygger mye av sin kunnskap om hybride trusselbilder på informasjon fra myndighetene. For å kunne forstå og overvåke de faktorene eller indikatorene som er meningsfulle i forhold til hybride trusler er det derfor viktig at myndighetenes informasjon ikke blir for generell, men også peker på konkrete indikatorer som faktisk kan ha betydning og som er mulig for virksomhetene å overvåke. Et resultat av manglende evne til å kunne fokusere på meningsfulle indikatorer i forhold til hybride trusler er at virksomhetenes respons blir reaktiv og ytterligere fokusert på håndtering av enkelthendelser.

Virksomhetene øver i svært liten grad på å håndtere komplekse og sammensatte trusselscenarier, og de har derfor vanskelig for å vurdere hvorvidt de faktisk er i stand til å kunne håndtere hendelser i et hybrid trusselscenario, og hva som eventuelt må forbedres. Dette peker på læringsfaktoren, og hvordan det er vanskelig å kunne verifisere at læring faktisk finner sted.

Langsiktige trusselvurderinger har i dag bare begrenset plass som beslutningsgrunnlag. Trusselvurderingenes relevans i forhold til et langsiktig eller strategisk bilde er på sin side avhengig av at analytikerne også er godt kjent med virksomhetens strategi og langsiktige tenkning. En økt bevissthet i forhold til forutseenhet vil derfor i større grad kunne gjøre virksomhetene i stand til å tilpasse seg nye utfordringer og trusselbilder, og dermed opptre på en resilient måte.

Med utgangspunkt i faktorene over, er det interessant å vurdere hvorvidt virksomhetenes rolleforståelse bidrar til å legge til rette for eller begrense deres evne til å fungere på en resilient måte. I forhold til Resilience Engineering-perspektivet vil en rolleforståelse som best lar seg beskrive ut fra et instrumentelt perspektiv danne et godt grunnlag for å fungere på en resilient måte. Dette innebærer at virksomhetens adferd og handlinger følger rasjonelle og forutsigbare mønstre, og at organisasjonens oppbygging og struktur bidrar som et instrument til å håndtere hendelser og trusler. I motsetning til dette vil virksomheter som har en mer statisk og rigid organisasjonskultur, som motsetter seg endringer eller viser uvilje til å tilpasse seg nye utfordringer eller trusselbilder best kunne beskrives og forstås ut fra et kulturelt

institusjonelt perspektiv, og ha større utfordringer i forhold til å kunne fungere på en resilient måte.

Funn i denne studien etterlater et inntrykk av at virksomhetenes nåværende rolleforståelse bare unntaksvis kan forstås fra et instrumentelt perspektiv, og i noen tilfeller helt klart best kan uttrykkes ved hjelp av et kulturelt institusjonelt perspektiv. En økende grad av modenhet i organisasjonene, både i forhold til forståelse og bevissthet rundt hybride trusler, og evnen til å selvstendig kunne danne seg og benytte seg av et trusselbilde som beslutningsgrunnlag, vil riktignok gi grunnlag for en utvikling i retning av en mer instrumentell tilnærming og dermed et bedre grunnlag for å fungere på en resilient måte i et hybrid trusselscenario.

En svakhet ved studien er at informantutvalget primært har sine roller knyttet til sikringsrissiko og utarbeidelse av trusselvurderinger. Dersom utvalget i større grad også hadde inkludert representanter fra virksomhetenes ledelse, kunne det synliggjort om det tilsynelatende fokuset på den operasjonelle dimensjonen på bekostning av den strategiske er reelt. Dersom inntrykket av at virksomhetene har en reaktiv rolle i forhold til trusselbilder som forekommer på samfunnsnivå stemmer, vil det på sin side påvirke virksomhetenes evne til å kunne drive strategisk virksomhetsstyring ut fra idealet om å være proaktiv og risikobasert fremfor hendelsesbasert og reaktiv.

Her spiller også reguleringsregimet inn, da et funksjonelt lovverk innebærer at virksomhetene selv har ansvar for å analysere og vurdere hvilket trusselbilde de må forholde seg til. Så lenge lovverket ikke peker konkret på at virksomhetene har et ansvar for å bidra til samfunnssikkerhet, oppfatter virksomhetene at deres rolle og ansvarsområde er begrenset til egen virksomhet.

Evnen til å kunne oppfatte og forstå en trussel i et hybrid trusselscenario har betydning i både den operasjonelle og den strategiske dimensjonen. Å oppnå en høyere grad av modenhet på tvers av organisasjonen, både i forhold til forståelse og bevissthet med tanke på et hybrid trusselbilde, samt i forhold til investering i kapasitet for å kunne benytte seg av trusselvurderinger som beslutningsgrunnlag, er et premiss for virksomhetenes evne til å ha et langsiktig og strategisk fokus i forhold til hybride trusler, og for å kunne opptre på en resilient måte.

Videre forskning

Dette studiet har vist en sammenheng mellom hvordan olje- og gasselskaper oppfatter og forstår sin rolle i forhold til hybride trusler, og hvordan dette påvirker deres evne til å legge til rette for å fungere på en resilient måte. En konklusjon det er mulig å trekke er at virksomhetene primært forstår sitt ansvar og rolle knyttet til håndtering av enkelthendelser rettet mot dem selv, og ikke fokuserer i samme grad på langsiktige og strategiske dimensjoner. Det kan være interessant å gjøre et tilsvarende studie med et annet utvalg informanter, der ledere og beslutningstakere får bredere representasjon, for å vurdere om det strategiske fokuset får en mer sentral plass. Samtidig vil det også være interessant å se om andre sektorer viser et tilsvarende bilde.

Som det også er påpekt, er virksomhetenes evne til å oppfatte hybride trusler, og ikke minst forstå når de utsettes for hybride trusler, en sårbarhet av stor betydning. Det kan da være interessant å se nærmere på aktiviteter som ligger nært opp til legitim virksomhet. Når går for eksempel vanlig legitim lobbyvirksomhet over streken og blir til en påvirkningsoperasjon som betraktes som en trussel?

Som beskrevet, vil virksomhetenes grad av modenhet i forhold til hybride trusler påvirke deres evne til å fungere på en resilient måte. En faktor her er hvordan trusselvurderinger benyttes som en del av beslutningsgrunnlaget, både fra operasjonelt og strategisk synspunkt. Det vil være interessant å se nærmere på selve beslutningsprosessene, og om usikkerheten som ligger i hybride trusler bidrar til å øke sansynligheten for gå i kjente beslutningsfeller.

Til slutt vil det i fremtiden være interessant å se på betydningen av hvordan selve trusselvurderingene knyttet til et hybrid trusselbilde utarbeides. Spesielt hvilken betydning det har å se på et bredt og sammensatt bilde, om det også fokuseres på økonomi og teknisk operativ evne, og hvilken betydning en bredt sammensatt gruppe analytikere har. Også hvilket eierskap virksomhetene har til trusselvurderingene er interessant, altså om de er utarbeidet internt, basert på egne eller andres datamateriale og hvordan organisasjonen som helhet er involvert.

Referanser

Altaher, N. & Westcott, B. (2019). Four ships targeted in mystery "sabotage attack," says UAE. *CNN World News.* Hentet den 14. August 2021 fra https://edition.cnn.com/2019/05/12/middleeast/uae-cargo-ship-sabotage-intl/index.html

Andersen, S.S. (2006). Aktiv informantintervjuing. *Norsk statsvitenskaplig tidsskrift* (22), s. 278-298.

Andreassen, N. & Bjørkelo,B. (2020). Organisasjonsteori om krisehåndtering i teori og praksis. I: Larsen, A.K. & Dyndal, G.L. (red.), *Strategisk ledelse i krise og krig: Det norske systemet* (s. 86-100). Oslo: Universitetsforlaget

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

BBC (2019, 18. Juni). Gulf of Oman tanker attacks: What we know. *BBC News.* Hentet den 15. August 2021 fra https://www.bbc.com/news/world-middle-east-48627014

Busmundrud, O., Maal, M., Kiran, J.H. & Endregard, M. (2015). Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger. FFI-rapport 2015/00923. Kjeller: Forsvarets forskningsinstitutt.

Caspari,B.C. (2021). *Norges forståelse av hybride trusler: Effektene av ulike konseptualiseringer på myndighetenes samarbeid* (Masteroppgave). Universitetet i Stavanger, Stavanger

Christensen, T., Egeberg, M., Lægreid, P., Roness, P.G. & Røvik, K.A. (2015). *Organisasjonsteori for offentlig sektor* (3. utgave). Oslo: Universitetsforlaget.

Cotovio, V., Regan, H. & Fox, K. (2019, 13. Juni). Two tankers struck in apparent attack in Gulf of Oman. *CNN World News*. Hentet den 14. August 2021 fra https://edition.cnn.com/2019/06/13/middleeast/sea-of-oman-tanker-intl/index.html

Cullen, P. (2018). Hybrid threats as a new “wicked problem” for early warning. *Strategic Analysis, May 2018. Hybrid CoE.* Hentet den 4. August 2021 fra https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-2018-8-Cullen.pdf

Cullen, P. & Wegge, N. (2019). Å varsle om hybride trusler. I Stenslie, S., Haugom, L. og Vaage, B.H. (red.), *Etterretningsanalyse i den digitale tid – en innføring* (1. utgave, s.107-130). Bergen: Fagbokforlaget.

Dey, I. (2004). Grounded Theory. I: Seale, C., Gobo, G., Gubrium, J.F. & Silverman, D. (red.) *Qualitative research practise* (s. 80-93). London: SAGE

Engen, O.A.H., Kruke, B.I., Lindøe, P.H., Olsen, K.H., Olsen, O.E. & Pettersen, K.A. (2016). *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm Akademisk.

Fishbacher-Smith, D. (2016). Framing the UK's counter-terrorism policy within the context of a wicked problem. *Public Money & Management, 36 (6)*, pp. 399-408

Forsvaret (2019). *Et styrket forsvar. Forsvarssjefens fagmilitære råd 2019*. Hentet 23. oktober 2021 fra: https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fagmilitaert-rad/FMR%202019%20fullversjon.pdf/_/attachment/inline/526c0c89-19f5-4be0-a734-d846bafd52e8:14e16c306e4518a1857b6ac69e8e647c5e716bb0/FMR%202019%20fullversjon.pdf

Forsvaret (2022). Fokus 2022: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer. Hentet den 30. mars 2022 fra: https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus-2022-til-web.pdf/_/attachment/inline/ec6bec00-d2d3-41c0-af08-02b3b494e8b7:e4014ab4d0e3bd8b2509e7974430fe121e0473ba/Fokus-2022-til-web.pdf

Forsvarsdepartementet og Justis- og beredskapsdepartementet (2018). *Støtte og samarbeid - En beskrivelse av totalforsvaret i dag.* Hentet den 12. desember 2021 fra: https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/stotte-og-samarbeid-en-beskrivelse-av-totalforsvaret-i-da.pdf

Gassco (2020). *Vurdering av gasstransportalternativer i Barentshavet sør*. Hentet den 12. desember 2021 fra: https://www.npd.no/globalassets/1-npd/publikasjoner/rapporter/rapport-vurdering-av-gasstransportalternativer-barentshavet-sor-2020.pdf

Greenberg, A. (2018, 22. August). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Hentet den 14. August 2021 fra https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hollnagel, E. (2011). Prologue: The Scope of Resilience Engineering. I: Hollnagel, E., Pariès, J., Woods, D.D. & Wreathall, J. (red.) *Resilience Engineering in Practice, a Guidebook*. Boca Ranton: CRC Press.

Hollnagel, E. (2011). Epilogue: The Resilience Analysis Grid. I: Hollnagel, E., Pariès, J., Woods, D.D. & Wreathall, J. (red.) *Resilience Engineering in Practice, a Guidebook*. Boca Ranton: CRC Press.

Hollnagel, E. (2014). *Safety-I and Safety-II – The Past and Future of Safety Management*. Boca Ranton: CRC Press.

Hollnagel, E. (2018). *Safety-II in Practice – Developing the Resilience Potentials*. London & New York: Routledge.

Hollnagel, E., Woods, D.D. & Leveson, N. (2006). *Resilience Engineering, Concepts and Precepts*. Boca Ranton: CRC Press.

Hollnagel, E. & Woods, D.D. (2006). Epilogue: Recilience Engineering Precepts. I: Hollnagel, E., Woods, D.D. & Leveson, N. (red.) *Recilience Engineering, Concepts and Precepts* (s. 347-358). Boca Ranton: CRC Press.

Johansen, P.A. (2019, 7. mars). Da GPS-nettet falt ut på nytt i januar, ble norsk politi forbløffet. Nå peker de på en ny og urovekkende forklaring. Hentet den 7. april 2022 fra: https://www.aftenposten.no/norge/i/XwVWqm/da-gps-nettet-falt-ut-paa-nytt-i-januar-ble-norsk-politi-forbloeffet-n

Jore, S.H. (2020). Is Resilience a Good Concept in Terrorism Research? A Conceptual Adequacy Analysis of Terrorism Resilience. *Studies in Conflict & Terrorism*, http://doi.org/10.1080/1057610X.2020.1738681

Jørgenrud, M.B. (2017, 7. november). Mærsk tapte opptil 2,5 milliarder kroner på dataangrep. *Digi.no.* Hentet den 14. august 2021 fra https://www.digi.no/artikler/maersk-tapte-opptil-2-5-milliarder-kroner-pa-dataangrep/411585

Kovacs, E. (2018, 16. februar). U.S., Canada, Australia Attribute NotPetya Attack to Russia. *Securityweek.com.* Hentet den 14. August 2021 fra https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia

Kvale, S. (1997). *Det kvalitative forskningsintervju*. Oslo: Ad Notam Gyldendal

Ladegård, G. & Vabo, S.I. (2010). *Ledelse og styring*. Bergen: Fagbokforlaget.

Leveson, N. (2020). Safety III: A Systems Approach to Safety and Resilience. Hentet den 22. Mars 2022 fra http://sunnyday.mit.edu/safety-3.pdf

Malerud, S., Hennum, A.C. & Toverød, N. (2021). *Situasjonsforståelse ved sammensatte trusler – et konseptgrunnlag* (FFI-rapport21/00246). Kjeller: Forsvarets forskningsinstitutt.

Mathews, L. (2017, 16. august). NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million. *Forbes.com.* Hentet 14. August 2021 fra https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/?sh=19e54fe54f9a

Monaghan, S. (2019). Countering Hybrid Warfare – So What for the Future Joint Force? *Prism 8*, No. 2, s. 83-98.

Nasjonal sikkerhetsmyndighet (2021). *Risiko 2021 – helhetlig sikring mot sammensatte trusler*. Hentet den 15. august 2021 fra https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler

Nasjonal sikkerhetsmyndighet (2021). Oversikt over innmeldte grunnleggende nasjonale funksjoner. Hentet 30. Oktober 2021 fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/grunnleggende-nasjonale-funksjoner/oversikt-over-innmeldte-grunnleggende-nasjonale-funksjoner/

Nasjonal sikkerhetsmyndighet (2022). Risiko 2022: Økt risiko krever økt årvåkenhet. Hentet den 30. mars 2022 fra: https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

Nilssen, V. (2012). *Analyse i kvalitative studier: den skrivende forskeren*. Oslo: Universitetsforlaget

NOFO (u.å.). Baser og depot. Hentet den 12. desember 2021 fra https://www.nofo.no/kontakt/baser/

NRK (2019, 18. mars). Jamming påvirker oljenæringa. Hentet den 7. april 2022 fra: https://www.nrk.no/tromsogfinnmark/jamming-pavirker-oljenaeringa-1.14477996

Næringslivets sikkerhetsråd (2019). *The Hybrid Survey, Hybrid threats and incidents targeting the Norwegian business community*. Hentet den 15. August 2021 fra https://www.nsr-org.no/uploads/documents/Publikasjoner/hybridundersokelsen-2019-ENG.pdf

Oljedirektoratet (2020, 13. januar). Grunnlag for økt gasstransport fra Barentshavet sør. Hentet den 12. desember 2021 fra https://www.npd.no/fakta/nyheter/generelle-nyheter/2020/grunnlag-for-okt-gasstransport-fra-barentshavet-sor/

Petroleumsloven (1996). Lov om petroleumsvirksomhet (LOV-1996-11-29-72). Hentet fra: https://lovdata.no/dokument/NL/lov/1996-11-29-72?q=petroleumsloven

Politiets sikkerhetstjeneste (2020). *Etterretningstrusselen mot norsk petroleumssektor*. Hentet den 15. August 2021 fra https://www.pst.no/globalassets/artikler/utgivelser/2020/etterretningstrusselen-mot-norsk-petroleumssektor.pdf

Politiets sikkerhetstjeneste (2022). Nasjonal trusselvurdering 2022. Hentet den 21. mars 2022 fra: https://www.pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-norsk.pdf

Prop. 153 L (2016-2017). *Lov om nasjonal sikkerhet (sikkerhetsloven)*. Forsvarsdepartementet.

Rammeforskriften (2010). Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg (FOR-2010-02-12-158). Hentet fra: https://lovdata.no/dokument/SF/forskrift/2010-02-12-158

Reichborn-Kjennerud, E. & Cullen, P. (2016). What is Hybrid Warfare? *Policy Brief 01/2016*, Norwegian Institute of International Affairs (NUPI).

Ritchey, T. (2013). Wicked Problems: Structuring Social Messes with Morphological Analysis. *Swedish Morphological Society - Acta Morphologica Generalis Vol.2 No.1*

Schnelle, S. (2018). *Kartlegging av maritime hybride trusler* (Masteroppgave). Forsvarets høgskole, Oslo.

Sikkerhetsloven (2019). Lov om nasjonal sikkerhet (LOV-2018-06-01-24). Hentet 26. oktober 2021 fra https://lovdata.no/dokument/NL/lov/2018-06-01-24

Society for Risk Analysis (2018). *Society for Risk Analysis Glossary*. Hentet den 26. Oktober 2021 fra: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Statoil (2013). The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas. Prepared for Statoil ASA's board of directors. Hentet den 11. April 2022 fra: https://www.equinor.com/content/dam/statoil/documents/In%20Amenas%20report.pdf

Store norske leksikon (u.å.). *NGO (ikke-statlig organisasjon).* Hentet den 11. april 2022 fra: https://snl.no/NGO_-_ikke-statlig_organisasjon

Store norske leksikon (2021). *Rolle*. Hentet 31. oktober 2021 fra https://snl.no/rolle

Styringsforskriften (2010). Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (FOR-2010-04-29-611). Hentet fra https://lovdata.no/dokument/SF/forskrift/2010-04-29-611?q=styringsforskriften

Sveen, S.L. (2022, 26. februar). Nasjonal sikkerhetsmyndighet ber norske bedrifter om å være årvåkne. *VG*. Hentet den 27. februar 2022 fra https://www.vg.no/nyheter/innenriks/i/Bj2O9E/nasjonal-sikkerhetsmyndighet-ber-norske-bedrifter-om-aa-vaere-aarvaakne

Tjora, A. (2021). *Kvalitative forskningsmetoder i praksis* (4. utg.). Oslo: Gyldendal norsk forlag AS

Tvetbråten, K. & Knutsen, B.O. (2019). Hva nå, norsk forsvarsindustri? Instrumentelle og institusjonelle svar på Eus nye politikk på det sikkerhets- og forsvarspolitiske området. *Internasjonal politikk, Skandinavisk tidsskrift for internasjonale studier. 77 (4).* s. 398-419.

Woods, D.D. & Hollnagel, E. (2006). Prologue: Resilience Engineering Concepts. I: Hollnagel, E., Woods, D.D. & Leveson, N. (red.) *Resilience Engineering, Concepts and Precepts* (s. 1-6). Boca Ranton: CRC Press.

Young, W. & Leveson, N. (2014). An Integrated Approach to Safety and Security Based on Systems Theory. *Communications of the ACM, 57* (2). s. 31-35.

Vedlegg A

Intervjuguide operatørselskaper

Innledende spørsmål knyttet til forståelse og oppfatning av begrepet «hybride trusler» og bevissthet i virksomheten rundt hybride trusler:

1. Hvordan forstår du begrepet «hybride trusler» og hva legger du i begrepet (gjerne med konkrete eksempler)?
    a. Er dette et begrep som benyttes i din virksomhet?
    b. Deler resten av virksomheten din forståelse for begrepet (spesielt beslutningstakere)?
    c. Har hybride trusler egentlig betydning for din virksomhets aktivitet? Hvorfor/hvorfor ikke? (altså: *anser du din virksomhet som et potensielt mål for en trusselaktør eller at virksomheten kan rammes på annen måte i et hybrid trusselscenario?*)
    d. Har din virksomhet trent på å håndtere hybride trusler? (hele eller deler av virksomheten? Samøving med andre virksomheter/sektorer?)
2. Hva slags type trusler mot din virksomhet/sektor vil du omtale som hybride?
    a. Hvilke virkemidler kan ha størst skadepotensiale? Hvorfor?
    b. Hva gjør din virksomhet spesielt sårbar?

Spørsmål knyttet til rolleforståelse:

3. Hvilken rolle har olje- og gasselskaper generelt i forhold til å identifisere hybride trusler?
    a. Hva er din rolle i [din] virksomhet?
    b. Er arbeid med et hybrid trusselbilde formelt en del av ditt (eller andres) ansvarsområde eller gjøres det «på eget initiativ»? Er dette annerledes i forhold til andre typer trusler?
    c. I forhold til hybride trusler, er din rolle anerkjent i virksomheten? (Altså: *Vil organisasjonen (spesielt beslutningstakere) høre på deg og respondere på dine innspill?*)
    d. Har det betydning for securityarbeidet i din virksomhet at en hendelse kan være del av et [større] hybrid trusselbilde?
    e. Har du inntrykk av at hybride trusler er inkludert i virksomhetens risikovurdering og risikostyring? Tas det hensyn til eventuelle hybride trusler i virksomhetens strategiske beslutninger? Hvor lenge har det eventuelt vært det, og hva er grunnen til at det er inkludert? (*er det etter ytre påvirkning eller pga økt fokus internt i virksomheten?*)
4. Hva definerer olje- og gasselskapers rolle i forhold til å identifisere hybride trusler?
    a. Hvilke formelle krav forholder du deg til i forhold til et hybrid trusselbilde?
    b. Er disse [formelle kravene] dekkende i forhold til et hybrid trusselbilde?
    c. Ut over formelle krav, oppfatter du at myndighetene har forventninger til din virksomhet i forhold til å kunne identifisere og håndtere hybride trusler?
5. Oppfatter du at din virksomhet er tilstrekkelig og riktig organisert og utformet for å kunne møte hybride trusler på en tilfredstillende måte?
    a. Hva er i så fall tilfredstillende? (*Er det relatert til myndighetskrav og/eller interne krav?*)
    b. Hvorfor er dere organisert på denne måten?
    c. Er det en generell forventning i virksomheten at en skal kunne håndtere et bredt spekter av trusler, eller er det anerkjent i virksomheten at det finnes begrensninger i hva en er i stand til å kunne identifisere og håndtere?
6. Gitt din oppfatning av din virksomhets rolle i forhold til hybride trusler, har dere tilstrekkelig kapasitet og evne til å kunne identifisere og håndtere hybride trusler?
    a. Hvorfor har dere denne kapasiteten (eller eventuelt hvorfor ikke)?
    b. Hvilke begrensninger har dere, og hva er eventuelt konsekvensene av dette?

Spørsmål knyttet til situasjonsbevissthet (evne til å oppfatte, forstå og forutsi videre utvikling av en trussel):

7. Hva bygger din egen og din virksomhets kunnskap om aktuelle hybride trusler på?
    a. Hvordan vil du normalt oppfatte/identifisere signaler/varsler om pågående eller mulige fremtidige hendelser i et hybrid trusselscenario (*deteksjon*)? Både generelt og spesielt relatert til et case om petroleumsaktivitet i Barentshavet?
    b. Hvor relevant er kunnskap fra andre sektorer og andre (geografiske) områder/land i forhold til hybride trusler mot petroleumsaktivitet i Barentshavet?
    c. I forhold til petroleumsaktivitet i Barentshavet, hvilke faktorer gjør det vanskelig å oppdage og forstå hybride trusler?
8. Hvem anser du som de mest sansynlige trusselaktørene i et hybrid trusselscenario knyttet til et case om petroleumsaktivitet i Barentshavet? (*Både skjulte og eventuelt åpenlyse aktører*)
    a. Spiller det noen rolle for din virksomhet hvem som står bak de hybride truslene? (*attribuering*)
9. Gitt et case som omhandler petroleumsaktivitet i Barentshavet, vil din virksomhet gjøre spesielle forberedelser for å forebygge eller identifisere hybride trusler tidlig?
    a. Kan du se for deg spesielle [lavintensive] hendelser du vil legge større vekt på enn andre som tidlige indikatorer eller varsler om en hybrid trussel?
    b. Hvordan vil du og din virksomhet eventuelt respondere på tidlige varsler?
10. Hvilke sikringshendelser kan forekomme i et hybrid trusselbilde knyttet til et case om petroleumsaktivitet i Barentshavet?
    a. Hvilken betydning har disse hendelsende for andre virksomheter og sektorer?
    b. Hvordan vil du respondere dersom andre virksomheter raporterer om mulige hendelser?
    c. Dersom andre virksomheter rammes, hvordan kan det påvirke din virksomhets aktivitet? (*avhengigheter*)

Oppsummering og avslutning:

11. Har du noen utfyllende kommentarer eller refleksjoner om temaet?
12. Er det andre aktører eller potensielle informanter du mener jeg burde kontakte?

Vedlegg B

Intervjuguide tilsynsmyndigheter

Innledende spørsmål knyttet til forståelse og oppfatning av begrepet «hybride trusler» og bevissthet i virksomheten rundt hybride trusler:

13. Hvordan forstår du begrepet «hybride trusler» og hva legger du i begrepet (gjerne med konkrete eksempler)?
    a. Er dette et begrep som benyttes i din virksomhet?
    b. Deler resten av virksomheten din forståelse for begrepet (spesielt beslutningstakere)?
    c. Har hybride trusler egentlig betydning for din virksomhets aktivitet? Hvorfor/hvorfor ikke? (altså: *anser du din virksomhet eller virksomhetens ansvarsområde som et potensielt mål for en trusselaktør eller at de kan rammes på andre måter i et hybrid trusselscenario?*)
    d. Har din virksomhet trent på å håndtere hybride trusler? (hele eller deler av virksomheten? Samøving med andre virksomheter/sektorer?)
14. Hva slags type trusler mot din virksomhet/sektor vil du omtale som hybride?
    a. Hvilke virkemidler kan ha størst skadepotensiale? Hvorfor?
    b. Hva gjør ditt virksomhetsområde/sektor spesielt sårbart?

Spørsmål knyttet til rolleforståelse:

15. Hvilken rolle har din virksomhet generelt i forhold til å identifisere hybride trusler?
    a. Hva er din rolle i [din] virksomhet?
    b. Er arbeid med et hybrid trusselbilde formelt en del av ditt (eller andres) ansvarsområde eller gjøres det «på eget initiativ»? Er dette annerledes i forhold til andre typer trusler?
    c. I forhold til hybride trusler, er din rolle anerkjent i virksomheten? (Altså: *Vil organisasjonen (spesielt beslutningstakere) høre på deg og respondere på dine innspill?*)
    d. Har du inntrykk av at petroleumssektoren legger vekt på eller ser betydningen av at en sikringshendelse kan være del av et [større] hybrid trusselbilde?
    e. Har du inntrykk av at hybride trusler er inkludert i de ulike virksomhetenes risikovurdering og -styring? (*tas det for eksempel hensyn til eventuelle hybride trusler i virksomhetenes styringssystemer?*) Hvor lenge har det eventuelt vært det, og hva er grunnen til at det er inkludert? (*er det etter ytre påvirkning eller pga økt fokus internt i virksomheten?*)
16. Hva definerer olje- og gasselskapers rolle i forhold til å identifisere hybride trusler?
    a. Hvilke formelle krav (lover, forskrifter, standarder etc.) ligger til grunn i forhold til å vurdere et hybrid trusselbilde?
    b. Er disse [formelle kravene] dekkende i forhold til et hybrid trusselbilde?
    c. Ut over formelle krav, oppfatter du at det er forventninger til at virksomhetene skal kunne identifisere og håndtere hybride trusler?
17. Oppfatter du at virksomhetene du møter i din sektor er tilstrekkelig og riktig organisert og utformet for å kunne møte hybride trusler på en tilfredstillende måte?
    a. Hva er i så fall tilfredstillende? (*Er det relatert til myndighetskrav og/eller interne krav?*)
    b. Hvorfor er de organisert på denne måten?
    c. Er det en generell forventning i virksomhetene at en skal kunne håndtere et bredt spekter av trusler, eller er det anerkjent i virksomhetene at det finnes begrensninger i hva en er i stand til å kunne identifisere og håndtere?

18. Gitt din oppfatning av din virksomhets rolle i forhold til hybride trusler, har den tilstrekkelig kapasitet og evne til å kunne identifisere og håndtere hybride trusler i forhold til virksomhetens ansvar og mandat?
    a. Hvorfor har den denne kapasiteten (eller eventuelt hvorfor ikke)?
    b. Hvilke begrensninger har den, og hva er eventuelt konsekvensene av dette?

Spørsmål knyttet til situasjonsbevissthet (evne til å oppfatte, forstå og forutsi videre utvikling av en trussel):

19. Hva bygger din egen og din virksomhets kunnskap om aktuelle hybride trusler på? Har du inntrykk av at andre virksomheter innen din sektor bygger sin kunnskap på annet grunnlag?
    a. Hvordan vurderer du hvorvidt virksomheter i din sektor er i stand til å oppfatte eller identifisere signaler/varsler om en pågående eller mulig fremtidig hendelse i et hybrid trusselscenario (*deteksjon*)?
    b. Hvor relevant er kunnskap fra andre sektorer og andre (geografiske) områder/land i forhold til hybride trusler spesifikt rettet mot petroleumsaktivitet i Barentshavet?
    c. I forhold til petroleumsaktivitet i Barentshavet, hvilke faktorer gjør det vanskelig å oppdage og forstå hybride trusler?
20. Hvilke trusselaktører anser du som mest sansynlig i et hybrid trusselscenario knyttet til et case om petroleumsaktivitet i Barentshavet? (*Både skjulte og eventuelt åpenlyse aktører*)
    a. Spiller det noen rolle [for virksomheter i din sektor] hvem som egentlig står bak de hybride truslene? (*attribuering*)
21. Gitt et case som omhandler petroleumsaktivitet i Barentshavet, vil du vurdere om virksomheter du fører tilsyn med har gjort spesielle forberedelser for å forebygge eller identifisere hybride trusler tidlig?
    a. Er det spesielle [lavintensive] hendelser du og/eller virksomhetene vil legge større vekt på som tidlige indikatorer eller som varsler om en hybrid trussel?
    b. Hvordan vil virksomhetene eventuelt respondere på slike tidlige varsler?
22. Hvilke sikringshendelser kan forekomme i et hybrid trusselbilde knyttet til et case om petroleumsaktivitet i Barentshavet?
    a. Hvilken betydning kan disse hendelsende ha for andre virksomheter og sektorer?
    b. Hvordan oppfatter du at virksomheter responderer dersom det raporteres om mulige hendelser som kan være del av et hybrid trusselbilde?
    c. Hvilke avhengigheter mellom virksomheter/sektorer har størst betydning dersom noen av disse utsettes for hendelser i et hybrid trusselbilde? (*avhengigheter*)

Oppsummering og avslutning:

23. Har du noen utfyllende kommentarer eller refleksjoner om temaet? Er det noe annet som det kan være nyttig for meg å ta med eller vite om?
24. Er det andre aktører eller potensielle informanter du mener jeg burde kontakte?

Vedlegg C

Informasjonsskriv

Vil du delta i forskningsprosjektet

«Hvilken oppfatning har petroleumssektoren av hybride trusler?»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å studere hvordan olje- og gasselskapers rolleforståelse påvirker deres evne til å oppfatte og forstå hybride trusler. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Prosjektet inngår i en masteroppgave i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger. Formålet er å vurdere hvordan rolleforståelse og -oppfatning påvirker olje- og gasselskapers evne til å oppfatte og forstå hybride trusler, og hvilken betydning dette kan ha for samfunnsikkerheten i en større kontekst. For å demonstrere problemstillingens relevans og for å illustrere hvordan rolleforståelse og situasjonsbevissthet kan teoretiseres i et hybrid trusselbilde, blir problemstillingen drøftet med utgangspunkt i et case rundt utforskning av olje- og gassresurser i Barentshavet.

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 en rolle innen prosjektstyring, sikring og/eller tilsyn i petroleumssektoren, eller tilstøtende sektorer. Datainnsamling i prosjektet foregår ved personlige intervjuer med et utvalg personer (5-15 personer) med disse rollene og funksjonene i sine respektive virksomheter.

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 hvordan du ser på hybride trusler og hvilken betydning hybride trusler har for din virksomhet. 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 oppfatning av hybride trusler generelt, hvilken rolleforståelse olje- og gasselskaper har i forhold til hybride trusler, hvordan hybride trusler kan identifiseres i petroleumssektoren og hvilken betydning disse blir ansett å ha.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. 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 intervuet 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 (Eivind Skare) og veileder (Sissel Haugdal Jore) 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?

Opplysningene anonymiseres når oppgaven er godkjent, noe som etter planen er i midten av mai 2022. Ved prosjektslutt vil alle personopplysninger slettes og/eller makuleres.

Dine rettigheter

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

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til 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 jeg 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 Eivind Skare (e-post: [redacted], telefon: [redacted]) eller veileder Sissel Haugdal Jore (e-post: [redacted], telefon: [redacted])
- Personvernombudet ved Universitetet i Stavanger: personvernombud@uis.no.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Eivind Skare
(student, UiS)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *«Hvilken oppfatning har petroleumssektoren av hybride trusler?»*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju med student (Eivind Skare)
- ☐ at personopplysninger kan oppbevares som beskrevet
- ☐ at data og informasjon som fremkommer i intervjuet kan sammenstilles, analyseres og benyttes i masteroppgaven i annonymisert form
- ☐ 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.

Vedlegg D

Meldeskjema for behandling av personopplysninger, vurdering fra NSD

NSD NORSK SENTER FOR FORSKNINGSDATA

Vurdering

Referansenummer

573214

Prosjekttittel

Hvilken oppfatning har petroleumssektoren av hybride trusler?

Behandlingsansvarlig institusjon

Universitetet i Stavanger / Det teknisk- naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Sissel Haugdal Jore, [redacted]

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Eivind Skare, [redacted]

Prosjektperiode

10.01.2022 - 29.04.2022

Vurdering (1)

20.01.2022 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 20.01.2022, samt i meldingsdialogen mellom innmelder og Personverntjenester. Behandlingen kan starte.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 29.04.2022.

LOVLIG GRUNNLAG

Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

· lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
· formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
· dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
· lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20).

Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.
Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
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).

Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

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. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-imeldeskjema

Du må vente på svar fra oss før endringen gjennomføres.

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

Lykke til med prosjektet!