DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering:
Samfunnssikkerhet

Vårsemesteret, 2022

Åpen

Forfatter: Tom A. Hetlevik

.....
(signatur forfatter)

Fagansvarlig: Ole Andreas Hegland Engen

Veileder(e): Ole Andreas Hegland Engen

Tittel på masteroppgaven: *Statlig etterretning mot petroleumssektoren – nasjonale sikkerhetsinteresser på anbud*

Engelsk tittel: Foreign intelligence aimed at the Norwegian oil and gas sector – national security interests for the lowest bidder

Studiepoeng: 30

Emneord: Sikring, petroleumssektoren
Etterretning, sikkerhetsloven,
petroleumsloven

Sidetall: 76

+ vedlegg/annet: 3

Stavanger, 13/06/2022

Vedtatt av dekan 30.09.21
Det teknisk-naturvitenskapelige fakultet

Statlig etterretning mot petroleumssektoren – nasjonale sikkerhetsinteresser på anbud

MASTEROPPGAVE I SAMFUNNSSIKKERHET
UNIVERSITETET I STAVANGER
VÅR 2022
TOM HETLEVIK

Forord

Denne masteroppgaven er slutten på en annerledes periode. Masterløpet og oppgaveskrivingen har vært preget av to år med pandemi, avløst av en ny krig i Europa. En krig som gjorde oppgavens tema særlig dagsaktuelt.

Jeg ønsker å takke alle som har støttet og bidratt til oppgaven. En familie som har sett mann og far særdeles lite det siste halve året, og en forståelsesfull arbeidsgiver som har gitt mulighet til å skrive oppgaven mens jeg har vært i arbeid. Jeg vil også rette en særlig stor takk til veilederen min Ole Andreas Hegland Engen, for kyndig veiledning som skal ha mye av æren for at jeg har klart å fullføre denne oppgaven.

Tom Hetlevik

Hundvåg, 10. mai 2022

i. Sammendrag

PSTs åpne trusselvurdering for 2020 nevner at etterretning mot norsk petroleumsteknologi kan ha «[…] et stort og langsiktig skadepotensial for Norge, både militært, økonomisk og for nasjonal sikkerhet.». Ved problemstillingen «*På hvilken måte er den økende trusselen fra utenlandsk statlig etterretning ivaretatt gjennom lovverk og reguleringsregimet for petroleumsnæringen?»* har denne oppgaven sett på petroleumssektorens strukturer og lovverk, for å drøfte hvordan disse ivaretar dette trusselbildet. Samt hvilken effekt det kan ha dersom deler av petroleumssektoren blir underlagt sikkerhetsloven. Oppgaven har sett på leverandørindustrien som representant for petroleumsnæringen, og drøfter på hvilken måte det samme trusselbildet påvirker dem.

Oppgaven konkluderer med at både myndigheter og næringen jobber samvittighetsfullt med å ivareta trusselbildet, men at det er noen utfordringer ved økonomisk press i leverandørindustrien som gjør at en etterretningstrussel mot nasjonen kan være vanskelig å ivareta. En tydeliggjøring i lovverket, enten i form av endringer i petroleumsloven eller i form av tilknytning til sikkerhetsloven, vil kunne sette næringen i bedre stand til å ivareta disse utfordringene.

Samtidig argumenteres det for at en tilpassing av PTILs risikodefinisjon kan bidra til å bedre ivareta konsekvenser som ikke er utløst av virksomhetene selv, men likevel er knyttet til dem. På denne måten hensyntar man en trusselaktør som benytter egen virksomhet for å påvirke en tredjepart, og har større mulighet for å ivareta sikringsaspektet.

ii. Innholdsfortegnelse

iii. Figurliste

iv. Forkortelser og begrepsforklaringer

AID	Arbeids- og inkluderingsdepartementet
ATIL	Arbeidstilsynet
COMINT	Communication intelligence - Kommunikasjonsetterretning
GEOINT	Geografisk etterretning
GNF	Grunnleggende nasjonale funksjoner
HUMINT	Human intelligence – Menneskelig etterretning
Leverandørindustri	Samlebetegnelse for leverandører til operatørselskap innen petroleumsnæringen
LNG	Liquid Natural Gas – Gass som komprimeres og kan fraktes på skip i flytende form
NOROG	Norsk Olje og Gass
NORSOK	Norsk Sokkels Konkurranseposisjon - Standard for petroleumsnæringen på norsk sokkel
NSM	Nasjonal Sikkerhetsmyndighet
OD	Oljedirektoratet
OED	Olje- og energidepartementet
OPEC	Organization of the Petroleum Exporting Countries
Operatørselskap (operatør)	Virksomhet som har driftansvar for utvinning/produksjon av petroleumsprodukter
OSINT	Open source intelligence – Åpne kilder
PST	Politiets sikkerhetstjeneste
PTIL	Petroleumstilsynet
Sikringsrisikoanalyse	Sikringsrisikovurdering, samt vurdering av strategier og tiltak

1 Innledning

Denne oppgaven setter søkelys på sikringsrisiko for statlig etterretningsvirksomhet rettet mot petroleumsnæringen i Norge, og hvorvidt denne risikoen er tilstrekkelig regulert av eksisterende rammer. Oppgaven vil vise at det er utfordringer med lovverket i form av sikkerhetsloven, som er ment å ivareta den nasjonale sikkerheten. Men også petroleumsloven, som skal regulere selve petroleumssektoren, er mangelfull for å ivareta sikringsaspektet ved sikkerhet. Utover mer typiske hendelser som terror og andre tidsriktige trusler; er det i stor grad overlatt til næringen selv å definere sine egne sikringstrusler. Dette står i sterk kontrast til hvor omfattende *sikkerhet* er regulert i petroleumsloven.

Som konsekvens av denne omfattende reguleringen har næringen et fokus på sikkerhetsaspektet ved virksomheten, og det finnes gode mekanismer for å ivareta dette. Det mangler likevel tilsvarende mekanismer for sikringstrusler, og da spesielt dem som ikke er definert av den tidligere nevnte petroleumsloven; som ansvarliggjør operatør for å påse at driften er forsvarlig. Dette påse-ansvaret er ikke like omfattende når det kommer til sikringsrisiko, ettersom det er færre målepunkter her i form av lov eller forskrift.

PST kom i 2020 med en åpen trusselvurdering for petroleumsnæringen, hvor etterretning mot norsk petroleumssektor vurderes til å kunne ha «[…] et stort og langsiktig skadepotensial for Norge, både militært, økonomisk og for nasjonal sikkerhet.» (PST, 2020, s. 3). Dette budskapet er gjentatt i senere års åpne trusselvurderinger; fra ulike sikkerhetsmyndigheter som PST, NSM og Etterretningstjenesten. Denne trusselvurderingen står i kontrast til sektormyndighetens tidligere beslutning om å ikke definere petroleumssektoren som tilhørende under sikkerhetsloven, selv om sikkerhetsloven i § 1-5 «Definisjoner»; nevner «forholdet til andre stater og internasjonale organisasjoner» og «økonomisk stabilitet og handlefrihet» som nasjonale sikkerhetsinteresser (Sikkerhetsloven (§1-5), 2018).

Sikkerhetsloven definerer grunnleggende nasjonale funksjoner (GNF) 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 (§1-1), 2018). I 2021 kom Olje- og Energidepartementet med et vedtak om at «kontroll med utvinning av petroleum på norsk

sokkel» (Olje- og energidepartementet, 2021) er ansett som en GNF, noe som vil kunne få betydning for sektorens forhold til sikkerhetsloven.

Ettersom sikring ikke er definert i petroleumsloven utover § 9.3 «Rettighetshaver skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag mot innretninger samt til enhver tid ha beredskapsplaner for slike anslag. […]» (Petroleumsloven (§9-3), 2003), er det en mulighet for at truslene som nevnes av PST ikke fanges opp av operatørselskapenes påseplikt. Dersom dette ikke er regulert av myndighetene er det lite sannsynlig at bedriftene på eget initiativ tar særlig hensyn til et statlig trusselbilde, med mindre dette direkte påvirker driftssikkerhet og til slutt økonomiske interesser for bedriften selv.

Leverandørindustrien er som utgangspunkt ikke direkte omfattet av petroleumslovens § 9.3 annet enn det som pålegges av operatør eller kunde, og de er i likhet med resten av petroleumsnæringen heller ikke omfattet av sikkerhetsloven i skrivende stund. I så måte er det ingen direkte sikringskrav til leverandørindustrien fra myndighetenes side. Det eksisterer ISO-sertifiseringer, standarder og bransjestandarder, men disse omfatter oftest andre ting enn statlig etterretningstrussel, og er heller ikke bindende i de fleste tilfeller. Selv om aspekter ved denne trusselen vil ivaretas der det sammenfaller med mer ordinære trusler som industrispionasje. Leverandørindustrien består også av en stor del internasjonale virksomheter med utenlandsk eierskap, som har få incentiver for å forholde seg til en eventuell differensiert etterretningstrussel i alle land de opererer.

Kombinasjonen av manglende fokus på sikringstrusler i petroleumsloven, internasjonalt eierskap og at næringen ikke er regulert av sikkerhetsloven, kan bidra til at petroleumsnæringen generelt, og leverandørindustrien spesielt, setter for høye risikoakseptkriterier for statlig etterretningsvirksomhet. Noe som igjen kan lede til at eventuelle trusselvurderinger og sikringsrisikovurderinger kan vise til feil risikonivå. Deler av trusselbildet vil likevel dekkes opp av generelle sikrings- og sikkerhetstiltak; for det man kan kalle normale trusler og potensielle hendelser. Petroleumsnæringen er også en høyrisikonæring, og vil dra nytte av overlappende interesser mellom sikkerhet og sikring. Der bedriften ikke har risiko for økonomiske konsekvenser, eller det dekkes av petroleumsloven, vil det derimot kunne oppstå gap i tiltak. Disse gapene vil kunne bli utnyttet av utenlandsk etterretning for å blant annet kartlegge infrastruktur.

Der det eventuelt er gjennomført en trusselvurdering; er det manglende incentiver for å sette statlig etterretningsvirksomhet som sikringstrussel. Dette vil dermed lede til at en etterfølgende sårbarhetsvurdering ikke vil avdekke de tidligere nevnte gapene som sårbarheter. Videre vil dette kunne føre til at eventuelle sikringstiltak ikke blir vurdert, ettersom det ikke vil være relevant for den trusselen man har definert. Dersom du tenker at bilen din er så gammel at ingen gidder å stjele den, ser du gjerne ikke behov for å låse den. Men hva om tyven bare er interessert i kopiere informasjon fra vognkortet for å gjøre et identitetstyveri? Ved å ikke kjenne til eller anerkjenne denne trusselen vil man heller ikke gjøre tiltak mot den.

Det kan diskuteres hvorvidt petroleumsnæringen og leverandørindustrien burde høre inn under sikkerhetsloven i kraft av definisjonene nevnt i sikkerhetslovens § 1-5. Uavhengig av om næringen er regulert av sikkerhetsloven eller ikke, eksisterer det et trusselpotensiale mot både enkeltselskaper, næringen og nasjonen Norge når det kommer til villede handlinger; fra både statlige og ikke-statlige aktører. Dette ettersom både teknologi og informasjon på avveie kan utløse store konsekvenser i ulike former, som vist i PSTs trusselvurdering.

1.1 Problemstilling

Oppgaven har som mål å drøfte hvordan petroleumsnæringen, representert ved leverandørindustrien, forholder seg til statlig etterretning som en sikringstrussel i lys av PSTs trusselvurdering for næringen (PST, 2020). Utgangspunktet for drøftingen er problemstillingen; *På hvilken måte er den økende trusselen fra utenlandsk statlig etterretning ivaretatt gjennom lovverk og reguleringsregimet for petroleumssektoren?* For å utdype denne problemstillingen er det også benyttet følgende forskningsspørsmål:

1. *På hvilken måte kan strukturer og lovverk bidra til å motvirke statlig etterretning som trussel mot petroleumssektoren?*
2. *Hva gjør petroleumssektoren til et attraktivt etterretningsmål?*
3. *Hvordan forholder leverandørindustrien seg til statlig etterretning som en nasjonal trussel?*

Ved hjelp av forskningsspørsmålene, vil det drøftes om det nåværende lovverket er dekkende for å motvirke en statlig trusselaktør mot petroleumsnæringen med tilhørende

infrastruktur, og hvordan petroleums-myndighetene og næringen forholder seg til statlig etterretning som en trussel. For det første vil det være nødvendig se på hvordan petroleumssektoren er organisert, og hvilke virkemidler man har tilgjengelig i form av lover og forskrifter. Deretter vil oppgaven drøfte hva som gjør petroleumssektoren til et attraktivt mål for statlig etterretning slik som oppgitt i PSTs, og senere andres trusselvurderinger. Til slutt er leverandørindustrien valgt som representant for petroleumsnæringen. Og oppgaven vil drøfte hvordan denne næringen forholder seg til statlig etterretning som nasjonal trussel. Ved å se på spørsmål en og to i sammenheng; vil oppgaven drøfte om det er en sammenheng mellom hvordan strukturer og lovverk er utformet, og hvordan dette gjenspeiles i leverandørindustriens tilnærming til risiko og risikoakseptkriterier for statlig etterretning som trussel.

1.2 Avgrensing

Oppgaven tar utgangspunkt i PSTs trusselvurdering for petroleumssektoren, som kom i 2020. Denne trusselvurderingen er i etterkant styrket og gjentatt, med fokus på statlig etterretning og inngripen. Oppgaven vil drøfte på hvilken måte petroleumssektoren forholder seg til denne trusselen ved å analysere lovverk, styringsregime, og næringen selv. Ettersom leverandørindustrien er siste ledd i både reguleringskjeden og den økonomiske kjeden, anses denne bransjen for å være en sårbarhet i petroleumssektoren. Grunnet oppgavens omfang er den derfor avgrenset til leverandørindustrien som representant for næringen.

1.3 Disposisjon

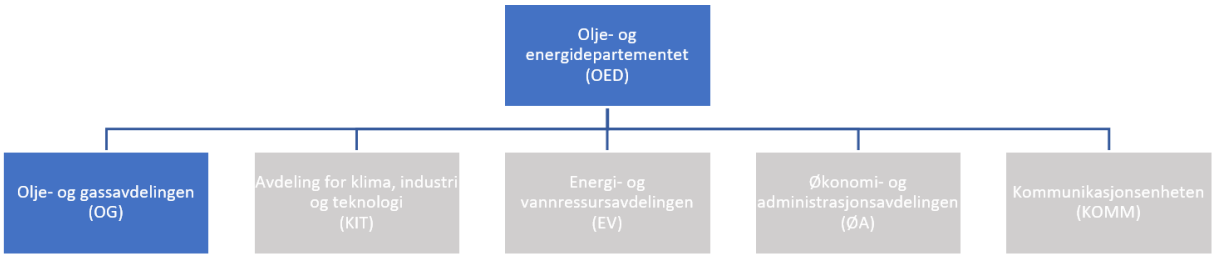
Oppgaven vil først etablere en kortfattet systembeskrivelse for petroleumssektoren i kapittel 2, før den i kapittel 3 gjennomgår relevante teoretiske hovedaspekter ved oppgavens tema; som oppsummeres i 3.7, etterfulgt av benyttet forskningsmetode i kapittel 4. Deretter vil den presentere empiri i form av funn fra litteraturstudie og informantintervjuer i oppgavens kapittel 5, før disse funnene drøftes i kapittel 6 og en konklusjon presenteres i kapittel 7.

2 Petroleumssektoren

Petroleumssektoren kan grovt deles inn i statlig og privat del; der staten er premissleverandør og reguleringsmyndighet for (privat) næring gjennom politisk styring. Staten representeres ved Olje- og energidepartementet (OED), Oljedirektoratet (OD) og Petroleumstilsynet (PTIL). Hvor OED har det overordnede sektoransvaret for petroleumssektoren. Herunder å definere hvorvidt sikkerhetsloven skal gjelde helt eller delvis for virksomheter som opererer innenfor denne sektoren. Sikkerhetsloven vil bli mer omfattende presentert i kapittel 3.6.

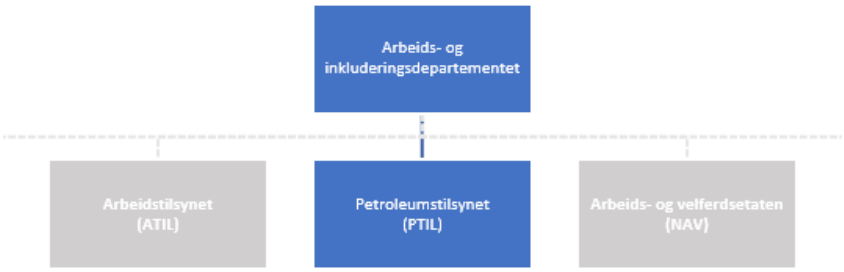
2.1 Petroleumsmyndighetene

Sektoransvarlig departement er som tidligere nevnt OED; med overordnet ansvar for petroleumssektoren. OEDs hovedoppgave «er å tilrettelegge en samordnet og helhetlig energipolitikk» (Regjeringen, 2022a). Figur 1 viser organisasjonskartet, hvor Olje- og gassavdelingen er en av flere avdelinger med ulike ansvarsområder.



Figur 1 Organisasjonskart for Olje- og energidepartementet

Petroleumssektoren faller naturlig under Olje- og gassavdelingens (OG) ansvarsområde. Men som vi vil se i 2.2, er det også deler av Energi- og vannressursavdelingens (EV) ansvarsområde som kan bli berørt av virksomheter innen det som tradisjonelt sett kalles petroleumsnæringen. Det er da spesifikt snakk om Seksjon for nett, energibruk og marked (NEM) som blant annet følger opp sikkerhet og beredskap i kraftforsyningen (Regjeringen, 2022d). OED har med sitt sektoransvar, i henhold til sikkerhetsloven, ansvar for å definere skjermingsverdige objekter eller informasjon innen petroleumssektoren.

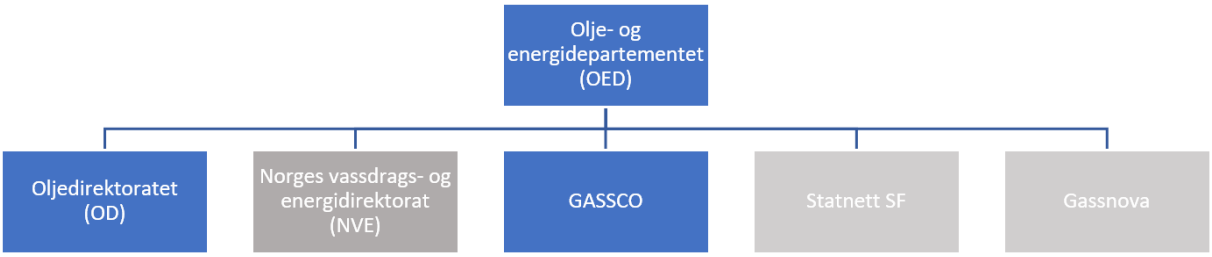


Figur 2 PTIL tilhørighet

Petroleumstilsynet som man kunne forventet at var underlagt OED, er derimot direkte underlagt Arbeids- og inkluderingsdepartementet; som vist i figur 2. PTIL er tilsynsmyndighet for petroleumsnæringen, og premissleverandør for hvordan denne næringen prioriterer sikkerhets- og sikringsarbeidet sitt. PTIL oppgir selv sin rolle som «[…] et statlig tilsyns – og forvaltningsorgan med myndighetsansvar for sikkerhet, arbeidsmiljø, beredskap og sikring i petroleumsvirksomheten» (Petroleumstilsynet, 2022b). Som vi ser, er både Olje- og energidepartementet (OED) og Arbeids- og inkluderingsdepartementet (AID) sektormyndigheter for petroleumssektoren. I 2013 ble ansvaret for ivaretakelse av petroleumslovens § 9-3 *Beredskap mot bevisste anslag*; overført fra OED til AID gjennom PTIL (FFI, 2016).

I Olje- og gassavdelingen (OG) er de mest aktuelle avdelingene for denne oppgavens tema *Seksjon for utbygging og drift* (UDR) som har etatsansvar for OD, *Seksjon for analyse og infrastruktur* (AI) som har ansvaret for «Planlegging, utvikling, drift og bruk av rørledninger og landbehandlingsanlegg for gass og olje.» (Regjeringen, 2022c) og *Petroleumsjuridisk seksjon* (PJS) som har «Utarbeidelse av traktattekster, lover, forskrifter og konsesjonsverk. […] Juridisk rådgivning. Behandling av juridiske spørsmål knyttet til avtaler og samtykker.» (Regjeringen, 2022b) som en del av sitt ansvarsområde.

Videre er det ulike etater, virksomheter og tilsyn som er relevante å trekke frem i sammenheng med styring og regulering av petroleumssektoren og tilhørende infrastruktur. Figur 3 viser hvordan de ulike enhetene er organisert i forhold til hverandre. Som vi ser er ikke GASSCO underlagt OG, men infrastrukturen er naturlig tilhørende under OGs jurisdiksjon og PTILs tilsynsmyndighet.

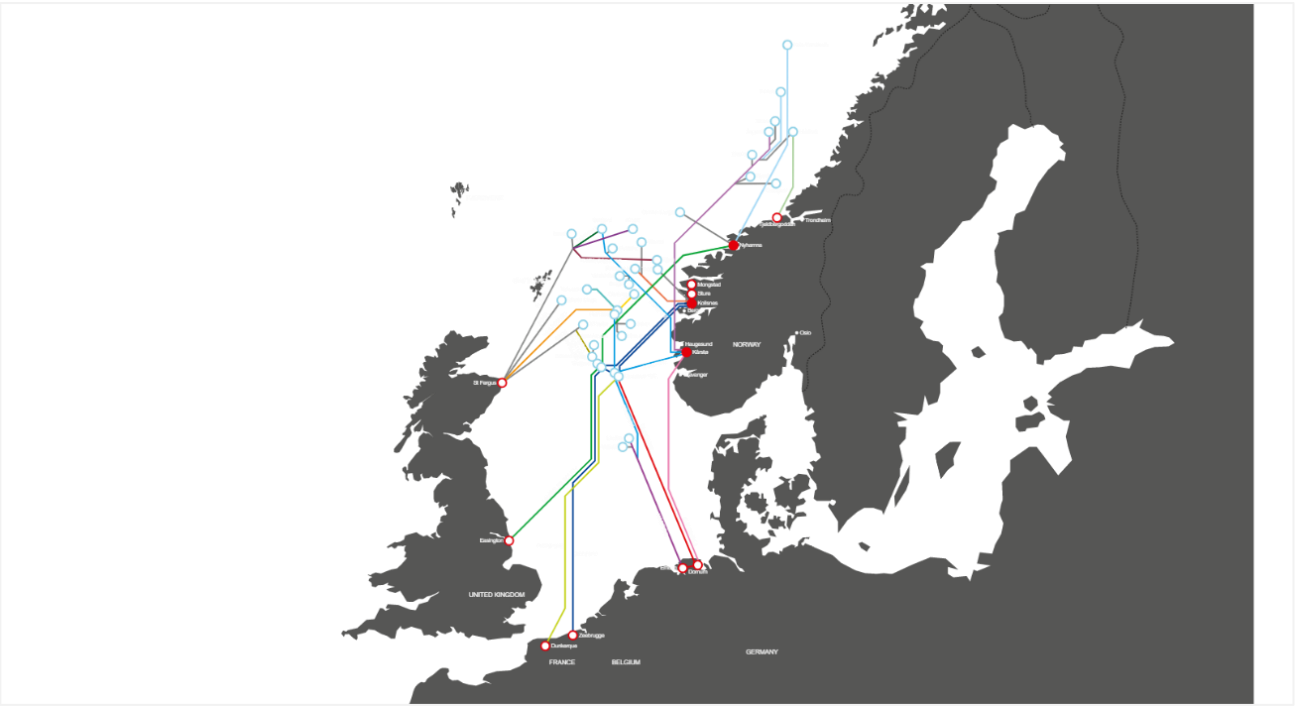


Figur 3 Etater og virksomheter under OED

Det er også i denne oversikten enkelte av virksomhetene og etatene som kan være aktuelle for petroleumsnæringen, selv om de ikke er direkte relatert til petroleumsutvinning og foredling. Ettersom denne oppgaven omhandler petroleumssektoren spesifikt, vil disse andre etatene og virksomhetene ikke bli videre utdypet her.

Av virksomhetene underlagt OED er det hovedsakelig OD og GASSCO som er direkte relevante for petroleumssektoren og den statlige etterretningstrusselen som er tema for oppgaven. OD som fagdirektorat «setter rammer, fastsetter forskrifter og fatter vedtak der dette er delegert […]» (Oljedirektoratet, 2022). OD er i hovedsak en ressursforvalter, og jobber for tilgjengelighet og åpenhet til data og effektiv ressursutnyttelse. OD, sammen med PTIL er også en naturlig aktør i vurderingen av hvorvidt petroleumssektoren skal omfattes av sikkerhetsloven som vil bli presentert i 3.6. Dette kan gi interessekonflikter ettersom de fra et forvaltnings- og effektivitetsperspektiv ønsker å minimere restriksjoner for sektoren.

GASSCO er regulert i petroleumsloven, med roller og oppgaver innenfor leveranse av gass utvunnet på norsk sokkel. Herunder; drift og utvikling av infrastruktur, kapasitetsadministrasjon og systemdrift (GASSCO, 2022b). Figur 4 viser det omfattende rørnettet under GASSCOs ansvarsområde. Dette rørnettet er kritisk for Norges produksjon og leveranse av gass, og hvordan GASSCO som virksomhet forholder seg til det statlige trusselbildet er derfor av stor betydning for hvor sårbar norsk, men også europeisk, forsyningssikkerhet av petroleumsprodukter er, jf. kapittel 5.2.



Figur 4 Eksport- og transportsystemer underlagt GASSCO (GASSCO, 2022a)

2.2 Petroleumsnæringen

Petroleumsnæringen består av flere kategorier av selskaper. Fra operatører som Equinor og Aker BP, via store leverandørbedrifter som Schlumberger og Halliburton, til små nisjeselskaper med et fåtall ansatte. Disse leverandørene arbeider gjerne tett integrert med operatøren av feltet; og i mange tilfeller på vegne av operatøren, noe som eksponerer dem for statlige etterretningsinteresser. I tillegg er det flere virksomheter innen leverandørindustrien som også jobber opp mot andre markeder, eksempelvis legging og inspeksjon av undersjøiske kabler og annen infrastruktur, både til lands og til vanns.

Det som tradisjonelt omtales som petroleumsnæringen har i det siste skiftet mer mot å kunne kalles energinæringen; ettersom det i stadig større grad også fokuseres på alternativer til petroleumsutvinning, eksempelvis havvindmøller og annen energiproduksjon til havs og på land. Energiproduksjon som staten Norge vil være avhengig av, men som også er den del av det europeiske kraft- og strømnettet, og dermed et mulig attraktivt mål for statlig etterretning for å kartlegge eventuelle sårbarheter.

2.3 Leverandørindustrien

Leverandørindustrien består av en mengde større og mindre virksomheter, som i varierende grad har nærhet til infrastruktur tilhørende produksjon, foredling og salg av petroleumsprodukter både på land og til havs. Samtidig er leverandørindustrien en bransje med spesialisering innen undersjøisk konstruksjon og teknologi, herunder fjernstyring av denne teknologien. Dette gjør bransjen til en naturlig aktør å benytte også i sammenheng med annen infrastruktur som befinner seg til havs, enten det er over eller under vannet. Som følge av spesialkompetansen de besitter; opererer leverandørindustrien også innenfor legging og inspeksjon av infrastruktur som kommunikasjonskabler og energioverføringskabler. I så måte vil en uønsket handling mot leverandørindustrien også kunne omfatte energiforsyning og annen kritisk infrastruktur utover petroleumssektoren.

Leverandørindustrien er preget av en del store selskaper som dominerer, ofte med utenlandske eiere og eierinteresser. Tre store aktører som utmerker seg innen overflatetjenester og brønnoperasjoner er Halliburton, Schlumberger og Baker Hughes. Når det kommer til undervannstjenester domineres dette markedet av aktører som Oceaneering, Subsea 7, Deep Ocean og IKM. Enkelte av leverandørene kan også finnes igjen på landanlegg, hvor de leverer tilsvarende tjenester som offshore. I tillegg til de store aktørene er det også et stort antall mer eller mindre spesialiserte bedrifter av varierende størrelse som opererer på sokkelen og tilknyttet infrastruktur.

For enkelhets skyld deles leverandørindustrien her opp i tre hoveddeler; offshore undervannstjenester (undervannstjenester), offshore overflatetjenester (overflatetjenester) og onshore infrastruktur (landtjenester). De ulike hoveddelene har også forskjellige aspekter som ingeniørvirksomhet med mer tilknyttet hoveddelen. Nummer én undervannstjenester; kan være design, konstruksjon, vedlikehold og inspeksjon av infrastruktur, men også dag til dag operasjoner under leting etter, og produksjon av, petroleumsforekomster. Dette gir leverandørvirksomheter tilgang til store mengder informasjon om hva som er bygget, hvordan det er bygget, og eventuelle kapasiteter og sårbarheter som eksisterer. Nummer to overflatetjenester; kan omfatte hele spekteret. Blant annet; dag til dag drift av lete og produksjonsinstallasjoner, konstruksjon, vedlikehold og inspeksjon av overflateinfrastruktur, innhenting og tolking av letedata, med mer. Nummer tre landtjenester; kan innebære arbeid på anlegg hvor petroleumsproduktene foredles og videresendes. Da i form av eksempelvis

inspeksjon og reparasjon av disse anleggene, men også daglig drift. Eksempler på slike anlegg er Melkøya, Mongstad, Kollsnes og Kårstø, som alle er ilandførings-, eksport- eller prosesseringsanlegg med tilhørende transportfasiliteter. Enten i form av undersjøiske og transnasjonale rørledninger, eller kaianlegg for tankskip som frakter olje og gass (LNG). Disse anleggenes sårbarheter vil kunne kartlegges i høy detalj av en aktør som infiltrerer leverandørindustrien, noe som kan gjøre leverandørindustrien av stor interesse for statlig etterretning.

Flere virksomheter i leverandørindustrien utvikler også sine egne fjernstyrte eller autonome undervannsfarkoster; med tiltenkt primærbruk av petroleums- og subsea-bransjen. Teknologien er like fullt aktuell i militær sammenheng, og enkelte av aktørene innen utvikling leverer produkter både til petroleumssektoren og til forsvarssektoren (Haugstad, 2019). Denne teknologien, blant flere andre, kan være interessant for fremmed etterretning å sikre seg tilgang til for å kunne kopiere eller forstyrre (PST, 2020).

3 Teori

Temaet sikring for petroleumssektoren og undersjøisk infrastruktur involverer flere lover, risiko- og sikkerhetsbegreper. Kompleksiteten kommer blant annet av en kombinasjon av uklarheter i lovverk, ulik opplevelse av trusselnivå, og delingen av det sektorielle ansvaret for ulike deler av det man kan definere som petroleumssektoren.

Disse ulike lovverkene og sektormyndighetene kan definere og forholde seg til risiko på forskjellige måter, basert på ulike utgangspunkter for hva som oppleves som den dominerende trusselen, og om denne er sikkerhets- eller sikringsrelatert. I petroleumssektoren har, kanskje med rette, sikkerhetsaspektet fått betydelig mer plass enn sikringsaspektet.

Dette kapittelet drøfter deler av kompleksiteten i sektoren, og hvordan lovverket påvirker hvordan næringen forholder seg til risiko for sikringstrusler. Først presenteres de mest fremtredende begrepene innen risiko og risikovurderinger, både innen sikkerhet og sikring. Deretter vil de ulike lovene presenteres, før det gis en oppsummering av teorigrunnlaget i kapittelets 3.7.

Det første og mest grunnleggende som presenteres er risikobegrepet, som deretter vil plasseres i sammenheng med oppgavens problemstilling. I sikkerhetsfaget, herunder sikring og sikkerhet, er *risiko* et sentralt begrep. Risikobegrepet kan brukes for å styrke sikringsarbeidet innen petroleumssektoren, men det kan også rettferdiggjøre et mindre strengt sikringsregime som et resultat av beslutninger i risikoanalyseprosessen, og dermed svekke sikringsarbeidet. I lys av problemstillingen (se side 8), er risikodefinisjonen man benytter av stor betydning for hvordan man forholder seg til risikovurdering som beslutningsgrunnlag. Dersom man benytter en ren sannsynlighet/konsekvens-tilnærming i en sikringssammenheng, vil det det kunne gi et misvisende resultat. Dersom man benytter en tilnærming med usikkerhet som faktor vil man kunne presentere en mer nyansert og presis risikovurdering, der beslutningstaker er bedre i stand til å fatte gode beslutninger.

Risikoanalysene som gjennomføres vil i stor grad diktere hvordan ulike etater og virksomheter forholder seg til sikringstrusler, det være seg statlige eller ikke-statlige. I forbindelse med risikovurderingene vil man som utgangspunkt måtte sette *risikoakseptkriterier*. Dette kapittelets 3.2 vil presentere ulike måter *risikoakseptkriterier* kan

påvirke hvordan man konkluderer med tanke på risikoreduserende tiltak. Det vil senere drøftes hvordan de valgte *risikoakseptkriteriene* i petroleumsnæringen er avgjørende for hvor sårbar næringen er for statlig etterretning.

Statlig etterretning har mange fellestrekk med de ordinære sikringstruslene ulike virksomheter til enhver tid må forholde seg til. Virksomhetene i petroleumsnæringen har som oftest et sikringsregime for ordinære trusler som industrispionasje, sabotasje og cyberangrep. Som følge av fellestrekkene vil de fleste sikringstiltakene også ha en effekt mot ulike deler av etterretningstrusselen. I kapittel 3.4 beskrives sikringsfaget og hvordan det skiller seg fra sikkerhetsfaget. Deretter vil det i kapittel 5 drøftes ulike aspekter ved statlig etterretning som gjør det unikt sammenlignet med ordinære sikringstrusler.

Sikkerhet som overordnet begrep på norsk, inneholder både sikkerhets- og sikringsbegrepet. Selv om denne oppgaven vil fokusere på sikringsaspektet, vil det være deler av sikkerhetsaspektet som kan være relevant også for statlig etterretningstrussel. Petroleumsnæringen er strengt regulert på sikkerhetsfeltet, noe som vil kunne ha synergieffekter mot sikringsfeltet; og dermed ivareta enkelte av svakhetene ved regimet for sikringsfeltet i petroleumsnæringen. Underkapittel 3.3 vil drøfte hvordan enkelte av disse synergiene kan fremstå.

I Norge er petroleumsnæringen på enkelte områder strengt regulert av myndighetene gjennom petroleumsloven. Det vil i 3.5 belyses hvordan petroleumsloven forholder seg til sikringsfeltet, og på hvilken måte den påvirker næringens eget sikringsarbeid. Videre vil dette kapittelet også beskrive hvilke muligheter for å regulere næringen som ligger i sikkerhetsloven dersom den gjøres gjeldende, enten helt eller delvis, for petroleumsnæringen.

3.1 Risiko

Lovverket som regulerer petroleumsnæringen og det nasjonale sikkerhetsarbeidet handler i stor grad om å redusere risiko for negative hendelser, det være seg innenfor sikkerhets- eller sikringsfeltet.

Risikobegrepet er brukt av flere fagfelt, med ulik tilnærming til temaet. Dette blant annet ettersom risiko, og hvordan det er hensiktsmessig å definere det, vil variere mellom ulike aktiviteter og kontekster. Aven (2015) argumenterer for at risiko ikke trenger å være

ensbetydende med negativt fortegn. Man kan også ønske å oppsøke risiko, eller vurdere risiko for mulige positive utfall. I sammenheng med statlig etterretning mot petroleumsnæringen er det ikke like aktuelt med positive sider ved risiko, selv om det kanskje er mulig å argumentere for at de eksisterer.

Som følge av ulike tilnærminger til risiko, er en utfordring med risikobegrepet at det eksisterer ulike forståelser. Dersom man ikke avklarer hvilken forståelse man legger til grunn kan det gjøre stort utslag på beslutninger som blir fattet på bakgrunn av risikobeskrivelsen. Mens en ingeniør naturlig vil forholde seg til matematiske beregninger av den klassiske definisjonen av risiko (sannsynlighet x konsekvens), vil andre grupperinger som sikring-, samfunns- og økonomifeltet fokusere mer på kvalitative vurderinger som inkluderer usikkerhet.

Når ingeniører beregner risiko ved å bruke sannsynlighet x konsekvens sier vi gjerne at de bruker en statistisk metode (Aven, 2015). I andre sammenhenger kan denne definisjonen som tidligere nevnt være villedende, ettersom den kan fremstille risiko som noe absolutt målbart, og ikke fanger opp usikkerhetsbegrepet. Følgelig er statistisk metode best egnet for bruk innenfor sikkerhetssegmentet og teknisk tilnærming, hvor man kan gjøre statistiske beregninger av feilprosent i produkter og toleranser i materialer.

Usikkerhet kan handle om usikkerhet knyttet til kvaliteten på datagrunnlaget, usikkerhet om hva vi trenger å få data om, og ikke minst usikkerheten om hva som vil skje i fremtiden. Når man har så mange usikkerhetsmomenter, hevder Aven (2015) at det er problematisk å hevde at det er mulig å kvantifisere risiko i en risikoanalyse. Risiko vil derimot kunne *beskrives* ved å inkludere kontekst og kunnskapsgrunnlag (Aven, 2015), dette er særlig relevant når man skal håndtere en trusselaktør med en intensjon. PTIL har som følge av utfordringen med usikkerhet som faktor; selv definert risiko som «[…] konsekvensene av virksomheten med tilhørende usikkerhet.» (PTIL, 2022). Ved å inkludere usikkerhet i risikodefinisjonen løfter man denne frem i beslutningsprosessen, slik at beslutningstakere har et bedre grunnlag for beslutninger som angår risiko og akseptkriterier. I rammeforskriften fremheves det at man skal redusere usikkerhet til et minimum (rammeforskriften, 2010, §11).

Risiko i sikringssammenheng er uløselig knyttet til usikkerhet. Så lenge det er snakk om menneskelige faktorer, herunder evne og vilje til å gjennomføre en handling, vil det innebære høy grad av usikkerhet. Motivasjon kan svikte, eller man kan ha tatt feil av ytre og indre motivasjonsfaktorer for trusselaktøren. Et menneske er også refleksivt, og kan endre sin tilnærming basert på mottiltak. I vårt tilfelle kan man feilvurdere den statlige aktørens risikovilje og frykt for å eksponeres, eller hva trusselaktøren ønsker å oppnå med en handling. Like fullt er ikke usikkerhet gjengitt som et moment i standarden for sikringsrisikoanalyse som lyder: «[Risiko er et] uttrykk for forholdet mellom trusselen […] mot en gitt verdi […] og denne verdiens sårbarhet […] overfor den spesifiserte trusselen» (Standard Norge, 2012). Oppgaven vil komme tilbake til ulike aspekter ved en sikringstrussel i kapittel 3.3 og 3.4.

Njå et al. (2020) definerer risiko i kontekst av samfunnssikkerhet som å være «[…] et uttrykk for konsekvens/utfall av uønskede hendelser og usikkerhet assosiert med hendelser og utfall.» Vi ser at både PTIL og Njå et al. fremhever usikkerhet som en viktig del av risikoforståelsen. I denne oppgaven vil Njå et als definisjon benyttes, ettersom den i størst grad tar hensyn til usikkerhet tilknyttet både hendelse og utfall.

I forbindelse med risikoanalyser er sårbarhet og resiliens viktige begreper, som gjerne kan sies å være motpoler i forbindelse med risiko. Aven (2015) beskriver en sårbarhet som betinget risiko, og gjengir Sårbarhetsutvalgets definisjon av sårbarhet som «[….] et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet. […]» (Aven, 2015, s. 44). En annen måte å beskrive sårbarhet på er ved å dele ordet sår-bar, altså at man er åpen for å såres eller påføres skade. På den andre siden beskriver resiliens som «[…] en enhets […] evne til å kjenne igjen, tilpasse seg og absorbere variasjoner, endringer, forstyrrelser og overraskelser.» (Aven, 2015, s. 45).

For gasseksporten som går til Europa kan en sårbarhet være strømbortfall ved ilandføringsanlegget. En hypotetisk situasjon kan være at man mister strøm, og dermed må stenge gasseksporten. For å motvirke denne sårbarheten; kan man sette opp en alternativ strømkilde i form av aggregater som kan overta strømforsyningen dersom man får brudd i primærforsyningen, og dermed gjøre anlegget mer robust mot denne typen hendelser. Når

man blir robust mot flere mulige hendelser, og evner å fange opp og håndtere dem, både teknisk og organisatorisk, vil man kunne si at gasseksporten er mer resilient.

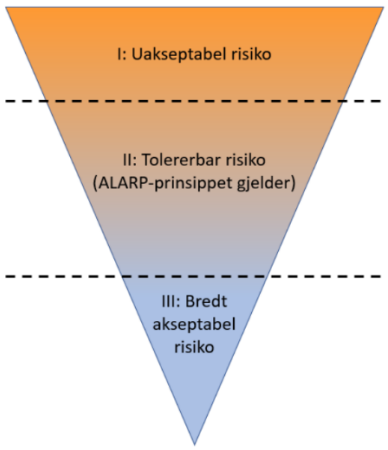
3.2 Risikoakseptkriterier

En risikovurdering er avhengig av referansepunkter for hva som er akseptabel risiko, og i petroleumsnæringen er risikoakseptkriterier en etablert måte å gjøre dette på. Det er eksempelvis skrevet inn krav om risikoakseptkriterier i styringsforskriften (Styringsforskriften, 2001). Dette kravet er dog knyttet til sikkerhetsperspektivet. I dette delkapittelet vil risikoakseptkriterier generelt presenteres, før de knyttes mer opp mot sikringsperspektivet. I oppgavens kapittel 6 vil det drøftes hvorvidt det er svakheter når det kommer til risikoakseptkriterier for sikringsfeltet.

PTIL definerer selv, i en rapport produsert av Proactima, risikoakseptkriterier som «[…] et kjennetegn, et prinsipp, en regel, test eller en standard for hvordan foreta en vurdering av hva som er akseptabel (godkjent/godtatt) risiko eller beslutte hva som er en akseptabel (godkjent/godtatt) risiko.» (Abrahamsen et al., 2020, s. 23) For deretter å dele det opp i «de som kan direkte relateres til en risikoanalyse og dennes resultater» og «de som ikke er det [Direkte relatert til en risikoanalyse]» (Abrahamsen et al., 2020, s. 23).

Et risikoakseptkriterie er altså et målepunkt og et verktøy man benytter for å sette grenseverdier for når man bør og skal gjøre risikoreduserende tiltak, og hvor omfattende disse skal være. Hvordan man forholder seg til arbeidet med å utarbeide disse kriteriene vil dermed kunne ha en stor påvirkning på hva som anses som «lav nok» risiko, enten vi snakker sikring eller sikkerhet.

Det er flere måter å bruke risikoakseptkriterier på. Disse kriteriene vil ofte variere med type risiko som skal beregnes; og kan blant annet uttales ved AIR (årlig individuell sannsynlighet for en person eller stilling), FAR-verdi (fatal accident rate), sannsynlighet for bortfall av sikkerhetsfunksjoner, med mer. Felles for dem alle er at de gir en referanseverdi som sier noe om forventet frekvens eller utfall av en hendelse (Abrahamsen et al., 2020).



Figur 5 TOR-rammeverket (Abrahamsen et al., 2020)

En etablert måte å tenke på risikonivå, er å forholde seg til en tredeling av risiko; mellom uakseptabel risiko, tolererbar risiko (ALARP), og bredt akseptabel risiko (Abrahamsen et al., 2020) som vist i figur 5. ALARP innebærer å gjøre en avveining mellom kostnad og videre oppnådd reduksjon i risiko. Og man vil gjerne komme til et punkt hvor den økte kostnaden ved en ytterligere reduksjon i risiko ikke vurderes som akseptabel. Grafisk fremstilles gjerne ALARP-nivået som gult i en klassisk risikomatrise, uakseptabel risiko vil da være rød og bredt akseptert risiko vil være grønn (Abrahamsen et al., 2020).

Når det kommer til sikringsrisiko, og da spesielt en trussel som statlig etterretning, er det gjerne enda vanskeligere å vite om risikonivået befinner seg i kategorien uakseptabelt, ALARP, eller om det er allment akseptert risikonivå. Her vil det være avhengig av hvem som definerer risikonivået, hva det defineres ut fra og hvem risikonivået vurderes for. Man kan gjerne si at det er mer akseptabelt med et høyt risikonivå innen rallycross enn det er innen vanlig biltrafikk. Hvordan denne defineringen av risikoakseptkriterier foregår i sammenheng med etterretningstrusselen mot petroleumsnæringen vil bli drøftet i kapittel 6.

3.3 Sikkerhet vs. sikring

Akademisk vil man gjerne skille de to feltene sikkerhet (safety) og sikring (security) på en av to måter: Den ene måten handler om intensjon, der man vil si at sikkerhet handler om farer og ulykker som kan oppstå uten at intensjonen er å skape denne situasjonen. Sikring derimot; handler om menneskeinitierte ondsinnede handlinger, og intensjon om å påføre en form for risiko eller skade. Den andre måten å skille dem omhandler hvem som skal beskyttes i risikohåndteringen; der sikkerhet beskytter menneskene/miljøet mot systemet, og sikring beskytter systemet mot mennesker/miljøet (Bieder & Pettersen Gould, 2020).

Som vi ser, er det uansett definisjon og tilnærming to ganske forskjellige innfallsvinkler til risiko. Og til tider kan de ulike feltene til og med komme i konflikt med hverandre, der et sikkerhetstiltak undergraver et sikringsbehov eller omvendt. Fra et sikkerhetsperspektiv vil man gjerne ha så mange rømningsveier som mulig, mens man fra et sikringsperspektiv vil ha så få potensielle entringspunkt som mulig. Men de to feltene kan også ha synergier på tvers av fagfeltene, der et sikringstiltak positivt påvirker sikkerhet og omvendt.

Nancy Leveson (2020) argumenterer for at man må se sikkerhet og sikring sammen i et systemperspektiv, hvor man i større grad fokuserer på sluttresultatet av sikkerhets- eller sikringsbruddet. Dersom vi skal trykke hennes modell på statlig etterretning mot petroleumsnæringen; vil det være viktig å legge inn mekanismer som kan håndtere et sikringsbrudd, eksempelvis der informasjon om undersjøisk infrastruktur har kommet på avveie. Hvor hensiktsmessig dette er; vil gjerne variere mellom virksomheter og objekter som beskyttes. Det vil også være lettere å gjøre slike tiltak mot en fysisk trussel enn mot en etterretningstrussel som kan fremstå på flere måter, både ved menneskelig og teknisk tilnærming. Det vil også være lettere å finne synergier mellom sikring mot sabotasje og påvirkningsoperasjoner som et resultat av tidligere etterretning, enn mot etterretningen selv.

Synergiene kan være større eller mindre, men dersom man har begge aspektene med i utarbeidelsen av tiltak og oppbygging av systemer/infrastruktur, er det iallfall ikke *mindre* sannsynlig å klare å utnytte disse på en god måte. Dersom en sikringstrussel kan påvirke sikkerhetsfeltet; vil man ofte finne at det vil være et system for å ivareta eventuelle sikkerhetskonsekvenser av hendelsen. I så måte har man mekanismer på plass for å kontrollere *konsekvensen*, og på samme måte gjerne tiltak for å forhindre at den utløsende sikringshendelsen skal oppstå. Dette ser man gjerne spesielt tydelig innen IKT.

Sikkerhets-, og kanskje spesielt sikringsarbeid, har også i stadig større grad fått et systemisk preg; der digitalisering og internasjonalisering påvirker hvordan man må tilnærme seg trusler og farer (Bieder & Pettersen Gould, 2020). Det er i dag mulig for en person med internettilgang i Moskva å hacke seg inn på en oljerigg i Nordsjøen og gjøre driftsmessige påvirkningsoperasjoner; som kan påvirke ikke bare sikrings-, men også sikkerhetsbildet.

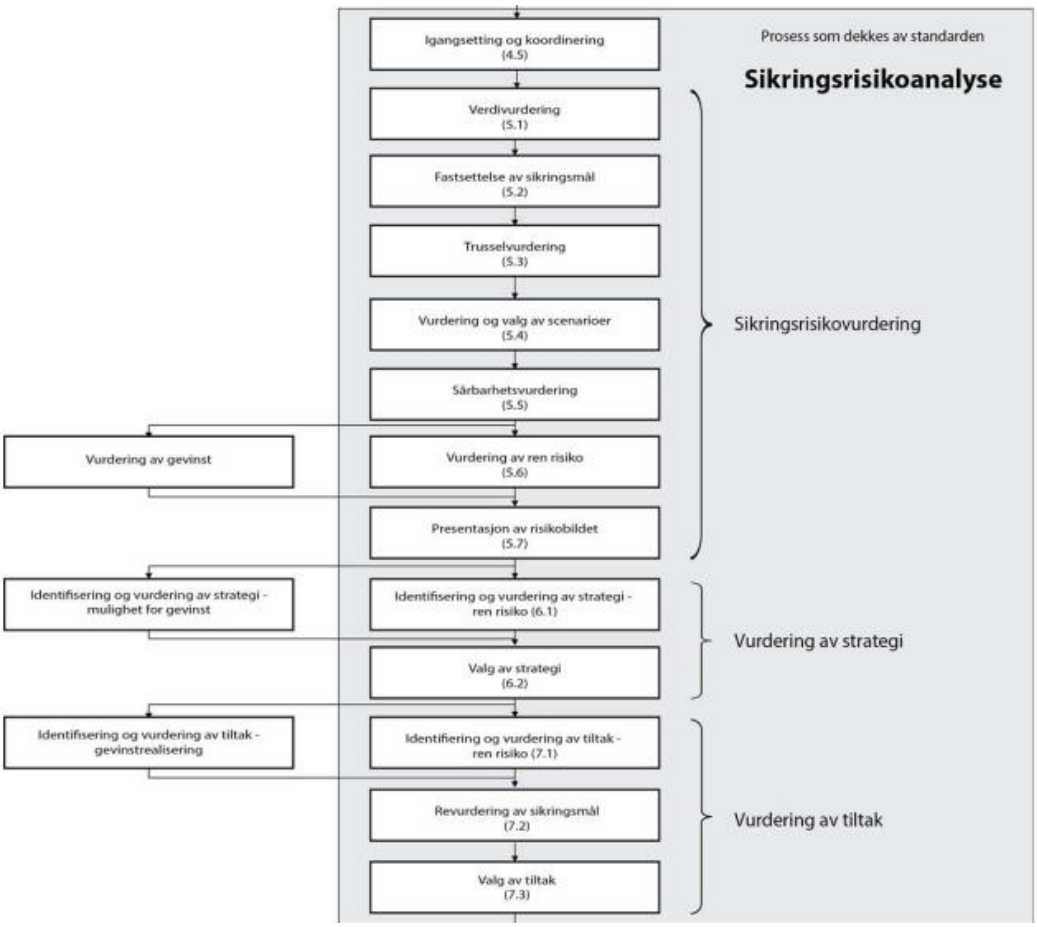
Der sikkerhet etter hvert er et relativt innarbeidet tankemønster gjennom HMS-kulturen som blant annet har blitt løftet frem i petroleumsnæringen, er det fremdeles mer naturlig å omtale sikringsfeltet som et nisjefelt for spesielt engasjerte mennesker. Selv om det i IT-bransjen gjerne er en mer integrert del av hvordan man til enhver tid tenker, er det gjerne ikke like stor del av den daglige tankegangen til andre deler av virksomhetene.

Sikkerhetsarbeid har et bedre utgangspunkt enn sikringsarbeid, og oftest vil de som er omfattet av et sikkerhetsregime i lettere kunne knytte en hendelse direkte til en konkret konsekvens enn ved en sikringstrussel. Sikkerhetsarbeid har også den fordelen at så lenge man gjøre det lettere å gjøre rett enn å gjøre feil; vil man umiddelbart redusere sannsynligheten for at en sikkerhetshendelse oppstår, ettersom det normalt ikke ligger en intensjon om å forårsake et sikkerhetsbrudd. Sikringsfeltet er mer abstrakt, og det kan være vanskeligere for personell omfattet av et sikringsregime å se sammenhengen mellom deres sikringsbrudd og en potensiell hendelse. Denne problemstillingen vil være særlig relevant dersom man snakker om et statlig etterretningsbilde og nasjonal sikkerhet, hvor trusselen ikke nødvendigvis rammer egen virksomhet direkte.

3.4 Sikring/security

Statlig etterretning tilhører, sammen med andre tilsiktede uønskede handlinger, sikringsfeltet. Sikring skiller seg fra sikkerhet blant annet ved at aktøren har en intensjon om å gjennomføre den uønskede handlingen, og mulighet til å tilpasse seg mottiltak. Sikringsfeltet inneholder også i enda større grad enn sikkerhetsfeltet subjektive vurderinger, da i form av både verdier og trusler. Ulike aktører kan ha ulik definisjon av begge disse faktorene, og uten lov- eller normfestede krav vil vurderingene kunne avvike stort fra hverandre.

Innenfor sikringsfaget vil man måtte forholde seg til en form for analyse av trusselbildet. En *sikringsrisikoanalyse* utført i henhold til NS 5832:2014 vil, dersom korrekt gjennomført, gjøres i henhold til modellen i figur 6. Kapittelet her vil spesielt trekke frem den første delen som er *sikringsrisikovurderingen*, ettersom den vil legge grunnlaget for alle senere vurderinger som blir gjort gjennom analysen.



Figur 6 Prosessen for sikringsrisikoanalyse og sikringsrisikostyring (Standard Norge, 2014)

Som utgangspunkt defineres verdiene som skal beskyttes i en *verdivurdering*. En verdi er definert som «[en] ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen» (Standard Norge, 2012, s. 4). En slik ressurs kan være infrastruktur, informasjon eller andre gjenstander eller konsepter som anses som verdifulle. Størrelsen på verdien er subjektiv og relativ til den som gjør vurderingen. Dersom nasjonale og internasjonale sikkerhetsinteresser ikke er definert som en verdi, vil det ikke bli hensyntatt videre når man setter sikringsmål. De fleste bedrifter som driver med teknologiutvikling i et konkurransemarked; vil likevel ha en

interesse av å sikre egne data mot konkurrenter, og i så måte vil man kunne ha overlapp i interessefelt med det sikkerhetspolitiske aspektet på enkelte områder.

Etter at verdivurderingen er gjennomført skal man fastsette *sikringsmål*. Sikringsmålene skal beskrive hva som er akseptabel tilstand på de definerte verdiene under og etter en hendelse (Standard Norge, 2014). For et angrep på en petroleumsinstallasjon kan man eksempelvis si at det alltid skal være strøm til å sikre brannvannspumper og annet nødutstyr, mens man for informasjon kan sette krav til at enkelte informasjonstyper ikke skal komme på avveie.

Neste vurdering er en *trusselvurdering,* hvor man vurderer selve trusselbildet. NS 5830 definerer trussel som «mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet» (Standard Norge, 2012, s. 4). Trusselbegrepet deles deretter inn i *potensiell* trussel og *reell* trussel. Disse skilles ved at en potensiell trussel forbindes med «en mulig intensjon […] eller kapasitet […] til å true en annen entitets sikkerhet» (Standard Norge, 2012, s. 4), mens en reell trussel forbindes med «en kjent intensjon […] og kapasitet […] til å true en annen entitets sikkerhet» (Standard Norge, 2012, s. 4). Vi ser at potensiell trussel kan bli brukt om mange entiteter, mens man for å definere noe som en reell trussel må kunne påvise både intensjon og kapasitet. Intensjon og kapasitet er gjerne også omtalt som *vilje* og *evne*.

I en trusselvurdering vil man vurdere trusselaktørens *evne* og *vilje* til å gjennomføre en definert uønsket handling. Evne/kapasitet innebærer trusselaktørens tilgjengelige «ressurser, kunnskap og ferdighet, til å utføre en handling» (Standard Norge, 2012, s. 5). Begrepet *vilje* inneholder gjerne ønske om å gjennomføre handlingen, sammen med forventning om et gitt resultat (Clifton & Brooks, 2013). Trusselvurderingen utføres som utgangspunkt med all tilgjengelig relevant informasjon, og det vil derfor være kritisk for en presis trusselvurdering at man har tilgang på så mye relevant informasjon som mulig. Dersom deler av situasjonsbildet er gradert eller på annen måte gjort utilgjengelig for den som utfører vurderingen, vil man kunne etablere et feil trusselbilde. Som tidligere nevnt er verdivurderingen som gjøres premissgivende for resten av sikringsrisikoanalysen. Dersom man legger til grunn feil verdier vil dette kunne lede til at feil trusselaktører defineres, og dermed en feilvurdering av evne og vilje til å gjennomføre en uønsket handling.

Gjennom trusselvurderingen har man avdekket trusler som er relevante og aktuelle. Dersom vi skal se dette opp mot statlig etterretning; har man i de statlige trusselvurderingene definert blant annet Russland og Kina som trusselaktører (PST, 2020), ettersom man ser at disse har både vilje og evne til å gjennomføre etterretningsaktivitet mot norsk petroleumssektor. Når verdi og trussel er definert; utarbeides det *scenarioer* for å kartlegge eventuelle fremgangsmåter som en trusselaktør kan benytte (Standard Norge, 2014).

Basert på verdi- og trusselvurdering gjøres det en *sårbarhetsvurdering*, hvor man avdekker hvilke sårbarheter som eksisterer overfor truslene i scenariene som er utarbeidet. I sårbarhetsvurderingen skal det vurderes om innførte barrierer og sikringstiltak vil være tilstrekkelig for å håndtere scenariene (Standard Norge, 2014). Disse sårbarhetene kan ofte reduseres eller fjernes helt, men i enkelte tilfeller er gjerne sårbarheten en viktig kvalitet med objektet, og dermed ikke hensiktsmessig å endre. Et eksempel på en slik sårbarhet kan være verdien åpenhet eller kostnadseffektiv drift. Her vil en reduksjon i sårbarhet kunne redusere verdien åpenhet eller kostnadseffektiv drift, og dermed vil man kunne få en interessekonflikt. Dette kan føre til at man bør vurdere å endre verdien på objektet, eksempelvis ved å akseptere et lavere nivå av kostnadseffektiv drift. I tilfellet statlig etterretning mot petroleumssektoren; vil det gjerne være hensiktsmessig å sette inn tiltak for å redusere sårbarheten på bekostning av kostnadseffektivitet.

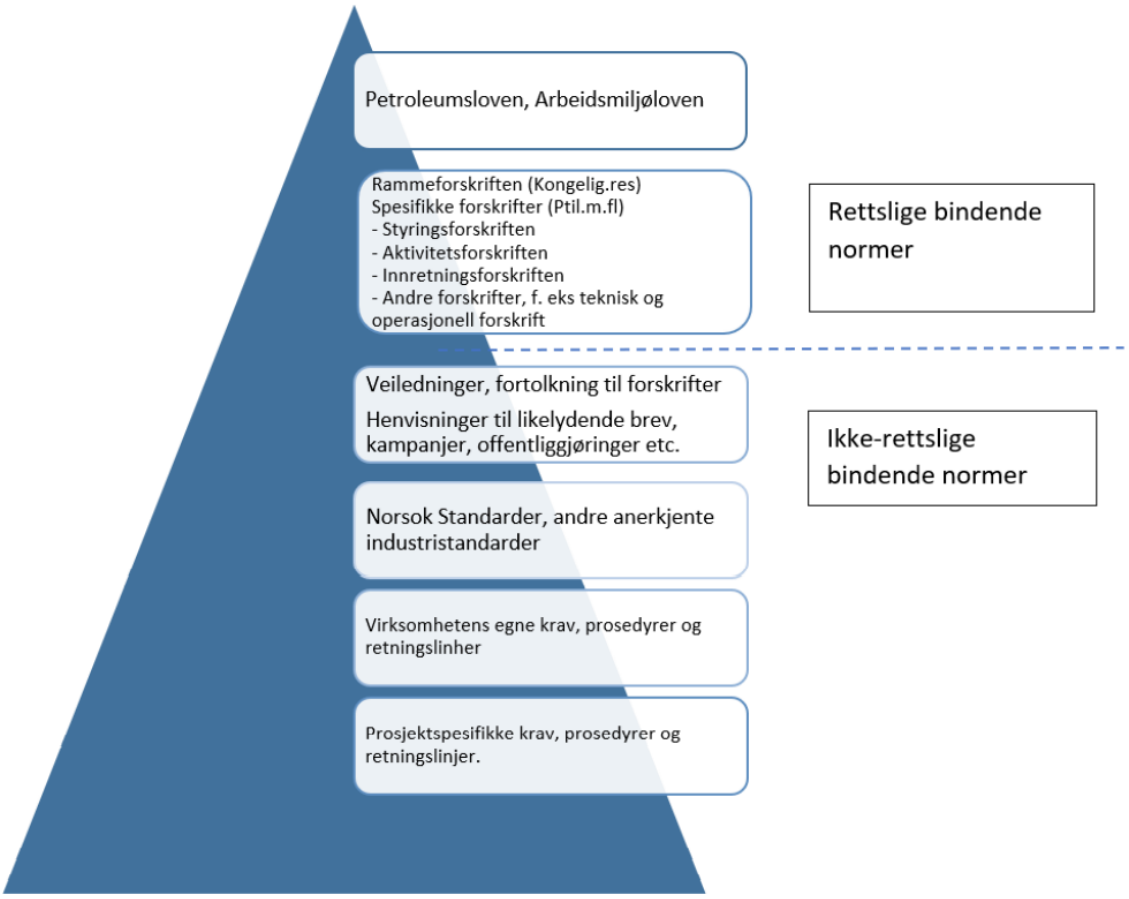
Etter at verdi, trussel og sårbarhet er vurdert; gjøres en ren risikovurdering for hvert av scenariene. Denne risikovurderingen skal fremstilles kvalitativt, med beskrivelse av de enkelte punktene og konklusjonen. Her er det viktig at man også beskriver usikkerheten i de enkelte delvurderingene og konklusjonen. Som tidligere nevnt i 3.1 ser vi at usikkerhet er en essensiell bestanddel i en sikringsrisikoanalyse, og det er derfor viktig å gi beslutningstakere en reell beskrivelse av denne usikkerheten.

3.5 Petroleumsloven

I forbindelse med statlig etterretning som trussel mot petroleumssektoren, er petroleumsloven som sektorspesifikk lov; og sikkerhetsloven som domenespesifikk lov, særlig aktuelle. Dette kapittelet vil omhandle petroleumsloven, og sikkerhetsloven vil bli utdypet i oppgavens 3.6.

Petroleumsloven er laget for å regulere petroleumsnæringen og petroleumsutvinning i Norge, og har sitt hovedvirkeområde for «[…] petroleumsvirksomhet knyttet til undersjøiske petroleumsforekomster underlagt norsk jurisdiksjon.» (Petroleumsloven (§1-4), 2003). Loven ivaretar alle aspekter av petroleumsutvinning, herunder tillatelser, økonomiske forhold, ansvarsforhold, med mer.

Petroleumsloven legger opp til et såkalt funksjonelt regime (Abrahamsen et al., 2020). Dette innebærer at lovgiver gir føringer for målsetning og tilnærming, men lar næringen selv velge fremgangsmåte. Dette gjøres gjennom rettslig- og ikke-rettslig bindende normer, eksemplifisert ved henholdsvis forskrifter for lovgiver og standarder for næringen. Som vist i figur 7; er det et hierarki hvor loven gir utgangspunkt for mer detaljerte forskrifter, herunder rammeforskriften, styringsforskriften, aktivitetsforskriften m.fl. Loven pålegger å følge beste praksis for de ulike delene av reguleringen, noe som gjør at ulike ikke-rettslig bindende normer i enkelte tilfeller kan veie tilnærmet like tungt som rettslig bindende normer.



Figur 7 Normhierarkiet for petroleumsloven (Abrahamsen et al., 2020)

Loven med forskrifter omsettes i praksis ved at PTIL og næringen selv etablerer lovtolkninger og veiledere; som gir utgangspunkt for standarder som NORSOK og andre. Med utgangspunkt i disse standardene utledes det virksomhetsinterne prosedyrer og regelverk. Ettersom veiledere, prosedyrer og regelverk ikke er rettslig bindende, er de til en viss grad frivillige å følge. Som tidligere nevnt er det likevel en sterk forventning i lovverket om å følge disse ikke-rettslig bindende normene, og PTIL vil kunne gi pålegg dersom næringen/virksomheter avviker stort fra veiledere.

En utfordring og fordel med et funksjonsbasert regelverk som petroleumsloven; er at det gir et stort handlingsrom for næringen, men med dette handlingsrommet følger også usikkerhet om forventninger (Abrahamsen et al., 2020). Denne usikkerheten vil vi se at blir aktualisert når vi nå skal se på petroleumslovens forhold til sikring.

Lovens kapittel 9 omfatter «Særskilte krav til sikkerhet» (Petroleumsloven (§9-1), 2003). Kapittelet omhandler hovedsakelig det man normalt vil omtale som sikkerhet, foruten § 9-3 *Beredskap mot bevisste anslag* som sier at «Rettighetshaver skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag mot innretninger samt til enhver tid ha beredskapsplaner for slike anslag.» (Petroleumsloven (§9-3), 2003). Lovens ordlyd tilsier at også denne delen primært tar sikte på *sikkerhets*konsekvensen av en sikringshendelse. En rettighetshaver kan med god grunn hevde at statlig etterretning ikke faller inn under rettighetshavers ansvar dersom det ikke kommer ytterligere føringer fra myndighetene.

Ettersom rettighetshaver (operatør) naturlig vil basere seg på petroleumslovens føringer i sin utøvelse av både egne sikringstiltak, og hvordan de utøver påseplikten, kan øvrige sikringstrusler som ikke defineres som «bevisste *anslag*» være avhengig av næringens egenopplevde behov for tiltak. Denne fortolkningen kan ytterligere forsterkes ved å studere de ulike forskriftene som eksempelvis *Rammeforskriften*, *Styringsforskriften*, *Aktivitetsforskriften,* og så videre.

Går man derimot inn i forarbeidene til petroleumsloven vil man finne at «bevisste anslag» eksemplifiseres som å «[…] kunne være terroraksjoner, sabotasje og ulike former for krigslignende handlinger» (Ot.prp.nr.46 (2002–2003), 2003). Denne ordlyden tillater en videre tolkning enn den gjengitt i lovens § 9-3, og vil kunne omfatte statlig etterretningsvirksomhet under «krigslignende handlinger» dersom lovgiver ønsker å

etablere dette som et fokusområde. Dersom man ser på sabotasje; vil dette ofte innebære en kartlegging av svakheter i forkant, og dermed vil etterretning være en naturlig trussel å ta hensyn til. Her er det tidligere nevnte handlingsrommet, og usikkerheten det medfører, en viktig faktor i utøvelsen av paragrafen. PTIL har mulighet til å definere denne forståelsen i en veileder, men det forutsetter at PTIL anser dette aspektet som vesentlig nok.

3.6 Lov om nasjonal sikkerhet (sikkerhetsloven)

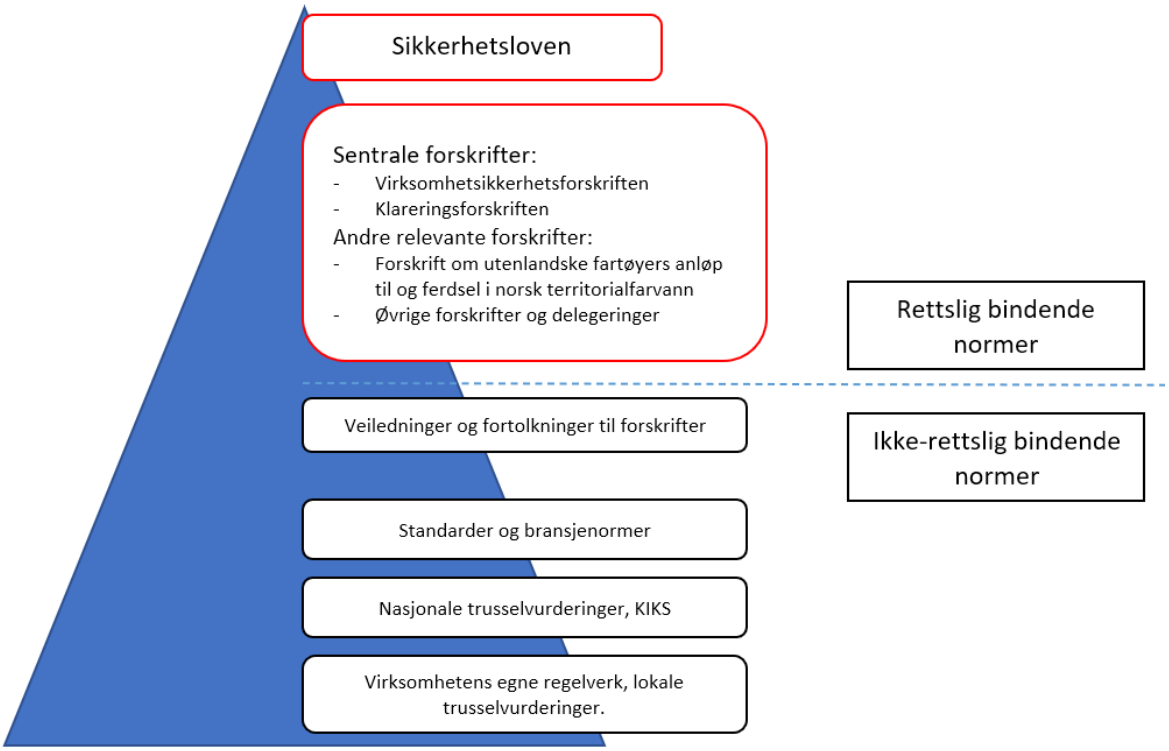
For å ivareta sikkerhetsarbeidet opp mot trusler mot nasjonale interesser; har det lenge vært etablert en lov som skal sikre et hjemmelsgrunnlag for å kunne gjennomføre tiltak som sikkerhetsklarering og skjerming av informasjon. Den siste utgaven av sikkerhetsloven trådte i kraft i 2019; og erstatter den gamle sikkerhetsloven av 2001. Den nye sikkerhetsloven er mer funksjonelt rettet enn forgjengeren, og inneholder mindre detaljerte krav til virkemidler. På samme måte som petroleumsloven; gir den nye sikkerhetsloven et større handlingsrom til å selv definere beste måte for å oppnå kravene i loven. Sikkerhetsloven skal styrke det nasjonale sikkerhetsarbeidet ved å «[…] forebygge, avdekke og motvirke sikkerhetstruende hendelser» (NSM, 2019, s. 2). Dette gjøres på samme måte som petroleumsloven ved å oppgi et ønsket resultat, og åpne for at det kan være flere måter å oppnå dette resultatet på.

Loven er underlagt Justis- og beredskapsdepartementet, og er som utgangspunkt fulgt opp av NSM i det daglige, men også gjennom delegert tilsynsmyndighet. Like fullt er det opp til ulike sektorielle ansvarshavere, i form av departementene, å definere hvem som skal være omfattet av loven basert på gitte kriterier med tolkningsrom. Denne delegeringen av definisjonsmyndighet til forskjellige aktører med tilhørende tolkningsrom gir rom for ulik praksis, som vi vil se senere i kapittelet. Nasjonal sikkerhetsmyndighet (NSM) har utgitt et stort antall veiledere til sikkerhetsloven (NSM, 2022b), disse veilederne gir en ytterligere detaljering av forskriftene, og bidrar blant annet med håndbøker for gjennomføring av de ulike aspektene av forskriftene.

Som illustrert i figur 8, har sikkerhetsloven noen sentrale forskrifter representert ved virksomhetsikkerhetsforskriften og klareringsforskriften (NSM, 2020). Virksomhetsikkerhetsforskriften har en detaljering av krav til sikkerhetsstyring, og kan i så måte minne om petroleumslovens styringsforskrift, bortsett fra at sikkerhetsloven utelukkende omhandler sikring. Klareringsforskriften har på samme måte en detaljering av

krav innen personellklarering, og definerer blant annet klareringsmyndighet. Grovt sett deles klareringsmyndigheten mellom Forsvaret ved Forsvarets sikkerhetsadministrasjon (FSA) som klarerer forsvarssektoren, og Sivil klareringsmyndighet som klarerer nødvendig personell i sivil sektor. Det som er nytt i den gjeldende sikkerhetsloven er adgangsklarering som virkemiddel (Sikkerhetsloven (§8-3), 2018). Denne klareringen er det laveste nivået på klarereringshierarkiet, og innebærer at man blir klarert for adgang spesifikt for det objektet man skal arbeide på eller ha adgang til (NSM, 2022a).

En annen forskrift som er verdt å nevne spesielt i denne oppgaven er *forskrift om utenlandske fartøyers anløp til og ferdsel i norsk territorialfarvann* (Forskrift om utenlandske fartøyers anløp til og ferdsel i norsk territorialfarvann, 2019). Denne forskriften angir restriksjoner for utenlandske fartøyers aktiviteter i norsk territorialfarvann, herunder kartleggingsfartøyer, forskningsfartøyer og andre fartøy med spesialkapasiteter. Forskriftens § 7 regulerer ulike typer utenlandske fartøys adgang til norsk indre farvann, mens § 15 begrenser retten til å gjennomføre målinger og registreringer med mindre det er nødvendig for sikker navigering (Forskrift om utenlandske fartøyers anløp til og ferdsel i norsk territorialfarvann, 2019).



Figur 8 Normhierarkiet for sikkerhetsloven

Sikkerhetsloven har som formål:

a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser
b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet
c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. (Sikkerhetsloven (§1-1), 2018)

Lovens § 1-2 sier videre at den gjelder for «statlige, fylkeskommunale og kommunale organer» og «leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser» (Sikkerhetsloven (§1-1), 2018). I så måte kan den tolkes som at den ikke er gjeldende for virksomheter som ikke driver direkte med handel dekket av sikkerhetslovens kapittel 9 *Sikkerhetsgraderte anskaffelser*. Det kan være hensiktsmessig å presisere at loven er gjeldende for statlige, fylkeskommunale og kommunale organer uavhengig av om de er omfattet av kapittel 9. Dette innebærer at organer som OD og PTIL som utgangspunkt er dekket av sikkerhetsloven. Loven kan også i henhold til § 1-3 gjøres helt eller delvis gjeldende for virksomheter som:

a) behandler sikkerhetsgradert informasjon
b) råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner
c) driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner. (Sikkerhetsloven (§1-3), 2018)

Det kan argumenteres for at petroleumssektoren faller inn under alle tre av disse benevnelsene, og da spesielt punkt b og c. Det er likevel ikke en automatikk i at en virksomhet som faller under definisjonen i §1-3 skal omfattes av loven. Det er opp til departementet som har virksomheten i sitt ansvarsområde å avgjøre hvorvidt, og i hvilket omfang, den skal gjøres gjeldende for virksomheten. Dette etter at departementet har definert en del av sin sektor som en grunnleggende nasjonal funksjon.

Dersom ansvarlig departement ikke på eget initiativ kommer til konklusjonen at et område skal omfattes av sikkerhetsloven; kan sikkerhetsmyndigheten fremme forslag, og eventuelt bringe saken inn for departementet med ansvar for forebyggende sikkerhetsarbeid i aktuell sektor. I vårt tilfelle vil det være Olje- og Energidepartementet som har sektoransvar for petroleumsnæringen, og Justis- og beredskapsdepartementet som har det overordnede ansvaret i sivil sektor. Innenriks forsyning av drivstoff er underlagt Nærings- og

fiskeridepartementet (NFD), og i så måte kan også NFD ha sektoransvar for deler av petroleumsvirksomheten. Men ettersom leverandørindustrien i praksis er en tverrsektoriell bransje som også gjør arbeid på fiberkabler og annen undersjøisk infrastruktur kan det også være andre departementer som har sektoransvar for områder leverandørindustrien jobber innen.

En deling av sektoransvar kan lede til uklare ansvarsforhold og fragmentering av ansvar. Man kan risikere at elementer av ansvarsområdet faller mellom to stoler dersom det oppstår usikkerhet om ansvarlig etat. Det kan også bidra til en beslutningsvegring, der man ser til den andre sektorens vurderinger og ikke selvstendig vurderer trusselbildet for eget ansvarsområde.

3.7 Oppsummering

Dette kapittelet har vist hvordan risikobegrepet, og hvilken definisjon av risiko man velger å benytte, er grunnleggende for hvilket resultat man får av en risikovurdering. Vi ser at risiko, spesielt i en sikringssammenheng, er uløselig knyttet til begrepet *usikkerhet.* PTIL anerkjenner at usikkerhet er viktig også innen sikkerhetssegmentet, og har tatt det inn i sin definisjon av risiko. Samtidig inneholder NS 5830:2012 «Samfunnssikkerhet Beskyttelse mot tilsiktede uønskede handlinger Terminologi» ikke begrepet usikkerhet i sin definisjon av risiko for sikringsrisikoanalyser. Videre ser vi at hvordan man forholder seg til risiko og usikkerhet kan ha store konsekvenser for hvilke risikoer man aksepterer i form av risikoakseptkriterier, og dermed også hvilke risikoreduserende tiltak man innfører.

Vi ser også at sikkerhet og sikring har overlappende sfærer, hvor tiltak innen sikring kan hindre hendelser innen sikkerhet, og motsatt; at tiltak innen sikkerhet kan begrense skadevirkningen av enkelte sikringshendelser. Samtidig er det mulig at sikrings- og sikkerhetsfeltet kan motarbeide hverandre. Videre ser vi at sikring er et felt med ulik verdisetting, trusselvurdering og sårbarhetsvurdering basert på hvem som gjennomfører vurderingene. Dette kan ha stor betydning for hvordan man forholder seg til statlig etterretning som trussel mot petroleumssektoren.

Når det kommer til lovverket ser vi at petroleumsloven, og reguleringsregimet for petroleumsnæringen, legger opp til stor grad av selvstendighet i bransjen for hvordan man skal oppnå kriteriene satt i loven. Når det kommer til sikring i petroleumsloven, har dette feltet én paragraf med lite detaljering. Vi ser likevel at lovens forarbeider kan tolkes strengere og mer omfattende enn det lovens § 9.3 gir uttrykk for.

Sikkerhetsloven er en omfangsrik lov, og vil medføre stor endring dersom den innføres i sin helhet for et område. Den har tydelige krav om omfattende restriksjoner og kontrolltiltak for eventuelle virksomheter som blir underlagt den. Restriksjoner som per nå kanskje ikke er realistiske dersom man skulle innført loven over natten. Det vil dermed kreve et stort arbeid å detaljere hvordan sikkerhetsloven i så fall skal gjelde for petroleumssektoren.

4 Metode

Forfatteren av denne oppgaven jobber selv i leverandørindustrien, og har et stort nettverk innen petroleumssektoren generelt, og leverandørindustrien spesielt. Dette kan medføre noen utfordringer i forskningsarbeidet. Gjennom informantbehandling og forskning har det vært viktig å se næringen fra utsiden. En utfordring ved å forske i egen kultur er man kan gå glipp av informasjon ettersom informanten tar det for gitt at forskeren har kunnskap om emnet, og at man dermed ikke trenger å sette ord på det (Wadel, 2016).

I kvalitativ forskning i egen kultur kan det være utfordrende å skille sine egne erfaringer fra det som kommer frem fra informanter og litteratur (Halvorsen, 2008). Dette har vært viktig å ha i bevisstheten mens oppgaven har blitt skrevet.

4.1 Valg av metode

For å kunne vurdere hvordan statlig etterretning som trussel ivaretas i petroleumssektoren generelt, og leverandørindustrien spesielt, er det valgt en kvalitativ blandingsstudie. Dette har blitt gjort ved en litteraturstudie av tilgjengelig eksisterende forskning og analyser på området. Hvordan rammevilkårene praktiseres er undersøkt gjennom litteraturstudie, semistrukturerte intervjuer og samtaler med informanter som representerer forskjellige deler av næringen.

Intervjuene og informanters bidrag har blitt brukt til å nyansere funnene som er gjort i litteraturstudien.

4.2 Valg av informanter

Informantene er valgt på bakgrunn av deres stilling og funksjon i virksomhetene som er representert i studien. De er valgt delvis ved utpeking fra den representerte organisasjonen, og delvis ved henvisninger fra andre informanter. I tillegg til dybdeintervju med enkeltinformanter; er det også gjennomført flere uformelle samtaler med ulike aktører innen petroleumssektoren for å bygge forståelse for sammenhenger. Men det har også vært tilfeller der informanten ikke har ønsket eller hatt mulighet til å stille til formelt intervju, men har ønsket å bidra til forskningen. Enkelte forespurte informanter har også gitt tilbakemelding på at de ikke har fått lov av arbeidsgiver å stille til intervju, noe som kan være forståelig gitt oppgavens tema, men som likevel har vanskeliggjort datatilgangen.

Informantene består av et utvalg av representanter for petroleumsnæringen, herunder leverandørindustrien, for å danne et bilde av hvordan virksomhetene forholder seg til statlig etterretningsvirksomhet som trussel, og hvordan lover og regulering påvirker dem. For å belyse myndighetenes forventninger og holdninger er det gjennomført et intervju med PTIL. PST er intervjuet for å få en forståelse av trusselbildet. NSM avslo intervju med bakgrunn i stor arbeidsbelastning som følge av Ukrainakrigen som startet undervis i oppgaveskrivingen.

4.3 Valg av litteratur

Litteratursøk er gjort gjennom bruk av nøkkelord i Google, Google Scholar og Oria. I tillegg til faglitteratur benyttet underveis i masterprogrammet. For å kartlegge de ulike reguleringsregimene er lovverk som petroleumsloven og sikkerhetsloven med tilhørende forskrifter undersøkt. Gjennom intervjuene og bakgrunnssamtalene er det også kommet tips om relevant litteratur for oppgavens tema. Disse tipsene har gjerne handlet om standarder, forskrifter, tidligere forskning, med mer.

4.4 Gjennomføring av intervjuer

Intervjuene er gjennomført som et semistrukturert intervju med åpne spørsmål som utgangspunkt for en dialog rundt sikringsrisiko relatert til et nasjonalt trusselbilde, og er rettet mot de ulike grupperingene av informanter (se vedlagt intervjuguide). De fleste intervjuene og samtalene er gjennomført fysisk, men flere av samtalene er gjennomført på telefon.

Det har vært høye forventninger om anonymisering og diskresjon fra informantene, og det er derfor ikke alle som har ønsket at intervjuet har blitt tatt opp på bånd.

4.5 Studiens begrensinger

Det er som følge av temaets sensitive natur begrensinger på hvilken informasjon som er tilgjengelig. Denne oppgaven er basert utelukkende på åpne kilder, og anerkjenner at det kan finnes sikkerhetsgradert informasjon som kan endre deler av bildet.

5 Empiri

Dette kapittelet besvarer problemstillingen «*På hvilken måte er den økende trusselen fra utenlandsk statlig etterretning ivaretatt gjennom lovverk og reguleringsregimet for petroleumssektoren?* (side 8). For å gjøre dette vil det være nødvendig å vise til hvordan statlig styring legger premisser for næringens handlingsrom, og hvordan næringen forholder seg til lovverket. Kapittelet vil også besvare forskningsspørsmålene (se side 8).

Dette innebærer for det første å analysere hvilke muligheter som finnes i eksisterende lover og forskrifter. Det mest aktuelle lovverket, petroleumsloven og sikkerhetsloven, er tidligere presentert i oppgavens teoridel; gjennom henholdsvis delkapittel 3.5 og 3.6. Her ser vi at det er rom i lov og forskrift til å innføre strenge sikringstiltak for petroleumssektoren dersom det er ønskelig fra myndighetenes side. Både petroleumsloven og sikkerhetsloven har hjemler som enten gjennom forskrift eller tolkning kan benyttes mot en fremmedstatlig etterretningstrussel, på lik linje med det som i dag er ansett som skjermingsverdig informasjon og objekter.

For det andre er det nødvendig å se på hvordan sektoren er bygget opp, og hvilke eventuelle sårbarheter både myndighetenes struktur og næringen har. Kapittel 2 har beskrevet hvordan sektoren er bygget opp, med ulike beslutningstakere og overlappende ansvar mellom ulike departementer. I 5.1 beskrives petroleumssektorens myndigheters tilnærming til sikringstrusler; i form av uønskede handlinger fra en statlig aktør. Men også hvilket handlingsrom som finnes dersom myndighetene ønsker det.

For det tredje er det nødvendig å se på statlig etterretning som fenomen, og de geopolitiske interessene som kan ligge til grunn for at petroleumssektoren er utsatt for dette trusselbildet. Dette blant annet i form av, på nåværende tidspunkt, å være nest største leverandør av gass til EU gjennom både undersjøiske eksportrør og ved hjelp av LNG-skip. I kapittel 5.2 vil vi se at leverandørindustrien innehar teknologi og kapasiteter som gjør at både menneskelig innhenting (HUMINT), innhenting fra åpne kilder (OSINT) og data om geografiske forhold (GEOINT) fra disse aktørene; vil kunne være interessant for en statlig etterretningsaktør. For det fjerde vil kapittel 5.3 drøfte hvordan næringen selv anerkjenner og forholder seg til lovverk og reguleringer, samt etterretningstrusselen generelt sett. Og til

slutt gå nærmere inn på hvordan leverandørindustrien praktiserer lovverk og regulering i sin tilnærming til statlig etterretning.

Dette kapittelet vil sammen med kapittel 3 legge grunnlaget for oppgavens drøftingsdel. I kapittel 6 vil det drøftes hvordan sektorens oppbygging og styring legger føringer for den praktiske utøvelsen av sikringsfaget når det kommer til statlig etterretningstrussel. Herunder hvordan næringen forholder seg til risikoen gjennom risikoakseptkriterier. Det vil også drøftes hvorvidt det er mulig å gjøre noe med sårbarhetene som presenteres i dette kapittelet.

5.1 Hvordan er strukturer og lovverk i stand til å motvirke statlig etterretning som trussel mot petroleumssektoren?

Som nevnt i 2.1.1 ble ansvaret for å ivareta petroleumslovens § 9-3 i 2013 overført fra OED ved OD til AID med PTIL som utøvende part. I den sammenheng kan det være interessant å se på PTILs tildelingsbrev for å si noe om hvordan det prioriteres fra AID. I tildelingsbrevet for 2022 forekommer ikke ordet sikring i det hele tatt. Det er gitt referanser til uønskede hendelser og reduksjon av risiko, men da alltid i en sikkerhetskontekst. Den eneste henvisningen til feltet sikring er et avsluttet fireårig prosjekt rettet mot IKT-sikkerhet (Arbeids- og inkluderingsdepartementet, 2022; Petroleumstilsynet, 2022a). Dette prosjektet har produsert seks rapporter fra SINTEF og DNV-GL som omhandler forskjellige aspekter ved IKT-sikkerhet. Fokuset i prosjektet fremstår i hovedsak å være driftssikkerhet og forhindring av skadelig programvare. Det er enkelte delkapitler som fremhever etterretning i form av COMINT; som eksempelvis:

> «Trusselbildet for bruk av teletjenester i petroleumssektoren er dynamisk og vil endre seg over tid. Det er viktig at enkeltpersoner er bevisste og opplært i å håndtere og rapportere det de mener er unormal oppførsel i systemer og tjenester. Bedriftene må ha tilstrekkelig beredskap og kunnskap til å håndtere slike meldinger.» (DNV-GL, 2020, s. 37).

Riksrevisjonen publiserte i 2019 en rapport med flere funn angående ODs sikring av egne IKT-systemer mot dataangrep, og lister følgende to funn med kritikknivå «Sterkt kritikkverdig»:

> Oljedirektoratets vurdering av IKT-systemer, med påfølgende risikovurdering og sikkerhetsplanlegging, er ikke kommet langt nok, og IKT-systemene har svakheter som uvedkommende kan utnytte.
>
> Oljedirektoratet feilinformerer om sikkerhetstilstanden i sin rapportering om IKT-sikkerhet til Olje- og energidepartementet. (Riksrevisjonen, 2018)

Denne revisjonen kommer to år etter at Riksrevisjonen i 2016 også fant det sterkt kritikkverdig at OD ikke hadde tilfredsstillende styringssystem for informasjonssikkerhet. Dette på tross av at OD som statlig forvaltningsorgan var og er underlagt sikkerhetsloven. Som konsekvens av 2016-rapporten krevde kontroll- og konstitusjonskomiteen i innstilling at OED umiddelbart gjorde tiltak for å utbedre manglene (Riksrevisjonen, 2018). Selv om både 2016- og 2018-rapporten var kjent for OED i 2019; er det ikke ført til endringer i tildelingsbrevene til OD før 2020 (Olje- og energidepartementet, 2019, 2020). Dette kan ha sammenheng med kritikknivået til Riksrevisjonen. «Sterkt kritikkverdig» har følgende kriterier: «[…] angir forhold som har mindre alvorlige konsekvenser, men gjelder saker med prinsipiell eller stor betydning.». Mens kritikknivå *Alvorlig* «[…] benyttes ved forhold som kan ha betydelige konsekvenser for samfunnet eller berørte borgere, eller der summen av feil og mangler er så stor at dette må anses som alvorlig i seg selv.» (Riksrevisjonen, 2022).

Man kan se likheter mellom Riksrevisjonens kritikknivåer og sikkerhetslovens klassifisering av skjermingsverdig materiale. Riksrevisjonen fremhever selv at OD er «et utsatt mål for informasjonsoperasjoner fra andre lands myndigheter og profesjonelle aktører.» (Riksrevisjonen, 2018). Når OD selv prioriterer sikringsaspektet så lavt, er det interessant å se det i sammenheng med sektormyndighetens valg om å ikke gjøre sikkerhetsloven gjeldende for virksomheter i petroleumssektoren, da spesielt ettersom OD er en hovedaktør i dette arbeidet.

PTIL oppgir selv i intervju at sikringsavdelingen hovedsakelig jobber mot fysisk sikring, og at IKT-sikkerhet blir håndtert av en annen avdeling (internt i PTIL). PTIL er likevel en så liten organisasjon at det er et tett samarbeid mellom disse. I årsrapporten for 2021 oppgir PTIL at de har hatt sikringstilsyn og at «Tilsynsaktivitetane har omfatta fysisk sikring, personelltryggleik og informasjonstryggleik. Blant anna har vi gjennomført ein tilsynsserie med sikring i heile logistikk-kjeda, som blir avslutta i 2022.» (Petroleumstilsynet, 2021, s. 39).

Videre fremkommer det av den samme årsrapporten at PTIL i 2020 og 2021 har gjennomført en møteserie med operatørselskapene, hvor de har orientert seg om operatørenes tilnærming til, og håndtering av sikringsrisiko (Petroleumstilsynet, 2021).

Dette tilsynet med hele logistikk-kjeden kan ses i sammenheng med standarden Norog 091 og sikringsavtalen benyttet av Norsk olje og gass, som har som formål å «hindre uautorisert materiell eller personell i å nå petroleumsinnretninger offshore via forsyningskjeden (herunder; leverandør, transportkjede, forsyningsbase, havneområder, fartøy og innretninger)» (Norsk olje og gass, 2019, s. 4). Denne sikringsavtalen forhindrer altså i utgangspunktet ikke uautorisert personell å få tilgang på informasjon. Og den har heller ikke som målsetting å forhindre tilgang på materiell som ikke har til umiddelbar hensikt å sendes offshore.

På spørsmål til PTIL om de har mulighet til, og i så fall har vurdert, å utforme forskrift basert på § 9-3 i petroleumsloven, svarer de at de ikke har vurdert det. Samtidig opplyser de at det har vært en dialog med næringen om det er hensiktsmessig å inkorporere sikring som en del av det allerede eksisterende regelverket. Dette ville i så fall kunne løfte sikring som et fokusområde på samme måte som HMS og arbeidsmiljølovverk, selvsagt basert på hvor og hvordan det blir plassert inn.

Det ble i 2021 sendt på høring et forslag til innstramming av sikkerhetsloven angående eierskapskontroll med mer, med svarfrist januar 2022. Her foreslås det blant annet å stramme inn hvem som faller inn under sikkerhetsloven. Denne endringen vil være betydelig fra den tidligere definisjonen, og vil under sikkerhetslovens § 1-3 legge til nytt andre ledd som lyder «Et departement kan innenfor sitt ansvarsområde fatte vedtak om at kapittel 10 [eierskapskontroll] skal gjelde for virksomheter av vesentlig betydning for grunnleggende nasjonale funksjoner» (Justis- og beredskapsdepartementet, 2021, s. 17). Denne endringen fra *avgjørende* til *vesentlig* betydning; innebærer en betydelig utvidelse av omfang. I tillegg er det foreslått flere andre endringer for å bedre sikkerhetsmyndighetenes kontroll på virksomheter og eiendommer av betydning for nasjonal sikkerhet. Sett i sammenheng med at OED i Prop. 1 S (2021-2022) har identifisert «[…] kontroll med utvinning av petroleum på norsk sokkel» (Olje- og energidepartementet, 2021, s. 133) som en grunnleggende nasjonal funksjon, vil det kunne medføre at store deler av petroleumsnæringen kan eller bør

underlegges sikkerhetsloven helt eller delvis. NOROG stiller seg i sitt høringssvar ikke prinsipielt imot de foreslåtte endringene i sikkerhetsloven, men ser ikke noen gevinst i å underlegge virksomheter i petroleumsnæringen sikkerhetsloven. NOROG løfter også en bekymring om økt administrativ byrde og kostnadsøkning, og hevder videre at det vil være overlappende lovverk med petroleumsforskriftens § 10.

NSM stiller seg, i motsetning til NOROG og flere andre, sterkt positive til en slik endring i sikkerhetsloven, og etterlyser attpåtil en ytterligere innstramming som vist i det etterfølgende sitatet.

> «NSM mener dette forslaget ikke går langt nok, og anbefaler at samtlige leverandører i sikkerhetsgraderte anskaffelser omfattes av meldeplikten etter sikkerhetsloven §10-1, også når leverandøren får tilgang til skjermingsverdig objekt eller infrastruktur eller informasjon gradert BEGRENSET. Også disse leverandørene vil ha kjennskap til skjermingsverdige verdier som det er behov for å kontrollere hvem som får tilgang til. Leverandørene kan også ha flere oppdragsgivere slik at summen av den informasjon de besitter kan være betydelig selv om de ikke er leverandørklarert.» (Furuseth, 2022, s. 2)

Sett opp mot hvordan leverandørindustrien jobber i petroleumssektoren er dette særlig interessant, ettersom dette forslaget vil utvide innslagspunktet for hvem som skal underlegges sikkerhetsloven ytterligere i forhold til det som er foreslått i høringsnotatet. Dermed vil det kunne omfatte både operatører og underleverandører til disse der leverandører har tilgang til skjermingsverdige informasjon, objekter eller infrastruktur.

Petroleumsforskriften har i § 10 fjerde ledd en henvisning til nasjonal sikkerhet, men da med ordlyden «Departementet kan av hensyn til nasjonal sikkerhet nekte adgang til og utøvelse av petroleumsvirksomhet hvis søkeren eller rettighetshaveren faktisk kontrolleres av en stat utenfor EØS eller av statsborgere fra slik stat.» (petroleumsforskriften (§10), 1997). Denne ordlyden er i utgangspunktet ganske romslig. Med kapittelets øvrige fokus på utvinningstillatelser kan den likevel tolkes til kun å gjelde utvinningstillatelser, og ikke nødvendigvis en så omfattende tolkning av petroleumsvirksomhet som ordlyden i utgangspunktet kan gi rom for.

Klareringsforskriften, som er hjemlet i sikkerhetsloven, gir departementet anledning til å vedta adgangsklarering eller utvidet adgangsklarering som vist i følgende sitat:

> Hvert departement kan innenfor sitt ansvarsområde fatte vedtak om krav til adgangsklarering der et objekt eller en infrastruktur kan være et mål for ikke-statlig terror, attentat eller annen alvorlig kriminalitet. Kan objektet eller infrastrukturen være mål for statlig sabotasje eller andre tilsiktede anslag fra en annen stat, kan departementet fatte vedtak om krav til utvidet adgangsklarering. (Klareringsforskriften (§15), 2019)

Vi ser her at adgangsklarering er tilgjengelig selv om objektet i utgangspunktet ikke oppfyller de øvrige kriteriene i sikkerhetsloven. Dette er ytterligere presisert i veilederen til klareringsforskriften, med ordlyden «Det avgjørende for hvilken type adgangsklarering som bør innføres er hvilken trussel objektet eller infrastruktur er mål for, og ikke objektet eller infrastrukturens klassifiseringsgrad.» (Nasjonal sikkerhetsmyndighet, 2019, s. 55).

5.2 Hva gjør petroleumssektoren til et attraktivt etterretningsmål?

Det er en kjensgjerning at stater driver etterretning mot hverandre, både venner og fiender ønsker å vite mest mulig om flest mulig for å kunne posisjonere seg i mellomstatlige forhold. Slik etterretning kan ha ulike mål, og russisk etterretning kan forventes å være rettet både mot sårbarheter og militærstrategiske mål, mens man fra amerikansk side kanskje kan forvente en mer diplomatisk orientert etterretning. På samme måte vil sivile virksomheter ofte forsøke å vite mest mulig om konkurrentenes planer og teknologi. Dette ønsket om å skaffe til veie informasjon kan handle om alt fra uskyldig innsamling av offentlig informasjon, til å begå lovbrudd ved å gjøre innbrudd i konkurrentens IKT-systemer eller lokaler (ikke-statlig etterretning). Statlig etterretning skiller seg fra ikke-statlig etterretning hovedsakelig ved evne og vilje til å gjennomføre uønskede handlinger, da i form av tilgjengelige ressurser og tidsperspektiv.

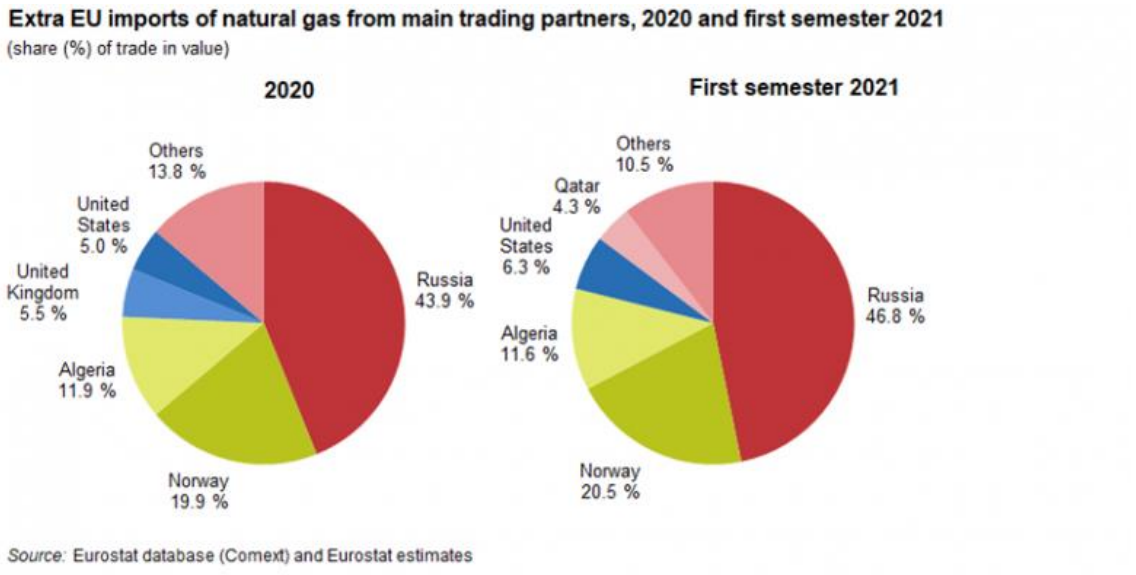
PST (2020) fremholder at blant annet informasjon om petroleumsteknologi, både i form av vanlig industrispionasje, men også med tanke på flerbruksområder innen militære formål, vil være av interesse for statlige aktører. I tillegg fremheves det at norske myndigheters holdninger til eksempelvis OPEC-avtaler, konsesjonsrunder og tildelinger vil være interessant. Hovedaktørene i Norge oppgis å være Russland og Kina (PST, 2020).

I nasjonal trusselvurdering for 2022 skriver PST at «[…] personer i Norge [vil] bli forsøkt rekruttert som kilder av andre lands etterretningstjenester. Andre stater vil ta i bruk stadig mer kompliserte selskapsstrukturer og utvise stor kreativitet for å anskaffe sensitiv teknologi fra norske virksomheter.» (PST, 2022a, s. 6). I en pressemelding etter Russlands invasjon av Ukraina sier PST at en allerede høy etterretningstrussel fra Russland nå er ansett for å være ytterligere økt.

> Olje og gass har sikkerhetspolitisk verdi for Russland, i tillegg til den rent økonomiske. Som en viktig konkurrent til Russland som olje- og gassleverandør, kan Norge både styrke Europa og svekke Russland gjennom kjøp og salg av olje og gass. Det øker etterretningstrusselen. (PST, 2022b)

Der en ikke-statlig virksomhet oftest har interesser som er styrt av relativt kortsiktige økonomiske interesser, har statlige aktører gjerne et lengre tidsperspektiv. Russlands militærdoktrine legger vekt på blandede (hybride) virkemidler for å oppnå strategiske mål (Zysk, 2018). Og dermed vil man kunne si at en eventuell økonomisk vinning fremstår som en bonus; opp mot hovedhensikten som er å innhente data av både sivil og militær strategisk verdi. En del av strategien kan også være oppkjøp eller posisjonering for å tilegne seg informasjon, eventuelt styrke egen nasjonal industri på området (PST, 2022a).

Denne datainnhentingen kan bidra til kjennskap om norske myndigheters beslutningsgrunnlag, skape splid i befolkningen i form av desinformasjonskampanjer (PST,



Figur 9 Oversikt over gassleveranser til EU (Eurostat, 2021)

2022a), eller gi kjennskap til mål for fysiske sabotasjeaksjoner for å presse myndighetene til å handle etter trusselaktørens vilje.

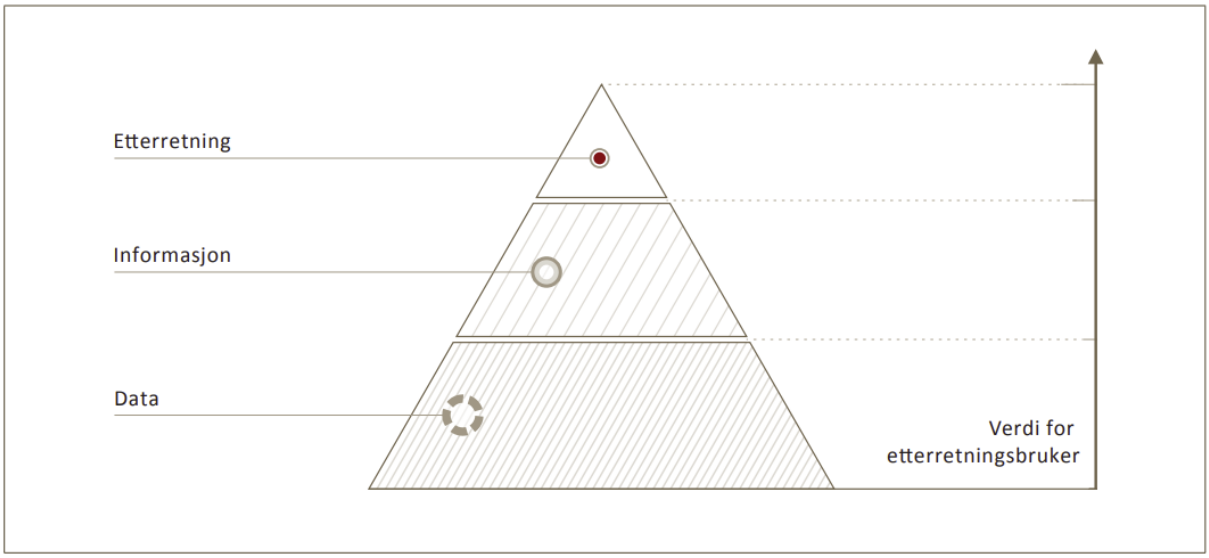
Som det vises i figur 9; står Norge for en betydelig andel av gassleveransen til EU (≈20%) i 2020-2021, og etter Russlands invasjon av Ukraina våren 2022 vil Norges andel av denne leveransen kunne øke ytterligere som følge av EUs ønske om å gjøre seg uavhengig av russisk gass (European comission, 2022). Dermed kan statlige trusselaktører ha interesse av å vite så mye som mulig om infrastrukturen som både produserer og leverer denne gassen. I den tidligere nevnte pressemeldingen fra PST skriver de også at «Alle personer og virksomheter med informasjon eller innflytelse av verdi for Russland må regne med å være mer utsatt enn før for russiske etterretningsaktiviteter.» (PST, 2022b).

Sammenlignet med en privat organisasjon; har en statlig etterretningsaktør i fredstid både tiden og ressursene på sin side. Der de fleste land har en dedikert etterretningsenhet med rendyrket kompetanse, og både menneskelig og økonomisk kapasitet til å stå i en operasjon over flere år, har gjerne private virksomheter mer kortsiktige målsetninger grunnet stadige endringer i markedet og teknologisk utvikling. Med referanse til PSTs tidligere nevnte antagelse om at personer vil bli forsøkt vervet; er det i tråd med etterretningspraksis å rekruttere informanter og agenter på et tidlig tidspunkt i karriereløpet, for deretter å følge dem gjennom karrieren som gjerne kan vare i 30-40 år. PST kan også fortelle at fremmedstatlig etterretning gjerne setter bort jobben med å infiltrere organisasjoner til private selskaper. Samtidig kan statlig etterretning gjerne deles med eget lands virksomheter, for å gi dem en markedsfordel, eller teknologisk drahjelp.

5.2.1 Petroleumsnæringen

Figur 10 viser hvordan forholdet mellom datainnsamling og etterretning kan fremstilles. Som vi ser, trengs det betydelige mengder data for å kunne filtrere det ned til brukbar etterretning. Leverandørbedrifter med drift- og inspeksjonsansvar på ulike anlegg har tilgang til disse objektene for å kunne utføre jobben sin, en tilgang som kan misbrukes til å samle inn data. I forbindelse med utvinning og transport av petroleumsprodukter innhenter petroleumsnæringen store mengder høyoppløselig kartdata over havbunnen. Denne dataen kan være interessant for utenlandsk etterretning i forbindelse med kartlegging av rør- og kabeltraseer, undervannsinstallasjoner, og undervannstopografi. Utenlandske fartøyer med

spesialkapasiteter på slik kartlegging kan vinne kontrakter på norsk sektor, hvor disse fartøyene i enkelte tilfeller kan dublere som etterretningsfartøy for utenlandsk etterretning.



Figur 10 Sammenhengen mellom data, informasjon og etterretning (Etterretningstjenesten, 2021b)

Kartleggingsvirksomhet er regulert i *Forskrift om utenlandske fartøyers anløp til og ferdsel i norsk territorialfarvann* (2019) med formål å unngå at utenlandske fartøyer ukontrollert skal kunne drive med slik innhenting; kalt geografisk innhenting (GEOINT) i etterretningsdomenet. Men dersom fartøyet er kontrahert til et norsk selskap har det lov å gjøre kartlegging på vegne av dette selskapet. Det er noe usikkerhet rundt hvem som fører tilsyn med denne virksomheten, ettersom PTIL selv opplyser i intervju at de ikke gjør det.

I 2003 leide det norske selskapet TGS-NOPEC inn flere russiske skip; blant dem Akademik Nemchinov, Akademik Shatskiy og Akademik Lazarev for å gjøre kartlegging av havbunnen i Norge (TGS-NOPEC, 2002). Skipene i Akademik-klassen har jevnlige jobber på norsk sektor, og de siste årene har de hatt jobber for blant andre Geoex MCG og ION Geophysical på norsk sokkel (ROSGEO, 2021a, 2021b). Ståle Ulriksen ved Sjøkrigsskolen har omtalt de russiske skipene av Akademik- og Mekhanik-klassen som «spionskip» (Kibar, 2021), med bakgrunn i skipenes tilknytning til den russiske staten. Han er også sitert på følgende uttalelse:

> Skipene i både Akademik- og Mekhanik-klassen opererer som forskningsskip for den russiske staten. Det er sivile forskningsskip som blir brukt til militære formål. […] De driver med klassisk kartlegging av sårbare punkter og industrispionasje, […]. (Kibar, 2021)

Sett i sammenheng med Etterretningstjenestens bekymringer om at Russiske Glavnoje Upravlenije Glubokovodnykh Issledovanija (Hoveddirektoratet for dypvannsforskning, GUGI) tilhørende det russiske forsvarsministeriet har et undervannsrekognoseringsprogram; som NATO ser i forbindelse med russisk utvikling av offensive undervannskapasiteter (Etterretningstjenesten, 2021a), kan man gjerne se noen koblinger som er uheldige. Etterretningstjenesten sier sågar at «Russlands økende satsing på undervannskapasiteter er i ferd med å bli en alvorlig trussel mot undersjøiske kabler og undervannssystemer.» (Etterretningstjenesten, 2021a, s. 64).

På spørsmål til informantene fra næringen vedrørende vurderinger av kontraktører relatert til bindinger mot statlige aktører; sier enkelte at det ikke oppleves at det er kapasitet til å gjøre slike vurderinger i en anbudsprosess. Dette kan medføre at statlige aktører kan benytte seg av helt åpne anbudsprosesser for å underby andre aktører, og dermed sikre seg helt lovlig tilgang til data man fra et myndighetsperspektiv gjerne ikke ønsker å dele. PTIL velger heller ikke å tillegge disse prosessene noe vekt, da det ikke anses som en del av trusselbildet. Enkelte av informantene forteller at de sjekker underleverandørene sine nøye der disse er i inngrep med deres egen teknologiutvikling.

Petroleumsnæringen, og kanskje spesielt leverandørindustrien, er opptatt av å vise seg frem på messer og i offentlighet. Både for å vise seg for potensielle kunder og myndigheter, men også for å ha åpenhet for befolkningen som en del av mediestrategien. Sammen med profilering på internett, gir denne store mengden åpent tilgjengelig informasjon gode muligheter for at en etterretningsaktør med stort hell kan gjøre nytte av innhenting fra åpne kilder (OSINT). Informantene anser likevel denne problemstillingen som ivaretatt av ordinære industritiltak for å beskytte egen virksomhet.

Etterretningstjenesten, NSM og PST gir alle ut jevnlige trusselvurderinger i form av en gradert, og en ugradert versjon. En utfordring med å kommunisere et trusselbilde til næringen; er at sikkerhetsmyndighetene som utgangspunkt ikke kan dele gradert informasjon dersom mottakeren ikke er sikkerhetsklarert. Ettersom sikkerhetsklarering i utgangspunktet fordrer arbeid mot skjermingsverdige objekter, og det ikke er definert skjermingsverdige objekter i sektoren, vil det heller ikke være naturlig å sikkerhetsklarere personell (FFI, 2016).

PST opplyser om at det er adgang til å autorisere personer opp til *Begrenset* uten sikkerhetsklarering, men at det da gjøres med et begrenset antall personer for en bestemt informasjonspakke. Man kan tenke seg at PST innehar informasjon om en trussel som er spesielt relevant for en definert gruppe virksomheter, og dermed autoriserer personell som kan trenge informasjon om denne trusselen for å fatte en informert beslutning om risikoreduserende tiltak. Det er uklart i intervjuet med PST hvilken paragraf som gir anledning til dette, men det antas at det er sikkerhetslovens § 8-1 som gir denne adgangen; selv om det ikke er åpenbart fra ordlyden i loven at det er mulighet til dette. Loven sier at «Personer som skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, må ha gyldig sikkerhetsklarering.» (Sikkerhetsloven (§8-1), 2018).

Informantene er delte i synet på hvorvidt en sikkerhetsklarering av sikringspersonellet i virksomhetene ville vært hensiktsmessig. Noen mener det ville vært et godt tiltak slik at de kan få bedre tilgang på kontekst i trusselbildet. Ettersom sikkerhetstjenestene allerede nå nedgraderer informasjonen til dem, mener andre at det ikke vil medføre vesentlige fordeler. Av grunner for dette nevnes blant annet at beslutningstakere i virksomheten også måtte blitt sikkerhetsklarert for å kunne få den samme informasjonen som beslutningsgrunnlag.

Alternativet til å dele gradert informasjon med beslutningstakere, er at disse har tillit til at den sikringsansvarlige har pålitelig informasjon *og* har vurdert verdien av tiltak rett. I en virksomhet som har til hensikt å maksimere fortjeneste; kan man fort komme i interessekonflikt når man ikke har et fullstendig bilde som beslutningsgrunnlag. Tillit kan fremstilles som det som dekker gapet mellom det man vet og fullstendig kunnskap om et emne. Når man ikke vet hvor stort dette gapet er, blir det vanskeligere å brolegge det med tillit der man gjerne opplever press fra flere interesser. Like fullt informerer PTIL i intervju at de opplever operatørselskapene som å «være sitt ansvar bevisst», og at de følger opp trusselbildet samvittighetsfullt der det er relevant for dem.

Som en konsekvens av krigen i Ukraina har Equinor, Lundin, Forskningsrådet og Sintef Digital besluttet å bruke 20 millioner kroner på å ruste opp den digitale sikkerheten mot ondsinnede handlinger (Kibar, 2022). Dette vil mest sannsynlig også bidra til å beskytte sensitive data mot etterretningsvirksomhet, men det fordrer at man anser denne informasjonen som sensitiv. Dersom opprustingen starter én måned etter at krigen startet;

er det også sannsynlig at store mengder sensitive data allerede er kompromittert. Både gjennom flere års innhenting, men også ved mer aktiv innhenting siden krigen startet.

Samtidig som bransjen erkjenner en sårbarhet for digitale trusler; jobber enkelte bedrifter for å drive deler av virksomheten sin fra utenlandske kontorer i lavkostland. Halliburton har blant annet vurdert å drive et kontrollsenter for offshoreoperasjoner fra Dubai. (Helgesen, 2022). Dette kan være tjenester som er i direkte inngrep i den daglige driften offshore på norsk sokkel, og en slik utflagging vil kunne tilføre sårbarheter heller enn å redusere dem. Det å operere fra utlandet fratar for det første kontroll over hvem som har tilgang på datatrafikken, men også en eventuell sikkerhetsklarering av personell involvert i driften vil bli vanskeligere, om i det hele tatt mulig. Dersom petroleumssektoren hadde helt eller delvis vært underlagt sikkerhetsloven ville muligens denne driftsmodellen ikke vært tillatt.

5.3 Hvordan forholder petroleumsnæringen seg til statlig etterretning som nasjonal trussel?

Leverandørbedriftene er i stor grad avhengig av kontrakter med operatørselskaper som Equinor, Aker BP og Vår Energi. De store kontraktene roterer gjerne mellom de største aktørene; i en bransje som er syklisk og presset på marginer. Dette gjør at leverandørbedriftene baserer seg på innleiepersonell for å ta en del av variasjonen i arbeidsmengde, og i større eller mindre grad også baserer seg på utenlandsk personell for å holde kostnaden nede der det er mulig. Denne store utskiftingen av personell og den kostnadsfokuserte driftsmodellen, presenterer en sårbarhet som kan utnyttes av aktører med onde hensikter, enten det er statlige eller ikke-statlige. Dette sammenfattet med at leverandørene supplerer personell til både drift og inspeksjon av landanleggene som er sentrale i produksjon og distribusjon av olje og gass, presenterer en ytterligere sårbarhet med tanke på datainnhenting som nevnt i 5.2.

Bransjeorganisasjonen Norsk olje og gass (NOROG) har utgitt en veileder (091) for sine medlemsbedrifter; som omhandler «sikring av forsyninger og materiell i Olje- og gassindustrien» (Norsk olje og gass, 2019). Denne veilederen gjenspeiler fokuset i petroleumslovens § 9-3 ved å utelukkende omtale fysisk sikring av logistikken ut til offshoreinstallasjoner, der den kontrollerte kjeden starter allerede hos leverandøren. Den

gir, gjennom en signert avtale, mulighet for å bli en godkjent direkteleverandør til offshore-installasjoner.

I likhet med fokuset i petroleumsloven er det heller ingen bransjeveiledere fra NOROG som omhandler etterretnings- eller sabotasjedomenet utover det digitale domenet. Blant informantene fra næringen er det blandede synspunkter på hvilken nytte 091 har. De fremholder alle at den har en effekt for logistikk og kontroll på transportkjeden for å hindre uautorisert materiell og personell fra å komme ut på offshoreinstallasjonene. Denne effekten kan likevel sies å hovedsakelig være en administrativ fordel for å redusere behov for omlastinger, og i mindre grad ivareta et trusselbilde; så lenge man har denne sikringen ved siste omlastingssted.

Det eksisterer en NOROG-veileder for informasjonssikkerhet, denne fokuserer hovedsakelig på IKT-*sikkerhet* og omstendighetene ved mulig driftsavbrudd eller tekniske komplikasjoner, men også sikringsaspektet som generelt er tilstedeværende i IKT-sammenheng (Norsk olje og gass, 2016). Begge de omtalte veilederne er underlagt fagsjef «HMS og standardisering»; ettersom NOROG ikke har en dedikert sikrings-avdeling eller person. De har dog et sikringsforum, bestående av representanter fra medlemsbedriftene. Det er verdt å merke seg at NOROG er en bransje- og medlemsorganisasjon, og dermed ikke har instruerende myndighet ovenfor sine medlemmer. Det vil også være begrenset med ressurser til å utvikle egne standarder og veiledninger utover det som gjøres av, og i samråd med, PTIL. Et annet aspekt er at det er et fåtall av leverandørbedriftene som er tilknyttet NOROG, og dermed vil eventuelle standarder utarbeidet for og av NOROG ha begrenset virkning utover medlemsbedriftene, med mindre det kreves av kunde.

IKT-sikkerhet er en vesentlig faktor for å hindre sabotasje som har til hensikt å skape driftsavbrudd. Det vil likevel ikke hindre kartlegging av sårbarheter; med mindre det finnes systemisk kontroll på hvilken informasjon som er sensitiv. Hvilken informasjon som anses som sensitiv vil være opp til de ulike virksomhetene så lenge dette ikke defineres i lovverket. På spørsmål om informantene fra næringen forholder seg til det statlige trusselbildet, svarer informantene at de som utgangspunkt ikke tar hensyn til etterretning som trussel dersom det ikke vil ramme virksomheten selv, og at de heller ikke har ressurser til å avdekke etterretning som foregår i et strategisk langtidsperspektiv. Dette handler både om

kost/nytte-vurderinger, og behov for å skape forståelse i organisasjonen for at slik etterretning foregår.

Flere informanter påpeker at innsidetrussel som fenomen har fått økt oppmerksomhet de siste årene, dog ikke nødvendigvis med et statlig trusselbilde som hovedårsak. PTIL har blant annet gjennomført et prosjekt med en prosjektrapport som adresserer innsidetrussel (Jerre & Funnemark, 2019). Rapporten beskriver innsidetrussel både fra private og statlige aktører. Den nevner blant annet sårbarheten ved å sette ut funksjoner som IKT til land som India, grunnet utfordringer med å utføre en tilstrekkelig bakgrunnssjekk (Jerre & Funnemark, 2019). Rapporten beskriver også utfordringen med å forankre en sikringsholdning blant de ansatte, som vist i sitatet «Enkelte kan lett ha den oppfatningen at «Vi har ikke informasjon som noen er interessert i.»» (Jerre & Funnemark, 2019, s. 64).

Informantene sier at den pågående krigen i Ukraina har, ikke overraskende, gjort at statlige aktører har blitt mer synliggjort som trussel. Det er likevel vanskelig å gardere seg mot slike aktører uten at det i stor grad går ut over den daglige driften. På spørsmål om sikkerhetsloven kunne hjulpet den sikringsansvarlige med å bedre kunne forebygge trusselen fra statlige aktører; svarer flere informanter bekreftende. Det er likevel ikke et uttrykt ønske om å underlegges deler av sikkerhetsloven; ettersom det vil kunne gi utilsiktede administrative og økonomiske konsekvenser. Informantene uttrykker at en tydeliggjøring i petroleumsloven med tanke på hvilke trusler man skal forebygge mot kanskje er nok.

5.4 Oppsummering

Oppsummert viser empirien oss at petroleumssektoren er kompleks, med flere departementer som ivaretar deler av samme overordnede sektor. OED har ansvaret for forvaltningen av petroleumsnæringen, med særlig trykk på å skape størst mulig verdier gjennom å gjøre informasjon og data fra petroleumsvirksomheten tilgjengelig. OED har også sektoransvar, og dermed ansvaret for å avgjøre om det finnes skjermingsverdige objekter innen sektoren; som vil gjøre at disse objektene da underlegges sikkerhetsloven. På den andre siden har AID ansvaret for å forvalte arbeidsmiljø, beredskap og sikkerhet på norsk sokkel. Denne forvaltningen gjøres gjennom tildelingsbrev til PTIL, som også har tilsynsmyndighet for sikring i petroleumssektoren. Vi ser også at NFD har ansvaret for petroleumsforedlingen og tilhørende infrastruktur.

Samtidig ser vi at leverandørindustrien; som man gjerne anser som en næringsspesifikk bransje, er en variert bransje som gjør arbeid innen flere sektorer. Bransjen består av høyteknologisk utstyr som gir mulighet for både geografisk etterretning (GEOINT), åpen innhenting (OSINT) og kommunikasjonsinnhenting (COMINT) for en kapabel aktør. Der det eksisterer myndighetskrav til IKT-sikkerhet er disse fulgt opp av PTIL. Tilsynsvirksomheten til PTIL gjøres dog mot operatørene, og eventuelle sårbarheter i sikringsarbeidet som følge av operatørens driftsmodell vil dermed kanskje ikke avdekkes. Det er sterke kommersielle interesser i spill i hele sektoren. Og PTIL som har tilsynsmyndigheten for petroleumssektoren; har sitt hovedfokus mot sikkerhet, arbeidsmiljø og forurensning, som selvsagt er viktige tema i denne bransjen.

Vi ser at etterretningstrusselen mot Norge har vært høy over tid, og at denne er blitt enda høyere etter Russlands invasjon av Ukraina. Denne etterretningen retter seg mot både politiske og militærstrategiske mål. Norge som en av to hovedleverandører av gass til EU har både nasjonale og transnasjonale interesser som kan bli skadelidende av den informasjonen en fiendtlig etterretningsaktør samler inn.

6 Drøfting

Som vist i kapittel 2 «Petroleumssektoren» er sektoren omfattende, med en sektoroverskridende næring. OED har som utgangspunkt ansvaret for sektoren, mens NFD har ansvaret for infrastrukturen til distribusjon av petroleumsprodukter. Tilsynsmyndighet for sektoren er ikke administrert under OED, men heller AID gjennom PTIL. PTIL kan gjerne omtales som Arbeidstilsynet for sektoren, og har sitt hovedfokus på petroleumsloven med forskrifter. Herunder hovedsakelig på hvordan operatører etterlever de strenge sikkerhetsforventningene som er til petroleumsbransjen.

PTIL hadde sin opprinnelse i OD, og ble i 2004 skilt ut til eget tilsyn, men da uten tilsynsansvar for sikring i henhold til § 9-3. Da de i 2013 overtok også dette ansvaret ble det avdekket mangler ved sikringsarbeidet. Det bemerkes likevel fra PTIL at de har sett en stor fremgang i virksomhetenes kompetanse og fokus på sikring siden 2013. Det kan fremstå som OD ikke har hatt et særlig fokus på sikringstrussel som en problemstilling mens de har hatt ansvaret for dette emnet, noe som også gjenspeiles i Riksrevisjonens rapporter om ODs sikring av egen organisasjon (Riksrevisjonen, 2018). Petroleumsloven fikk denne paragrafen som dekker sikringsaspektet først i 2003, og man kan gjerne se den i sammenheng med terroranslaget mot New York 11. september 2001. Den tidligere forskningen som er gjort på området gjenspeiler også dette fokuset på terror som den bærende sikringstrusselen mot petroleumssektoren. Dette er forståelig, ettersom terror er en skremmende trussel som gis stor oppmerksomhet i mediebildet. Samtidig er det viktig at myndighetene og bransjen selv erkjenner at det er en kontinuerlig etterretningstrussel fra aktører som har mulighet til å ta tiden til hjelp, og som hele tiden samler inn data for å bygge opp til nyttig etterretning som vist i figur 10.

Ordlyden «Rettighetshaver skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag mot innretninger samt til enhver tid ha beredskapsplaner for slike anslag.» (Petroleumsloven (§9-3), 2003) indikerer at paragrafen hovedsakelig retter seg mot terrorsikring, eventuelt andre fysiske trusler mot petroleumsinstallasjoner, og det er lite i paragrafen selv som indikerer at den skal ivareta etterretning som en trussel. Man omtaler normalt ikke etterretningstrusselen som et anslag ettersom tidsaspektet er usikkert, en

etterretningshendelse kan forløpe over kort eller lang tid. Ved en digital inntrengningshendelse som et cyberangrep vil man gjerne lettere kunne definere det som et anslag; ettersom det, i utgangspunktet, er en mer akutt hendelse med en mer definert start og slutt. Dermed er det lettere å konkretisere tiltak mot cyberhendelser; i form av IKT-sikkerhet og øvelser på å stanse inntrengingsforsøk.

PTIL har i 2013 fått ansvaret for tilsyn etter petroleumslovens § 9-3, og selv om det fremstår som noe usikkert hvor høyt sikring prioriteres i PTILs tildelingsbrev og organisasjonen generelt; er det ingen grunn til å tvile på at de som jobber med sikring i PTIL jobber kompetent og samvittighetsfullt med sikring i tråd med de føringene som gis fra oppdragsgiver. Når denne oppgaven finner at statlig etterretning ikke er prioritert nok som trussel, er det basert på flere funn der tunge aktører som NSM og PST omtaler trusselen som høy og økende, mens det er usikkerhet om tiltakene som gjøres fullt ut klarer å ivareta denne økningen. Når man med relativt enkle midler kan finne at leverandørselskaper som TGS-NOPEC leier inn det som betraktes som russiske spionskip til å kartlegge havbunnen på norsk sektor, fremstår det usikkert om industrien tar trusselen på alvor når det kan medføre til tider store kostnadsøkninger. På samme måte viser Halliburtons ønske om å flytte kontrollfunksjoner for offshoreaktivitet til lavkostland; at bedriftsøkonomiske vurderinger utfordrer de sikringsfaglige vurderingene, og kanskje spesielt når det kommer til en statlig etterretningstrussel. Denne utflaggingen av tjenester vil bli ytterligere drøftet i 6.4.2.

En bekymring som kommer frem fra ulike aktører; er at et for komplisert regelverk vil kunne føre til at en etterlevelse av sikringsregelverket vil medføre økt administrasjon, som vil gjøre at virksomhetene vil få utfordringer med å drive på en kosteffektiv måte. Norsk olje og gass (NOROG) har i sitt høringssvar på den omtalte endringen i sikkerhetslovens kapittel om eierskapskontroll; fremholdt økonomisk byrde som en grunn til å ikke gjøre sikkerhetslovens § 10 gjeldende for petroleumssektoren (Jordanger, 2022). Dette blant annet med bakgrunn i at de mener at Petroleumsloven allerede ivaretar dette aspektet. Henvisningen til rettighetshaver i petroleumsforskriften som refereres av NOROG gjør at dette argumentet kan fremstå svakere enn NOROG kanskje selv opplever. Selv om det er et poeng at man ikke bør ha overlappende regelverk som kan gi usikkerhet om virksomheten skal forholde seg til den ene eller andre loven.

Ettersom sikringstrussel, og da spesielt i form av statlig etterretning, kan oppleves abstrakt og lite konkret, er det ikke unaturlig at det er vanskeligere å forholde seg til denne trusselen på samme måte som sikkerhetsutfordringer. Denne forskjellen i tilnærming til sikkerhets- og sikringsfeltet; kan komme av ulike kulturer som kolliderer. Det har over lengre tid vært en utvikling for å drive virksomheter på en smidig måte, slik at man har en effektiv og kostnadseffektiv drift. HMS er et veldig konkret felt å måle resultater på. Samtidig er det i den enkelte ansattes egeninteresse å ha en sikker arbeidsplass. Når det gjøres en risikovurdering i en HMS-sammenheng er det oftest konkrete hendelser, som man kan si at enten skjedde eller ikke skjedde. En HMS-hendelse vil normalt påvirke enten den ansatte eller virksomheten direkte, og gjerne begge deler. Slik regelverket er bygget opp vil en rettighetshaver eller operatør kunne miste retten til dette ved for mange eller grove hendelser. Dette samme konsekvensregimet er ikke like tydelig innen sikringsregelverket for sektoren. Dette kan blant annet knyttes til usikkerheten ved en etterretningstrussel. Når har man forebygget mot det, og hva er godt nok?

Et sikringsregime som skal være i stand til å hindre en statlig etterretningsaktør; krever en del strukturelle sperrer i organisasjonen. All informasjon skal ikke være tilgjengelig for alle, og alle kan ikke jobbe med alt. Næringens kostnads- og forenklingsfokus kan gi utfordringer i møte med en sikringskultur som er i stand til å forhindre at en trusselaktør kan tilegne seg data om infrastruktur og tilhørende sårbarheter. Dette er likevel ikke unikt for næringen, og vi ser de samme utfordringene som gjentas også på direktoratsnivå i OD som vist i 5.1.

Sikkerhetsloven har som hensikt å ivareta slike problemstillinger som presentert ovenfor, og har som følge av dette en del virkemidler som kan benyttes. Dette fordrer likevel at sikkerhetsloven kommer til benyttelse, samtidig som det er utfordringer med definisjoner rundt hvor og i hvor stort omfang sikkerhetsloven skal benyttes. OED har brukt flere år etter introduksjonen av loven før de har definert en relativt rund betegnelse som GNF. Dette på tross av at flere fagetater har gitt sine innspill på nødvendigheten av å definere deler av sektoren som GNF. Det er usikkert om det er kompleksiteten i spørsmålet, eller hvorvidt OEDs syn på petroleumssektoren som viktig for nasjonale sikkerhetsinteresser, som har ledet til tidsbruken.

Det er ikke gitt at sikkerhetsloven er svaret på spørsmålet om hvordan ivareta den statlige etterretningstrusselen mot petroleumssektoren. Men sett opp mot beskyttelsesinstruksen

og petroleumsloven, har sikkerhetsloven flere virkemidler som kan benyttes for å klare å møte trusselbildet. Som også Etterretningstjenesten sier i sitt høringssvar til tidligere nevnte høring om endring i sikkerhetsloven § 10, er det ikke et reelt alternativ å underlegge alt næringsliv sikkerhetsloven. Det må derfor nøye vurderes hvor denne kan ha effekt, og hvordan det kan administreres, før loven innføres for nye virksomheter eller næringer.

Videre vil dette kapittelet drøfte de ulike begrepene og lovverkene som er introdusert gjennom oppgaven, og hvordan de kan bidra til å styrke eller svekke sektorens tilnærming til statlig etterretning som trussel.

6.1.1 Sikring vs. sikkerhet

Om man ser på de tidligere nevnte definisjonene av sikkerhet og sikring presentert i 3.3, kan dette kanskje forklare noe av utfordringen med statlig etterretning i et sikringsregime. Dersom man benytter delingen av feltene som handler om intensjon, der sikkerhet handler om ikke-intensjonelle hendelser, mens sikring handler om intensjonelle hendelser. Vil sikkerhet i stor grad bestå av å hindre tekniske svikter og å gjøre det lettere for mennesker å gjøre rett enn å gjøre feil. Her vil man ved opplæring og kvalitetskontroll kunne innføre standardiserte barrierer med høy treffsikkerhet. I tillegg vil det jevnlig være mulig å evaluere og forbedre disse gjennom nesten-ulykker og ulykker. Implementeringen av reviderte barrierer i etterkant av en ulykke vil ha en relativt stor sannsynlighet for å redusere sannsynligheten for at den samme typen ulykke skjer igjen. Kostnadene ved en slik tilnærming vil dermed kunne reduseres over tid, gjennom en systematisk tilnærming. En intensjonell handling derimot, vil kreve at virksomheten til enhver tid tilpasser seg hvilken aktør som er aktuell, vurderer dennes evne og vilje, samt evaluerer sin egen sårbarhet på flere områder. Dette gjør det forlokkende å fokusere på en fysisk trussel, enten i form av direkte terroranslag eller IKT-trusler. Som tidligere nevnt har et cyberangrep flere likhetstrekk med et direkte fysisk anslag, blant annet ved at det er avgrenset i tid og rom. Både terrorangrep og IKT-trusler er relativt lette å forebygge mot, ettersom de på samme måte som sikkerhetstrusler i stor grad kan forebygges gjennom generiske barrierer i form av gjerder, enkel adgangskontroll og opplæring. For IKT vil et cyberangrep fra en statlig aktør i liten grad skille seg fra en ikke-statlig aktør.

Dersom vi benytter den andre delingen, som handler om hvem man skal beskytte, vil det kunne forklare utfordringen med å klart definere statlig etterretning som en trussel mot

virksomheten. Der sikkerhet beskytter menneskene og miljøet mot systemet er det klart definert hvem som er eksponert, og hva potensielle konsekvenser av en hendelse er. Det er også en «trusselaktør» som er kjent, og som virksomheten som utgangspunkt kan styre helt selv. Man kan velge akseptabel eksponering og risikonivå, og man kan også legge inn mekanismer som ivaretar svikt i enten teknisk eller menneskelige faktorer. Når man ser på sikring som å beskytte systemet mot mennesker, er det vanskeligere å få en konkret vurdering av hva dette systemet man skal beskytte er. Som utgangspunkt vil en virksomhet vurdere trusselbildet ut fra sin egen virksomhet, og beskytte dette systemet mot trusler. Dersom de ikke anser nasjonal sikkerhet som en del av sitt ansvarsområde; vil de naturlig ikke fokusere på dette bildet i sin sikringstilnærming.

Dersom man vurderer sikringsfeltet i samspill med sikkerhetsfeltet, vil man kunne oppnå synergier som nevnt i 3.3. Et sikkerhetstiltak som å hindre uautorisert tilgang til kritisk teknisk utstyr som kan føre til ulykker, vil også kunne hindre en villet handling mot det samme utstyret. Men der man kanskje har mest igjen for å se sikring og sikkerhet i sammenheng er for å påse at det ikke innføres sikkerhetstiltak som svekker sikringen, og motsatt, at det ikke innføres sikringstiltak som svekker sikkerheten unødvendig.

6.1.2 Risiko

Risikobegrepet er godt etablert i petroleumssektoren, men da hovedsakelig i en sikkerhetstenkning. Flere forskrifter og lovparagrafer nevner risiko og risikoreduksjon eksplisitt som en overordnet prioritering. Og PTIL har utviklet risikobegrepet sitt til å inkludere usikkerhet gjennom definisjonen «[…] konsekvensene av virksomheten med tilhørende usikkerhet.» (PTIL, 2022). Selv om denne definisjonen ivaretar usikkerheten i sikkerhetsregimet, er den ikke like egnet til å ivareta sikringsrisiko. En definisjon som bedre ivaretar både sikkerhet og sikring, iallfall i et nasjonalt bilde, vil måtte innarbeide et større bilde enn direkte konsekvens av virksomheten.

En mulig definisjon av risiko som bedre ivaretar det store bildet kan være «Risiko er konsekvensene av en hendelse tilknyttet virksomhetens aktiviteter, med tilhørende usikkerhet». Alternativt kan man bruke Njå et als definisjon av risiko i en samfunnssikkerhetskontekst; som lyder «Risiko er et uttrykk for konsekvens/utfall av uønskede hendelser og usikkerhet assosiert med hendelser og utfall.» (Njå, 2020, s. 46). Begge disse åpner for at konsekvenser ikke trenger å være utløst av virksomhetens aktivitet,

og kan dermed være bedre i stand til å ivareta sikringsaspektet samtidig med sikkerhetsaspektet.

6.2 På hvilken måte kan strukturer og lovverk i bidra til å motvirke statlig etterretning som trussel mot petroleumssektoren?

Både Petroleumsloven og sikkerhetsloven er såkalte funksjonelle regelverk. Dette innebærer at de i stor grad er intensjonsbaserte, og angir i hovedsak hva som skal oppnås heller enn hvordan det skal oppnås. Som følge av dette er det stor grad av selvregulering innen begge områdene, dog med noen spesifiserte minimumskrav, og da spesielt i sikkerhetsloven med forskrifter. Dette kapittelet vil drøfte de ulike lovene med tilhørende beslutningsstrukturer og hvordan de praktiseres i dag. Deretter vil de ulike lovene settes opp mot hverandre for å se om det er gap i dekningsområder.

6.2.1 Petroleumsloven

Petroleumsloven har som nevnt i 3.5 flere aspekter, og de ulike forskriftene som er hjemlet i petroleumsloven utdyper i stor grad de fleste aspektene. Ettersom petroleumsloven med forskrifter er et funksjonelt regelverk, er det likevel et stort handlingsrom i tolkninger. Vi ser at det hovedsakelig er *styringsforskriften*, *petroleumsforskriften*, og *Forskrift om informasjons- og påseplikt og innsynsrett* som kan relateres til sikringsaspektet i større eller mindre grad. Ved en analyse av forskriftenes paragrafer er det likevel tydelig at de har sitt hovedfokus mot regulering av risiko og sikkerhet i det tradisjonelle HMS-perspektivet.

Foruten petroleumslovens § 9-3 og petroleumsforskriftens § 10; er det vanskelig å finne konkrete sikringsfaglige vurderinger i petroleumslovverket. Petroleumstilsynet med sitt ansvar for å følge opp og gjennomføre tilsyn i lys av petroleumslovens § 9-3 sier i intervju at de fremholder at påseplikten i § 6 av *Forskrift om informasjons- og påseplikt og innsynsrett* er gjeldende også for petroleumslovens § 9-3. De presiserer at det er en vesensforskjell mellom rettighetshaver som oppgitt i § 9-3 og operatør, det er likevel enighet mellom dem som tilsyn og bransjen; om at rettighetshaver og operatør er ensbetydende i denne sammenheng. Dette medfører at de i sin tilsynsrolle som hovedregel forholder seg til operatørselskapene i sine tilsyn, og påser at disse har et system for å videreføre tilsynet til leverandørbedriftene. Det gjennomføres også intervjuer med leverandørbedriftene som

stikkprøver på operatørens påseansvar. Dette gir mening med tanke på at det er samme modell som benyttes for alle PTILs tilsyn.

Det er likevel ikke gitt at det er den beste måten å gjøre tilsyn på. Det er en mulighet for at man ikke fanger opp leverandørbedriftenes unike utfordringer, som til tider kan være påført av operatørbedriftene. Dersom operatørbedriftene presser leverandørbedriftene på marginene, kan dette medføre at leverandørbedriftene må ha et suboptimalt sikringsregime for å klare å konkurrere i markedet, eller at de ikke har mulighet til å etterleve sikringsregimet i praksis. PTIL sier selv at de ikke har anledning til å gå ned i detaljer på sine tilsyn, men hovedsakelig retter dem mot styringssystemer og ledelsesnivå. Det kan stilles spørsmål ved om et slikt tilsynssystem er like bra for sikringstrusler som for sikkerhetsregimet. Dette gjelder spesielt den statlige etterretningstrusselen, ettersom både trusselvurdering og effekt av tiltak vil kunne ha en tidvis høy grad av subjektivitet ved seg ved en slik trussel. En etterretningstrussel kan inneholde så stor usikkerhet om både evne, vilje og verdier, at det kan oppleves som vanskelig å balansere dersom man ikke har konkrete tiltak å forholde seg til.

PTILs tema for 2021 var «På lag med leverandørene», noe PTIL selv opplyser er en konsekvens av at de har identifisert at leverandørindustrien er i en presset markedssituasjon. PTIL sier selv at årets tema gjennomsyrer alle tilsyn som gjennomføres, også sikringstilsynene. Det er knyttet noe usikkerhet til hvordan leverandørbedriftene har merket dette i praksis.

På spørsmål om PTILs vurdering av petroleumslovens § 9-3 opp mot statlig etterretning som trussel beskriver de petroleumsloven som en «fredstidslov», og at den «gjelder til den ikke gjelder lenger dersom det blir sikkerhetspolitisk krise eller krig». De forventer at beredskapsloven(e) skal tre i kraft dersom det oppstår en sikkerhetspolitisk krise eller krig truer, og dermed ivareta sikringsaspektet i den sammenheng. Beredskapslovens virkeområde er hovedsakelig «Når riket er i krig eller krig truer eller rikets selvstendighet eller sikkerhet er i fare […]» (beredskapsloven (§3), 1950), og det er vanskelig å se hvordan denne loven kan benyttes for å ivareta trusselbildet fra statlig etterretning før forsvaret mobiliseres i større eller mindre grad. I den grad man snakker om å forebygge statlig etterretning; må man anta at det er for sent å starte dette arbeidet ved en mobilisering av forsvaret.

PTILs tilnærming med å integrere sikring i petroleumsloven med forskrifters allerede eksisterende regelverk fremstår som en klok løsning for å fremme sikringsfeltet. Selv om PTIL i sin årsrapport for 2021 skriver at de har sett en bedring siden 2014 (Petroleumstilsynet, 2021), er dette over en periode på 6 år. En ytterligere integrering av sikring i regelverket vil kunne bygge videre på de allerede gode strukturene som eksisterer, og dermed slippe å måtte etablere nye måter å jobbe på.

6.2.2 Sikkerhetsloven

Nåværende sikkerhetslov kom ut i 2019, og det gjøres fremdeles tilpassinger med tanke på å konkretisere de svakheter man ser i loven og departementenes tolkning. Blant annet den tidligere nevnte høringen angående innstramming av loven når det gjelder eierskapskontroll. Samt utvidelse av tilknytning til Grunnleggende nasjonale funksjoner (GNF) fra avgjørende til vesentlig.

I forbindelse med lovens utforming ble det i forarbeidet til loven i 2016 levert en rapport fra Forsvarets forskningsinstitutt (FFI), hvor de henviser til petroleumstilsynets årsrapport for 2014 som sier

> «Etter at Petroleumstilsynet i 2013 ble delegert myndighet etter petroleumslovens § 9-3 har vi identifisert flere områder hvor det er nødvendig med en gjennomgang for å vurdere hvordan de ansvarlige selskapenes oppfølging av sitt ansvar i hht § 9. 3 innvirker på oppfølgingen av beredskap forøvrig. Dette gjelder både hvorvidt det underliggende regelverket i dag i tilstrekkelig grad dekker ansvaret gitt i § 9-3, og hvorvidt tilsynsmyndigheten må utvikle nye strategier for å følge opp sikringsforhold hos aktørene» (Petroleumstilsynet, 2014, s. 25).

Det er verdt å merke seg at dette er årsrapporten fra 2014, og FFI-rapporten er fra 2016. Det er likevel først i 2021, etter at sikkerhetsloven er innført, at vi ser departementene gjøre grep for å ivareta bekymringene som blir løftet i 2014.

Vi ser at FFI, på samme måte som petroleumsloven og PTIL fokuserer på en fysisk trussel i form av terror. Dette er ikke unaturlig sett i lys av hendelsene i In Amenas i 2013, hvor en terroraksjon på Statoils anlegg kostet flere personer livet (FFI, 2016). FFI ser likevel bredere og vurderer blant annet den manglende defineringen av skjermingsverdige objekter i petroleumssektoren som problematisk. De påpeker, som også er hevdet i denne oppgaven,

at definering av objekter innen sektoren som skjermingsverdige i henhold til sikkerhetsloven vil kunne «[…] bedre beredskapen overfor spionasje, sabotasje og terrorisme.» (FFI, 2016, s. 39). Spionasje i form av statlig etterretning har som nevnt i 5.2 flere hensikter. Én hensikt kan være å påvirke beslutninger og beslutningstakere, en annen kan være å bidra til strategiske vurderinger innen geopolitiske felt, og en tredje kan være kartlegging og forberedelse til sabotasje og krigshandlinger.

Man skulle tro at sikkerhetsloven blir gjeldende for store deler av petroleumssektoren allerede ved å definere «[…] kontroll med utvinning av petroleum på norsk sokkel» (Olje- og energidepartementet, 2021) som ny GNF. Hvordan dette skal avgrenses til enkeltvirksomheter, informasjon eller objekter vil mest sannsynlig bli debattert i sektoren i lang tid fremover. Blant annet grunnet usikkerhet om hva som er skjermingsverdig, men også fordi en så omfattende regimeendring som dette kan medføre vil kreve styrking av flere funksjoner som støtter opp om sikkerhetslovens krav.

I sikkerhetslovens kapittel 7 defineres skjermingsverdige objekter og infrastruktur som «[…] skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.» (Sikkerhetsloven (§7-1), 2018). En definisjon som skjermingsverdig fører videre til at man skal vurdere hvilken klassifisering det skjermingsverdige objektet eller infrastrukturen har i henhold til sikkerhetslovens § 7-2.

I det man kan kalle fredstid kan sikkerhetslovens fokus på nasjonal sikkerhet og statlige aktører virke overdrevet for en næring som petroleumsnæringen. Det er likevel viktig å sikre at nasjonal selvstendig beslutningsevne kan opprettholdes. Krigen i Ukraina har ytterligere vist hvor viktig norsk petroleumssektor er i et geopolitisk bilde, og det er nesten vanskelig å overdrive hvor store konsekvenser det kan få dersom eksempelvis Kårstø eller en av eksportrørledningene får driftsavbrudd over en lengre periode. Spesielt dersom dette skjer mens Russland bruker avhengighet av gassleveranse til å utøve press på EU.

Det er likevel, som påpekt i flere av tilsvarene på høringen, viktig å bygge opp støttestrukturene i forbindelse med en eventuell endring i klareringsregime innen petroleumssektoren. Dersom det vedtas at sektoren skal kreve bare noe så enkelt som adgangsklarering, vil det sannsynligvis kreve en betydelig styrking av Sivil

klareringsmyndighet for å klare å håndtere den store økningen av klareringer som må gjennomføres.

6.2.3 Sammenligning

Petroleumsloven og sikkerhetsloven er begge funksjonelle regelverk, og de har begge utledede forskrifter som detaljerer ulike deler av loven. De har likevel en forskjell i sikringstilnærming ved at petroleumslovens § 9-3 fokuserer på til dels lokale følger av direkteanslag mot en installasjon, med skade på mennesker og miljø som fokus. Mens sikkerhetsloven fokuserer på å beskytte nasjonen Norges interesser. En terror- eller sabotasjetrussel vil normalt være konkret og tidsavgrenset sammenlignet med en etterretningstrussel, som er kontinuerlig pågående kartlegging av sårbarheter og beslutningsgrunnlag for påvirkningsoperasjoner. Dette medfører at tiltaksnivåene i sikkerhetsloven fremstår bedre egnet til å ivareta denne trusselen. Det finnes som tidligere nevnt muligheter for å innføre lavterskeltiltak som adgangsklarering for objekter uten at hele sikkerhetsloven trenger å gjøres gjeldende, men dette krever at de ulike myndighetene selv velger å gjøre dette. Praksis til nå tilsier ikke at dette har vært ansett som en løsning. Ny GNF «[…] kontroll med utvinning av petroleum på norsk sokkel» (Olje- og energidepartementet, 2021) nødvendiggjør en ny vurdering av tiltak. Denne vurderingen vil mest sannsynlig medføre at deler av petroleumssektoren, både på myndighetsnivå og næringen, vil bli omfattet av sikkerhetsloven med klareringsregimer i større eller mindre grad. I så fall har NSM uttalt at PTIL mest sannsynlig vil være tilsynsorgan også for etterlevelsen av sikkerhetsloven (Petroleumstilsynet, 2019, 9:50). Dette vil medføre en endring i mandat, men også mest sannsynlig gjøre at PTIL må gjøre sikringstilsyn direkte mot virksomheter i alle ledd, og ikke lenger kan basere seg på operatørenes påseplikt. I så måte kan det bli nødvendig å øke størrelsen på petroleumstilsynets sikringsavdeling for å møte dette behovet.

6.3 Hvordan definerer leverandørindustrien risikoakseptkriterier for sikringstrusler?

Petroleumsnæringen er vant med å benytte risikoakseptkriterier i tilnærmingen til sikkerhet, som følge av dette var det derfor en forventning å se den samme tilnærmingen innen sikringsfeltet. Dette er derimot ikke tilfellet basert på informantenes tilbakemeldinger, og dette kapittelet vil drøfte noen av utfordringene som er presentert, før den også tar for seg hvordan bruk av risikoakseptkriterier kan bidra til å styrke sikringstilnærmingen.

6.3.1 Utfordringer med risikoakseptkriterier i et sikringsregime

Informantene som er intervjuet opplyser at de finner det vanskelig å definere risikoakseptkriterier for sikringstrusler, og da spesielt med tanke på etterretning. Dette gjør at de ikke benytter risikoakseptkriterier i det hele tatt for denne typen risikoer. Det oppleves likevel upresist å si at man ikke kan bruke risikoakseptkriterier, ettersom man enten formelt eller uformelt må ha en holdning til hvilken risiko man er villig til å akseptere. Det er likevel forståelig at næringen finner det vanskelig å bruke dem formelt, ettersom det vil kunne kreve relativt omfattende tiltak for å kunne sikre at man ivaretar det satte nivået. Dette viser igjen i krav til behandling av gradert informasjon etter sikkerhetsloven (Virksomhetsikkerhetsforskriften (§22), 2019). Sikkerhetsloven benytter en ordlyd som kan leses som risikoakseptkriterier i Kapittel 5. Informasjonssikkerhet:

> Virksomheten skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdig informasjon, slik at informasjonen
>
> a. ikke blir kjent for uvedkommende
> b. ikke går tapt eller blir endret
> c. er tilgjengelig ved tjenstlig behov. (Sikkerhetsloven (§5-2), 2019)

Vi ser her at det er et absolutt krav, og ikke en ALARP-tilnærming, det vil likevel måtte gjøres en vurdering for hva som er godt nok på de ulike nivåene av gradering. Dette kan virke som oppnåelige; og til og med ønskelige mål for enhver virksomhet. Dersom man skal garantere for en slik informasjonssikkerhet kan det likevel fort bli kostbart, og legge en stor administrativ byrde på organisasjonen ved å legge store restriksjoner på informasjonsdeling.

PTIL opplyser selv at ALARP-begrepet ikke benyttes i norsk regelverk ettersom det er varierende tolkning av hva det innebærer, og at det ikke alltid oppnår risikoreduksjon i henhold til intensjonen i norsk regelverk (Petroleumstilsynet, 2018). Det er rimelig å anta at man kan møte kost/nytte-vurderinger som vil utfordre virksomheters nyttevurdering av å innføre strenge tiltak. Med bakgrunn i at det kan være vanskelig å se en direkte kobling mellom tiltak, reduksjon i sårbarhet, og redusert risiko innen sikringsfaget, vil usikkerheten kunne medføre at «reasonably possible» er en lett konklusjon å trekke.

Denne usikkerheten vil gjerne først og fremst gjelde sannsynligheten for at en trussel er aktuell for den aktuelle virksomheten. Men all forebyggende aktivitet har usikkerhet

innebygget, også sikkerhet, like fullt bruker man risikoakseptkriterier for sikkerhet. Usikkerhet kan også omhandle kunnskap om verdiens betydning utover sin egen virksomhet. Dersom myndighetene er uklare i sin kommunikasjon av verdien av en bestemt type informasjon eller funksjon, vil det være vanskelig for å virksomheten å vurdere konsekvensen av en eventuell trussel, og dermed hva dette bør innebære for risikoakseptkriteriene.

Men også operatør bør gjerne ha en tydeliggjøring av hva som er akseptabel risiko i forbindelse med statlig etterretning som trussel. Ved å definere et risikoakseptkriterie vil man som utgangspunkt redusere usikkerheten. Ved å forholde seg til risikoakseptkriteriene heller enn et mer eller mindre abstrakt trusselbilde, vil det være tydeligere om tiltakene er tilstrekkelig for å ivareta sikringsnivået. Selv om trussel fremdeles vil være en faktor, vil de grunnleggende tiltakene ligge på et så høyt nivå; at trussel i utgangspunktet heller vil påvirke hvem og hvor mange som skal omfattes av innførte tiltak, heller enn nødvendigheten av de innførte tiltakene.

Dersom risikoakseptkriterie for et eksportanlegg som Kårstø; er at kun nødvendig personell skal kjenne til infrastrukturen, må man bygge rutiner som kan bidra til å hindre andre enn nødvendig personell å kunne kartlegge infrastrukturen. Uavhengig av om objektet er skjermingsverdig eller ikke, vil man kunne gjøre tiltak som adgangskontroll og begrensinger på dokumenttilganger til definerte personer det er gjennomført bakgrunnssjekk på. Dersom objektet blir definert som skjermingsverdig vil dette mest sannsynlig kreve at sikkerhetslovens egen tilnærming til risikoaksept blir gjort gjeldende.

6.3.2 Hvordan kan risikoakseptkriterier bidra til en bedre sikringsrisikostyring?

Det er tidligere nevnt at for strenge risikoakseptkriterier kan medføre komplikasjoner for den daglige driften av en virksomhet. Virksomheter og organisasjoner som er underlagt sikkerhetsloven, og da spesielt statlige, er kjent for å ha et strengt hierarki for deling av informasjon. I en virksomhet som skal drives med den hensikt å tjene penger i et åpent marked kan dette oppleves som en stor klump om foten. Dersom vi skal se på sikringsaspektet ved å benytte sikringsrisikoakseptkriterier kan det likevel ha stor nytte å benytte tydelige kriterier. De tidligere nevnte statlige organisasjonene som eksempelvis forsvaret har strenge regler for informasjonsdeling, men like fullt klarer man å drive organisasjonen.

De fleste private virksomheter vil kunne ha nytte av tydelige kriterier som kan kommuniseres på en klar måte. Med henvisning til utfordringen rundt bevisstgjøring om innsidetrusselen nevnt i 5.3, kan man gjerne se fordel av en tydeliggjøring av hva som er akseptabel risiko ved behandling av informasjon. Tydeligere linjer vil kunne gjøre det lettere for de ansatte å etterleve reglene ved at man kan henvise til et kjent regelsett. Det vil også kunne bidra til en større forståelse for arbeidet som gjøres av sikringsansvarlige. Summen av disse vil kunne bidra til å redusere virksomhetens sårbarhet.

6.4 Hvordan forholder leverandørnæringen seg til statlig etterretning som en nasjonal trussel?

Statlig etterretning er en komplisert trussel å forholde seg til, og det som er gjennomgående fra alle informanter, uansett tilhørighet, er at det er vanskelig å forholde seg til et slikt trusselbilde. Der man ikke har åpenbare indikasjoner på at virksomheten er av interesse; kan det være vanskelig å plassere seg selv inn i et slikt trusselbilde. I mange tilfeller kan det nok stemme at små virksomheter ikke er av stor interesse i seg selv, de presenterer likevel en sårbarhet og et gap i rustningen til operatørselskapene dersom de ikke har kontroll på egne sårbarheter. Dette kapittelet vil gå mer inn på hva dette innebærer for leverandørselskapene.

6.4.1 Tilsyn og revisjoner av sikring

Hierarkiet for tilsyn i petroleumssektoren er klart etablert, og er likelydende for alle områder PTIL har tilsynsansvar for. Dette gir en styrke i at det er tydelig ansvarsfordeling når det kommer til oppfølging. PTIL gjennomfører tilsyn med rettighetshaver/operatør, og operatør gjennomfører tilsyn med leverandørselskapene. På samme måte forventes det at leverandørselskapene fører tilsyn med sine underleverandører. Ettersom dette gjelder for alle deler av lovverket, kan man benytte samme rammeverk og fremgangsmåte for sikringstilsyn som for HMS eller for petroleumsloven for øvrig.

En utfordring med denne tilsynsmodellen er at man risikerer å ikke avdekke gap i leverandørenes sikringsarbeid som er forårsaket av operatørenes driftsmodell. Dersom man utelukkende ser det fra HMS- og arbeidslivsperspektivet er dette dekket opp av flere lovparagrafer, standarder, mekanismer og holdninger i samfunnet. Det finnes derimot ikke de samme mekanismene innenfor sikringsperspektivet. Store deler av

petroleumslovgivingen dekker HMS, og vernetjenesten på arbeidsplassen har en formell rolle i å ivareta dette arbeidet. Arbeidsmiljølovgivningen dekkes av trepartssamarbeidet med sterke fagforeninger, men sikringsfeltet har ingen slike innarbeidede mekanismer for å rapportere svikt til myndighetene.

PTIL sier, som nevnt flere ganger, at de opplever samarbeidet med næringen som godt. De opplever også at næringen erkjenner sin plass i det nasjonale sikkerhetsbildet. Vi ser likevel basert på svarene fra næringen selv, og funn gjort ved å ettergå eierskap av seismikkskip som er kontrahert av norske virksomheter, at det nasjonale sikkerhetsbildet kan komme til kort når det settes opp mot den daglige ressursforvaltningen i virksomhetene. PTIL sier også selv at de ikke vurderer tjenester som seismikk i sine sikringsoppgaver. En mulig måte å tette dette gapet; er å i større grad føre direktetilsyn med leverandørbedrifter. En styrking av petroleumslovens § 9-3 vil også kunne konkretisere det som allerede ligger i forarbeidene, men også gjøre det lettere for virksomheter underlagt petroleumsloven å vite hva som er forventet av dem. Dette vil nødvendigvis også gjøre det lettere for PTIL å stille krav til sikringsfeltet med henvisning til lovhjemmel.

6.4.2 Er leverandørindustrien bevisst sitt ansvar?

Leverandørindustrien består av flere ulike typer bedrifter, fra teknologi- til kunnskapsbedrifter, og fra flere tusen til under ti ansatte. Det de fleste har felles; er at de er nødt til å presse marginene til enhver tid for å vinne kontrakter. Fra et bedriftsøkonomisk perspektiv kan dette gjerne ses på som en sunn mekanisme for å redusere unødvendige kostnader, men det er samtidig en av hovedgrunnene til at denne oppgaven identifiserer leverandørindustrien som en sårbarhet sett opp mot statlig etterretning. PTIL sier selv at det er et fåtall av leverandørbedriftene som har personell dedikert som sikringsansvarlige, og at de fleste sitter i kombinasjonsstillinger. Uten at det er uttalt fra PTIL eller andre informanter er det naturlig å anta at disse sitter i en kombinasjonsstilling med HMS-ansvar.

Flere av leverandørene har allerede flagget ut forskjellige tjenester til lavkostland som eksempelvis India. Typiske eksempler på slik utflagging er IT-, regnskap-, HR, og ingeniørtjenester. Virksomheten ivaretar gjerne en lokal kjernekapasitet, men mye av arbeidet blir gjort i lavkostlandet. Dette medfører at man åpner deler av infrastrukturen sin for personell som befinner seg utenfor de tradisjonelle samarbeidslandene (NATO + EU), noe som vanskeliggjør den samme personellkontrollen som i Norge. PTILs rapport på

innsidetrusselen nevner dette som en problemstilling, «En utfordring er ved outsourcing av enkelte tjenester, f.eks. IT-tjenester til India dersom personellet har tilgang til kritiske funksjoner – det kan være vanskelig å kreve og/eller få gjennomført ønsket utvidet sjekk og godkjenning.» (Jerre & Funnemark, 2019, s. 63). Man må anta at bedrifter med avdelinger i andre land foretar en form for bakgrunnssjekk der det er relevant. Men man kan regne med at denne kontrollen er mindre eller mer streng enn den norske sjekken alt etter landets strukturer og personvernregler. Samtidig fordrer det at det foreligger en korrekt forståelse av trusselen og hvilke sårbarheter man har i organisasjonen og infrastrukturen.

Dersom det nå kommer en innstramming i sikkerhetsloven som gjør at deler av petroleumsnæringen vil være under sikkerhetsloven, og dermed kreve sikkerhetsklarering for enkelte funksjoner, vil sikkerhetsklarering av innbyggere i land utenfor sikkerhetssamarbeidet være tilnærmet umulig å gjennomføre. Det er tidligere avdekket at virksomheter underlagt sikkerhetsloven har flagget ut IT-arbeid til India, og dette medførte at driften måtte føres tilbake til Norge (Remen & Tomter, 2017). Det kan være vanskeligere å gjennomføre nasjonal kontroll på informasjon i globale bedrifter, som baserer driften sin på nettopp å ha sentraliserte interne tjenesteleverandører som betjener flere ulike lokasjoner basert i ulike land. I tillegg til utfordringen med sikkerhetsklarering, vil det også være mulig for ulike lands etterretningstjenester å lytte på, eller kutte, datatrafikk som sendes inn og ut, eller gjennom dette landets infrastruktur. Dersom denne datatrafikken er tilstrekkelig kryptert vil datastrømmen som utgangspunkt være sikker, men lokal infrastruktur på avsenderstedet kan bli påvirket.

I tillegg til denne driften av virksomhetenes infrastruktur og administrative tjenester, er det som tidligere nevnt også ønsket av Halliburton å flytte driften av et landanlegg for fjernstyring av offshoreoperasjoner til Dubai. Dette vil i tillegg til å eksponere egen infrastruktur også eksponere operatørens og potensielt statens interesser for både spionasje og direkte sabotasje. I tillegg vil man få den samme problemstillingen med tanke på sikkerhetsklarering; dersom dette blir aktuelt. Olje- og energiministeren uttrykker misnøye med tanke på arbeidsplassene som eventuelt blir flagget ut (Tollaksen, 2022), men basert på det trusselbildet som har blitt presentert i denne oppgaven; er det nesten viktigere å se på om det er forsvarlig fra et nasjonalt sikkerhetsperspektiv.

Det er høyt fokus på IKT-sikkerhet i næringslivet generelt, og det er utarbeidet flere veiledere og standarder for IKT-sikkerhet. Det er ingenting som tilsier at virksomhetene ikke etterlever det meste av slike veiledere i sine interne retningslinjer. Det er likevel vanskelig å si noe om hvorvidt disse etterleves i det daglige arbeidet i virksomhetene; uten å gjøre en dyptgående studie av enkeltvirksomheter.

Loven legger i dag opp til stor grad av autonomi i vurdering av eget trusselbilde for virksomhetene tilknyttet petroleumssektoren. De presenteres et overordnet trusselbilde fra myndighetene, og de får selv vurdere hvorvidt dette er aktuelt for dem. Denne praksisen bekreftes også av PST i intervju, hvor de er tydelige på at de kun presenterer et trusselbilde som må tolkes og risikovurderes av virksomheten. Informantene forteller at de gjør disse vurderingene, og innfører tiltak i henhold til hvordan de definerer trusselen for egen virksomhet. PST sier i intervju at de opplever en stor interesse for informasjonen de deler, men samtidig opplyser de om at et vanlig utsagn fra dem som blir rammet av etterretningsoperasjoner; er at de ikke anså seg selv som særlig viktige. Denne oppfatningen om at de ikke er viktige for en trusselaktør kan lede til at man legger tiltaksgrensen for høyt i forbindelse med sikringsrisikoanalysene. En annen problemstilling er at ikke alle leverandørselskaper har dedikert sikringspersonell, som kan utføre en sikringsrisikoanalyse på en faglig god måte. Dersom virksomheten ikke innehar kompetanse på sikring, og da spesielt i å gjøre en verdivurdering, vil det kunne medføre at virksomhetens IKT-ansvarlige i praksis blir sikringsansvarlig for informasjonssikkerhet. Dette vil kunne føre til en manglende forståelse av bedriftens verdier og hvordan disse kan påvirke det større sikringsbildet omtalt i denne oppgaven. Det å være en liten bedrift kan ha både fordeler og ulemper. Det vil være kortere vei fra vurdering til beslutning, men samtidig kan det bli veldig personavhengig hvorvidt man opplever seg som eksponert for trusselen.

For å markedsføre produktene sine må bransjen nødvendigvis eksponere dem for kundene, og i den sammenheng vil man gjerne stille ut på messer og offentliggjøre brosjyrer og annen reklame. Dette indikerer informantene ikke som noe sikringsutfordring sett opp mot statlig etterretning, all den tid de allerede må ta hensyn til industrispionasje og andre markedshensyn. Det kan gjerne være hensiktsmessig å ha en bevissthet om at trusselen eksisterer også fra statlige aktører, noe informantene også indikerer at de har. På direkte spørsmål sier informanter med aktuell teknologi at de har en bevissthet om statlig

etterretning mot produktene deres. De sier også at de ved hjelp av den åpne trusselvurderingen avgjør hvilken del av trusselbildet som er aktuelt for dem, og hvilke tiltak de må gjøre for å ivareta denne i henhold til tidligere nevnte praksis. Det er likevel spesifisert at det er hvordan trusselbildet gjør seg gjeldende mot dem som bedrift som er styrende for hvorvidt de treffer tiltak. Dette har både juridiske og praktiske årsaker. En bakgrunnssjekk kan være inngripende for den ansatte, og sikringstiltak koster bedriften penger både direkte i form av utgifter, men også indirekte i form av at arbeidsprosesser kan bli mer kompliserte og tidkrevende. Virksomheten har derfor flere grunner til å være restriktiv med hvem man gjennomfører bakgrunnssjekk på, og også hvilke sikringstiltak som innføres.

For å kunne benytte seg av adgangsklarering eller sikkerhetsklarering må det foreligge en hjemmel i sikkerhetsloven. Denne hjemmelen er hovedsakelig at man har tjenstlig behov, ved å håndtere skjermingsverdig informasjon eller arbeide ved et skjermingsverdig objekt. Denne defineringen som skjermet objekt kan, som tidligere nevnt, bli aktuell for flere objekter innen petroleumssektoren, og dermed vil det tjenstlige behovet foreligge.

6.5 Oppsummering

Kapittelet har drøftet ulike aspekter ved sikringsregimet for petroleumssektoren. Det er indikasjoner på at en videreutvikling av risikodefinisjonen som benyttes av PTIL kan bidra til å bedre ivareta etterretningstrusselen. Det er mulig at sektoren, som samfunnet for øvrig, har blitt preget av flere terrorhendelser, og dermed har rettet sitt forebyggende arbeid i stor grad mot fysiske trusler som kan knyttes mot sikkerhetsaspektet. Samtidig er næringen kompetente på IKT-sikring, som har en viktig funksjon i å motvirke datainnbrudd. Globalisert drift, med utflagging av tjenester som IKT og andre tjenester til lavkostland, kan gi utfordringer med bakgrunnssjekk og sikkerhetsklarering der dette er aktuelt. Dette kan medføre at sektoren og næringen kan være sårbar for innsidetrusler og andre etterretningsgrep i disse landene.

Næringen fremstår i utgangspunktet som opptatt av å leve opp til forventningene som blir gitt fra myndighetenes side. Det kan likevel være utfordrende å definere gode risikoakseptkriterier for sikringstrusler, og da spesielt etterretningstrusler. Ved manglende ressurser eller kunnskap til å tolke det trusselbildet som presenteres fra PST med flere, vil trusler som er rettet mot en tredjepart som nasjonen Norge kunne bli oversett eller misforstått.

7 Konklusjon

Denne oppgaven har tatt utgangspunkt i PSTs åpne trusselvurdering for petroleumssektoren som kom ut i 2020. Basert på denne trusselvurderingen er det utledet problemstillingen «*På hvilken måte er den økende trusselen fra utenlandsk statlig etterretning ivaretatt gjennom lovverk og reguleringsregimet for petroleumsnæringen?».* Gjennom litteraturstudie og informantintervjuer er det foretatt en analyse av det historiske utgangspunktet for å kunne møte denne trusselen, samt status i dag og hvilken utvikling man ser for seg fremover.

Oppgaven finner at det historisk har vært et lavt fokus på sikring generelt, og statlig etterretning har i stor grad blitt sett på som en av flere trusselaktører i cyber-domenet. Det kan fremstå som man historisk ikke har tatt inn over seg det som skiller statlig etterretning fra mer konvensjonelle trusselaktører. Både i form av evne og vilje, men også hva statlige trusselaktører ønsker å oppnå. For å bruke bildet fra innledningen; så kan det virke som man har vurdert tiltak for å unngå at verdisaker blir stjålet fra bilen, men ikke har kontroll på hva i bilen som kan defineres som verdisaker, og dermed blir tiltakene mangelfulle.

Petroleumsloven fremstår mangelfull med tanke på sikring, og § 9-3 i petroleumsloven leses i hovedsak som en lov om fysisk sikring av anleggene. Grepene som er gjort i senere tid med tanke på IKT-sikkerhet har stor verdi, men det kan bli en hvilepute slik at man ikke tar for seg eksempelvis leverandørene som byr på jobber; og hvorvidt disse har redelige hensikter eller ikke. Det er gjort et stort arbeid med å bedre sikringsnivået i næringen, men petroleumsmyndighetene har vegret seg for å i lovs form regulere sikring i større grad. Dog er dette i ferd med å endres.

Det er på slutten av 2021 og starten av 2022 kommet resultater av flere arbeider som har pågått de siste årene, og disse vil med stor sannsynlighet gi sikringsfokuset et stort løft i næringen. OEDs definisjon av deler av petroleumssektoren som GNF vil ha stor betydning for sektorens forhold til sikkerhetsloven. Dette sammen med de foreslåtte endringene av sikkerhetsloven; vil kunne medføre et betydelig strengere sikringsregime, og da spesielt rettet mot statlig etterretning som trusselaktør.

Det er på skrivende tidspunkt uklart nøyaktig hva de ovennevnte endringene vil innebære, men det vil med stor sannsynlighet medføre et behov for å styrke støttestrukturer som

eksempelvis Sivil klareringsmyndighet. Dette gjør også at en eventuell implementering av tiltak i henhold til sikkerhetsloven vil ha lang ledetid før de kan få full effekt.

På samme måte som myndighetene over tid har utviklet et robust og omfattende sikkerhetsregime for bransjen, er det nødvendig å bygge den samme aksepten for et sikringsregime som ikke bare sikrer mot IKT- og terrorhendelser, men også mot mer abstrakte trusler som statlig etterretning. Det er tydelig gjennom det gode arbeidet som er gjort med sikkerhetsarbeidet at de ansvarlige institusjonene og virksomhetene er godt utrustet for å gjennomføre dette, men det vil kanskje kreve hjelp i form av lovverksendringer.

Den foreslåtte tilpassingen av PTILs definisjon av risiko i sammenheng med petroleumssektoren «Risiko er konsekvensene av en hendelse tilknyttet virksomhetens aktiviteter, med tilhørende usikkerhet» (s.56), er knyttet mot virksomheten på samme måte som PTILs definisjon, men gir et større perspektiv og forventning om å hensynta konsekvenser; også dersom hendelsen ikke skyldes virksomhetens egne aktiviteter. Slik åpner den for å ivareta en trusselaktørs handlinger på en bedre måte; og spesielt dersom denne trusselaktøren ikke er ute etter å ramme virksomheten selv, men heller en tredjepart som operatørselskap eller staten. Njå et als definisjon (s.56) ivaretar det samme, men er mer nøytral i sin tilnærming, og forholder seg til hendelsen selv som eneste objekt i definisjonen.

8 Videre forskning

Denne oppgaven har for det meste skrapet i overflaten på det som er et omfattende og komplekst tema. En videre forskning spesielt rettet mot beslutningsprosesser på myndighetsnivå kan bidra til å belyse hvordan OED har kommet frem til at deler av næringen enten skal eller ikke skal falle inn under den nye GNFen for sektoren. Samtidig kan det være interessant å gjøre en nærmere studie av dynamikken i tilsynskjeden fra PTIL og ned til de minste leverandørene, for å se hvorvidt denne tilsynsmodellen fungerer slik den er tiltenkt.

9 Litteratur

Abrahamsen, E. B., Aven, T., Flage, R., Engen, O. A. H., Røed, W. & Wiencke, H. S. (2020). *Bruk av risikoakseptkriterier En evaluering*. Petroleumstilsynet. https://www.ptil.no/contentassets/4deea346d8cb4008a2eef488f85313ae/bruk-av-risikoakseptkriterier---en-evaluering.pdf

Arbeids- og inkluderingsdepartementet. (2022). *Tildelingsbrev 2022 – Petroleumstilsynet* (20/4594-7). Arbeids- og inkluderingsdepartementet. https://www.ptil.no/contentassets/5dfd37556c5d42e3af4d920db148c306/tildelingsbrev-2022--petroleumstilsynet.pdf

Aven, T. (2015). *Risikostyring*. Universitetsforlaget AS.

beredskapsloven (§3). (1950). *Lov om særlige rådgjerder under krig, krigsfare og liknende forhold* (LOV-1950-12-15-7). www.lovdata.no. https://lovdata.no/lov/1950-12-15-7/§3

Bieder, C. & Pettersen Gould, K. (2020). *The coupling of safety and security: exploring interrelations in theory and practice*. Springer Open

Clifton, L. S. & Brooks, D. J. (2013). *Security science - The theory and practice of security*. Elsevier Inc.

DNV-GL. (2020). *IKT-SIKKERHET - ROBUSTHET I PETROLEUMSSEKTOREN Telekommunikasjon og protokoller* (2019-0827, Rev. 0). Petroleumstilsynet. https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/dnv-gl---telekommunikasjon-og-protokoller.pdf

Etterretningstjenesten. (2021a). *FOKUS 2021*. Etterretningstjenesten. https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf

Etterretningstjenesten. (2021b). *Forsvarets etterretningsdoktrine*. Forsvaret. Forsvarssjefen. https://www.forsvaret.no/om-forsvaret/organisasjon/etterretningstjenesten/Etterretningsdoktrine_2021.pdf/_/attachment/inline/55bb2c9b-7d43-4e7d-b7fa-c44991654a40:45144a0f0efb5dfe84d424ff06d61c0d80dc111a/Etterretningsdoktrine_2021.pdf

European comission. (2022, 08.03.2022). *REPowerEU: Joint European action for more affordable, secure and sustainable energy*. EU. Hentet 03.04.2022 fra https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1511

Eurostat. (2021). *EU imports of energy products - recent developments*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_imports_of_energy_products_-_recent_developments

FFI. (2016). *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart*. Forsvarets forskningsinstitutt. https://publications.ffi.no/nb/item/asset/dspace:2596/16-00702.pdf

Forskrift om utenlandske fartøyers anløp til og ferdsel i norsk territorialfarvann. (2019). *Forskrift om utenlandske fartøyers anløp til og ferdsel i norsk territorialfarvann,* (FOR-2018-12-20-2056). Lovdata. https://lovdata.no/forskrift/2018-12-20-2056

Furuseth, H. R. (2022). *Høringssvar – endringer i sikkerhetsloven (eierskap mv.)*. Nasjonal Sikkerhetsmyndighet (NSM).

https://www.regjeringen.no/contentassets/6f6c7d8b6cb1499e854db502d504b9d4/annen-offentlig-etat/nasjonal-sikkerhetsmyndighet-nsm.pdf?uid=Nasjonal_sikkerhetsmyndighet_(NSM)
GASSCO. (2022a). *Interaktivt kart over gasstransportsystem*. Hentet 07/03/2022 fra https://www.gassco.no/static/transport-3/#/
GASSCO. (2022b). *Roller*. Hentet 06/03/2022 fra https://www.gassco.no/om-gassco/roller/
Halvorsen, K. (2008). *Å forske på samfunnet* (5. utg.). J.W Cappelen Damms Forlag AS.
Haugstad, T. (2019). Den kan gå minst 20 mil på batteri og jobbe på 6.000 meters dyp i 6 måneder. *Teknisk ukeblad*. https://www.tu.no/artikler/den-kan-ga-minst-20-mil-pa-batteri-og-jobbe-pa-6-000-meters-dyp-i-6-maneder/473674
Helgesen, A. E. (2022, 28.01.2022). *Halliburton vil flytte arbeidsplasser fra Norge til Dubai: Dette skal vi slåss imot, sier Industri Energi-lederen*. Hentet 28.01.2022 fra https://industrienergi.no/nyhet/halliburton-vil-flytte-arbeidsplasser-fra-norge-til-dubai-dette-skal-vi-slass-imot-sier-industri-energi-lederen/
Jerre, J. & Funnemark, E. (2019). *Håndtering av innsiderisiko* (2019-0280, Rev. 1). DNV GL Oil & Gas. https://www.ptil.no/contentassets/d0de842c25b84fcebda5c24fe6daa6fa/handtering-av-innsiderisiko-rev-1.pdf
Jordanger, Ø. (2022). *Endringer i sikkerhetsloven (eierskapskontroll mv.)* (22-35). Norsk olje & gass. https://www.regjeringen.no/no/dokumenter/horing-om-endringer-i-sikkerhetsloven-eierskap-mv/id2876352/Download/?vedleggId=66c67120-4f1f-4a53-89cc-ade994e19b64
Justis- og beredskapsdepartementet. (2021). *HØRINGSNOTAT OM ENDRINGER I SIKKERHETSLOVEN (EIERSKAPSKONTROLL MV.)* (21/5593). J.-o. beredskapsdepartementet. https://www.regjeringen.no/contentassets/f521121e63a642f797f5c577742ed605/horingsnotat-om-endringer-i-sikkerhetsloven-eierskapskontroll-mv..pdf
Kibar, O. (2021, 22.10.2021). OPERASJON LAZAREV: Slår alarm om kartlegging av Norges kritiske infrastruktur. *Dagens Næringsliv*. https://www.dn.no/magasinet/teknologi/spionasje/russland/etterretningstjenesten/operasjon-lazarev-slar-alarm-om-kartlegging-av-norges-kritiske-infrastruktur/2-1-1085420
Kibar, O. (2022). Ruster opp cybersikkerheten i norsk olje- og gass – frykter fysiske skader fra digitale angrep. *Dagens Næringsliv*. https://www.dn.no/teknologi/lundin/cyberangrep/cybersikkerhet/ruster-opp-cybersikkerheten-i-norsk-olje-og-gass-frykter-fysiske-skader-fra-digitale-angrep/2-1-1194103
Klareringsforskriften (§15). (2019). *Forskrift om sikkerhetsklarering og annen klarering* (FOR-2018-12-20-2054). www.lovdata.no. https://lovdata.no/forskrift/2018-12-20-2054/§15
Leveson, N. (2020). Safety and Security Are Two Sides of the Same Coin. I C. B. a. K. P. Gould (Red.), *The coupling of safety and security: exploring interrelations in theory and practice*. Springer Open
Nasjonal sikkerhetsmyndighet. (2019). *Veileder i personellsikkerhet*. Nasjonal Sikkerhetsmyndighet. https://nsm.no/getfile.php/132407-1590749199/Filer/Dokumenter/Veiledere/Veileder%20i%20personellsikkerhet.pdf
Njå, O. (2020). *Samfunnssikkerhet : analyse, styring og evaluering*. Universitetsforlaget.

Norsk olje og gass. (2016). Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. I(Bd. 104). Norsk olje og gass. https://norskoljeoggass.no/contentassets/15263fd7f781409286f319bbeb427d93/104-recommended-guidelines-on-security-baseline-requirements2.pdf

Norsk olje og gass. (2019). Anbefalte retningslinjer for sikring av forsyninger og materiell i Olje- og gassindustrien. I(Bd. 091). Norsk olje og gass. https://norskoljeoggass.no/arbeidsliv/retningslinjer/helse-arbeidsmiljo-og-sikkerhet/sikring/091-anbefalte-retningslinjer-for-sikring-av-forsyninger-og-materiell-i-olje--og-gassindustrien/

NSM. (2019, 21.08.2019). Veileder for virksomheters håndtering av uønskede hendelser. I N. Sikkerhetsmyndighet (Red.),(1 utg.). Nasjonal Sikkerhetsmyndighet. https://nsm.no/getfile.php/133116-1591610609/Filer/Dokumenter/Veiledere/veileder-for-virksomheters-handtering-av-uonskede-hendelser.pdf

NSM. (2020). *Sikkerhetsloven og forskrifter - Nasjonal sikkerhetsmyndighet*. https://nsm.no/regelverk-og-hjelp/sikkerhetsloven-og-forskrifter

NSM. (2022a). *Sikkerhetsklarering*. NSM. Hentet 04.05.2022 fra https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/

NSM. (2022b). *Veiledere og håndbøker til sikkerhetsloven*. Hentet 14/02 fra https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/

Olje- og energidepartementet. (2019). *Tildelingsbrev til Oljedirektoratet for 2019*. Olje- og energidepartementet. https://www.regjeringen.no/contentassets/ca56606d0dd14bb2818580bfbb14a91a/tildelingsbrev-til-oljedirektoratet-for-2019.pdf

Olje- og energidepartementet. (2020). *Tildelingsbrev til Oljedirektoratet for 2020*. Olje- og energidepartementet. https://www.regjeringen.no/contentassets/ca56606d0dd14bb2818580bfbb14a91a/tildelingsbrev-til-oljedirektoratet-for-2020.pdf

Olje- og energidepartementet. (2021). *Prop. 1 S (2021 –2022)*. O.-o. energidepartementet. https://www.regjeringen.no/contentassets/f2da0c393fb24b1cb2ed0254d76521da/no/pdfs/prp202120220001oeddddpdfs.pdf

Oljedirektoratet. (2022). *Om oss*. Hentet 06/03/2022 fra https://www.npd.no/om-oss/

Ot.prp.nr.46 (2002–2003). (2003). *Ot.prp.nr.46 (2002–2003) Om lov om endringer i lov 29. november 1996 nr. 72 om petroleumsvirksomhet* www.lovdata.no. https://lovdata.no/pro/forarbeid/otprp-46-200203/KAPITTEL_2-6

petroleumsforskriften (§10). (1997). *Forskrift til lov om petroleumsvirksomhet* (FOR-1997-06-27-653). Lovdata.no. https://lovdata.no/forskrift/1997-06-27-653/§10

Petroleumsloven (§1-4). (2003). *Lov om petroleumsvirksomhet* Lovdata. https://lovdata.no/lov/1996-11-29-72/§1-4

Petroleumsloven (§9-1). (2003). *Lov om petroleumsvirksomhet* Lovdata. https://lovdata.no/lov/1996-11-29-72/§9-1

Petroleumsloven (§9-3). (2003). *Lov om petroleumsvirksomhet* (9-3). Lovdata. https://lovdata.no/lov/1996-11-29-72/§9-3

Petroleumstilsynet. (2014). *Årsrapport 2014*. https://www.regjeringen.no/contentassets/d33a5ffb762447a486acf0363d42fbde/arsrapport_2014_petroleumstilsynet.pdf

Petroleumstilsynet. (2018). Integrert og helhetlig risikostyring i petroleumsindustrien. I. https://www.ptil.no/contentassets/15b49e2079c1497eb117009f2e229133/risikostyring-2018.pdf
Petroleumstilsynet. (2019, 29.10.2019). *Forebygging og håndtering av alvorlige dataangrep* [Video]. Petroleumstilsynet. https://www.ptil.no/fagstoff/utforsk-fagstoff/video/2019/forebygging-og-handtering-av-alvorlige-dataangrep/
Petroleumstilsynet. (2021). *Årsrapport 2021*. https://www.ptil.no/contentassets/754137a590df47949f7e731a6b5c395c/arsrapport-20213.pdf
Petroleumstilsynet. (2022a). *IKT-sikkerhet – robusthet i petroleumssektoren*. PTIL. Hentet 12.03.2022 fra https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/2020/ikt-sikkerhet--robusthet-i-petroleumssektoren/
Petroleumstilsynet. (2022b). *Rolle og ansvarsområde*. Hentet 12.03.2022 fra https://www.ptil.no/om-oss/rolle-og-ansvarsomrade/
PST. (2020). *Etterretningstrusselen mot norsk petroleumssektor*. Politiets Sikkerhetstjeneste.
PST. (2022a). *Nasjonal Trusselvurdering 2022 - Statlig etterretningsvirksomhet*. PST. Hentet 08/03/2022 fra https://pst.no/alle-artikler/trusselvurderinger/ntv-2022/statlig-etterretningsvirksomhet/
PST. (2022b). *PST vurderer etterretningstrusselen fra Russland i Norge som økt* https://www.pst.no/alle-artikler/pressemeldinger/oppdatert-trusselvurdering-pst-ser-en-okt-etterretningstrussel-fra-russland-i-norge/
PTIL. (2022). *Risiko og risikoforståelse*. Hentet 30.01.2022 fra https://www.ptil.no/om-oss/rolle-og-ansvarsomrade/risiko-og-risikoforstaelse/
rammeforskriften. (2010). *Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg (rammeforskriften)* (FOR-2019-04-26-533). https://lovdata.no/forskrift/2010-02-12-158/§11
Regjeringen. (2022a). *Olje- og energidepartementet*. Hentet 06/03/2022 fra https://www.regjeringen.no/no/dep/oed/id750/
Regjeringen. (2022b). *Petroleumsjuridisk seksjon (PJS)*. Hentet 06/03/2022 fra https://www.regjeringen.no/no/dep/oed/org/avdelinger/og/pjs/id445341/
Regjeringen. (2022c). *Seksjon for analyse og infrastruktur*. Hentet 06/03/2022 fra https://www.regjeringen.no/no/dep/oed/org/avdelinger/og/gi/id445338/
Regjeringen. (2022d). *Seksjon for nett, energibruk og marked (NEM)*. Hentet 06/03/2022 fra https://www.regjeringen.no/no/dep/oed/org/avdelinger/ev/seksjon-for-nett-energibruk-og-marked/id2868623/
Remen, A. C. & Tomter, L. (2017, 31.03.2017). IT-arbeidere i India har fortsatt tilgang til Nødnettet. *NRK*. https://www.nrk.no/norge/it-arbeidere-i-india-har-fortsatt-tilgang-til-nodnettet-1.13452434
Riksrevisjonen. (2018). *Revisjonsrapport for 2018 om Sikring mot dataangrep i Oljedirektoratet* (2018/01015-100). Riksrevisjonen. https://www.riksrevisjonen.no/globalassets/rapporter/no-2019-2020/dataangrepoljedirektoratet.pdf
Riksrevisjonen. (2022). *Slik jobber vi*. Hentet 04.04.2022 fra https://www.riksrevisjonen.no/om-riksrevisjonen/slik-jobber-vi/
ROSGEO. (2021a, 03.08.2021). *Akademik Lazarev completed seismic survey offshore North Sea.* http://smng.com/press-center/news-and-media/320

ROSGEO. (2021b, 22.09.2021). *Akademik Nemchinov commenced seismic survey in North Sea* http://smng.com/press-center/news-and-media/322
Sikkerhetsloven (§1-1). (2018). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/lov/2018-06-01-24/§1-1
Sikkerhetsloven (§1-3). (2018). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/lov/2018-06-01-24/§1-3
Sikkerhetsloven (§1-5). (2018). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). www.lovdata.no. https://lovdata.no/lov/2018-06-01-24/§1-5
Sikkerhetsloven (§5-2). (2019). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). www.lovdata.no. https://lovdata.no/lov/2018-06-01-24/§5-2
Sikkerhetsloven (§7-1). (2018). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/lov/2018-06-01-24/§7-1
Sikkerhetsloven (§8-1). (2018). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). www.lovdata.no. https://lovdata.no/lov/2018-06-01-24/§8-1
Sikkerhetsloven (§8-3). (2018). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/lov/2018-06-01-24/§8-3
Standard Norge. (2012). *Samfunnssikkerhet Beskyttelse mot tilsiktede uønskede handlinger Terminologi* (NS 5830:2012). Standard Norge.
Standard Norge. (2014). *Samfunnssikkerhet Beskyttelse mot tilsiktede uønskede handlinger Krav til sikringsrisikoanalyse* (NS 5832:2014).
Styringsforskriften. (2001). *Forskrift om styring i petroleumsvirksomheten FOR-2001-09-03-1099* Lovdata. https://lovdata.no/dokument/LTI/forskrift/2001-09-03-1099
TGS-NOPEC. (2002, 12.09.2002). *TGS-NOPEC Restructures Long-Term 2D Vessel Capacity* https://www.globenewswire.com/news-release/2002/09/12/1814128/0/en/TGS-NOPEC-Restructures-Long-Term-2D-Vessel-Capacity.html
Tollaksen, T. G. (2022, 10.05.2022). Oljeministeren skeptisk til Halliburton-utflagging. *E24*. https://e24.no/olje-og-energi/i/EarMw3/oljeministeren-skeptisk-til-halliburton-utflagging
Virksomhetsikkerhetsforskriften (§22). (2019). *Forskrift om virksomheters arbeid med forebyggende sikkerhet* (FOR-2018-12-20-2053). www.lovdata.no. https://lovdata.no/forskrift/2018-12-20-2053/§22
Wadel, C. (2016). *Feltarbeid i egen kultur*. Cappelen Damm AS.
Zysk, K. (2018). RUSSLANDS MILITÆRSTRATEGI I ENDRING - Implikasjoner for Nordflåten, nordområdene og Norges strategiske veivalg. *IFS Insights*, *12/2018*, 12.

Vedlegg 1: Intervjuguide for PTIL

Kort innledning og introduksjon

Definerer PTIL statlig etterretning som en trussel mot næringen?

På hvilken måte opplever du at lovverket ivaretar det nasjonale trusselbildet for petroleumssektoren?

På hvilken måte opplever du at sektoransvaret bidrar til å ivareta det nasjonale trusselbildet? (Oppleves det som avklart hvem som har sektoransvar?)

Kan du si noe om hvorvidt du opplever fokuset på statlige sikringstrusler som tilstrekkelig?

Hvordan påvirker det nasjonale trusselbildet PTILs praktiske tilnærming til sikringsarbeid i næringen?

Hvordan defineres PTILs risikoakseptkriterier for sikringstrusler, de spesielt med tanke på vekting av verdier?

På hvilken måte legger PTIL til rette og følger opp at sikringsarbeidet har tilstrekkelig og rett fokus?

PTIL er bemyndiget til å fastsette og håndheve forskrifter. Men gjelder dette også forskrifter tilknyttet §9-3?

Hvordan kan eksempelvis styringsforskriftens §4 eller rammeforskriftens § 17 benyttes for å bedre sikringsrisikostyringen?

Dersom dere har kjennskap til det, på hvilken måte endret oppfølgingen av petroleumslovens §9-3 seg etter at AID tok over fra OED?

I hvilken grad opplever du at PTIL kan gi nye tolkninger av eks. §9-3 for å utvide nedslagsfeltet, og i større grad kunne ivareta trusselbildet fra statlige aktører?

Hvordan opplever du at oljeservicebedrifter forholder seg til sikringstrusler generelt, og etterretning spesielt?

Hvordan følges bedriftene opp i sin tilnærming til sikringstrusler?

Hvordan opplever du at næringen selv ivaretar det trusselbildet PTIL ser?

Vedlegg 2: Intervjuguide for PST

Kort innledning og introduksjon

Opplever du noen begrensinger ved formidlingen av et trusselbilde til næringen?

Hvordan opplever du presisjonen på informasjonen som blir gitt til næringen, gitt at den må nedgraderes?

Hvordan opplever du samarbeidet med næringen? (hvem er til stede i et eventuelt samarbeidsforum?)

Hvordan opplever du at næringen tar til seg informasjonen fra PST?

Kan du si noe om endringer i trusselbildet etter Russlands invasjon av Ukraina?

Vedlegg 3: Intervjuguide for bedriftsinformanter

Kort innledning og introduksjon

Hvor godt kjenner du til PSTs trusselvurdering for petroleumsnæringen?

Hvordan oppfatter du petroleumslovens §9-3 og dens hensikt?

Kjenner du til at statlig etterretning har vært nevnt som trussel i forbindelse med sikringsarbeid i næringen? (Kjenner du til at det er avdekket slike hendelser?)

Hvordan opplever du at operasjon/forretningsdelen av bedriften forholder seg til sikringstrusler, og da spesielt statlig etterretning?

På hvilken måte merket du at PTIL tok over ansvaret for §9-3 i 2013?

På hvilken måte definerer din bedrift trusselbildet for sikringstrusler (hvor involvert er du)?

Hvordan påvirker det nasjonale trusselbildet din bedrifts trusselbilde og tilnærming?

Hvordan defineres bedriftens risikoakseptkriterier, de spesielt med tanke på vekting av verdier?

Hvordan opplever du at operatørselskapene følger opp sikringsarbeidet i bedriften?

På hvilken måte samarbeider petroleumsnæringen om sikringstemaet?