Analysemetodikk i forbindelse med terrorisme

- Bruk eller ikke bruk av sannsynlighet

Master i Samfunnssikkerhet

Institutt for medie-, kultur- og samfunnsfag

Universitetet i Stavanger

Anne Egeli

Våren 2014

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I
SAMFUNNSSIKKERHET

MASTEROPPGAVE

SEMESTER: Våren 2014

FORFATTER: Anne Egeli

VEILEDER: Sissel H. Jore

TITTEL PÅ MASTEROPPGAVE: Analysemetodikk i forbindelse med terror – Bruk eller ikke bruk av sannsynlighet

EMNEORD/STIKKORD: Terrorisme, Security, safety, sikring, tilsiktede handlinger, risiko, risikoanalyse, risikovurdering, sannsynlighet, subjektiv sannsynlighet, usikkerhet, Black Swan, ekspertvurderinger, verdi, trussel, sårbarhet

SIDETALL: 77 (UTEN VEDLEGG)

STAVANGER ……16. juni 2014……

Table of Contents

Sammendrag

Terrorangrepet i New York 11. september 2001, bombingen av regjeringskvartalet og massakren på Utøya 22. juli 2011, samt gisseltakingen på In Amenas gassanlegg i Algerie er blant flere hendelser som har skapt økt fokus på terrorisme og risiko for uønskede tilsiktede handlinger. Dette økte fokuset gjelder også for petroleumsvirksomheten. Petroleumsindustrien utgjør viktig infrastruktur og på grunn av sin høye profil og dets globale operasjoner i kombinasjon med det brede spekteret av trusler, må industrien beskytte seg mot angrep fra terrorister ved å sysselsette sikkerhetsprosedyrer og opprettholde et høyt nivå av sikringsbevissthet (Relf og Stubblefield, 2000). Petroleumsindustrien har velutviklet analysemetodikk når det gjelder ikke-intenderte uønskede hendelser, men det har blitt diskutert om det er behov for spesifikk analysemetodikk for Securityfeltet. Tre standarder for beskyttelse mot tilsiktede handlinger har enten blitt publisert eller påventer godkjenning (Norsk Standard 5830; prNS5831, prNS5832). Det er ulike meninger om hvorvidt det bør tas i bruk egne framgangsmåter for analyse av sikringsrisiko og om sannsynlighet kan brukes eller ikke. Avhandlingen ser dermed på hvordan petroleumssektoren og relevante myndigheter analyserer terrorisme, og i hvilken grad sannsynlighet kan være en del av disse analysene.

For å finne svar på avhandlingens problemstilling ble det benyttet en kvalitativ metode. Dette fordi det var lite forskning på området og fordi jeg ønsket å få en mer grundig og dypere forståelse. Jeg gjennomførte intervjuer med oljeselskaper, konsulentfirma og relevante myndigheter. Flere av disse hadde bakgrunn innenfor Securityfaget, samt noen innenfor risikoanalysefaget. Avhandlingen er preget av en risikobasert tilnærming til Security, og en del av teorien som blir presentert har vært pensum i samfunnssikkerhetstudiet, blant annet er mye hentet fra Terje Aven. Noe teori har også vært nødvendig å hente fra Securityfagfeltet.

Terrorhendelser kan bli betegnet som Black Swans dersom de oppfyller visse kriterier. Det gjelder uforutsigbare hendelser som har svært alvorlige konsekvenser. Det finnes lite historisk data og erfaring, trusselaktøren er ofte rasjonell, kalkulerende, fleksibel, samt tilpasningsdyktig. Dette stiller ekstra store krav til risikostyring og risikoanalyse. Komplekse, usikre og tvetydige risikoer fører til behovet for en annen tilnærming enn hva som er nødvendig for enkle risikoer som har en åpenbar årsakssammenheng og en betydelig mengde empirisk data. Jeg foreslår at et klassisk teknisk-naturvitenskapelig syn og bruk av frekvens-

og statistiskbasert sannsynlighet ikke er egnet. Det kreves en grundigere tilnærming, som vektlegger usikkerhet og kunnskapsgrunnlag. Flere innenfor risikoanalysefaget mener at sannsynlighet kan bli brukt i analysene, såfremt dette gjelder subjektiv og kunnskapsbasert sannsynlighet. Fagfolk innenfor Securityfeltet derimot, mener man ikke kan vurdere sannsynlighet i det hele tatt. Det virker som de ulike fagpersonene legger ulik betydning i begrepet sannsynlighet, og at det dermed skaper store misforståelser. Flere tenker enda på risiko og sannsynlighet innenfor det teknisk-naturvitenskapelige perspektivet. Dermed blir det lett å avskrive enhver bruk av sannsynlighet. Risikoanalysefaget har derimot utviklet seg gjennom mange år, og den bayesianske tilnærmingen til risiko står som et eksempel på denne utviklingen.

Avhandlingens resultater peker på at virksomheter må gjøre en vurdering av egne verdier, trusselaktører som kan være interessert i disse verdiene, deres intensjon, samt kapasitet og hvilke sårbarheter virksomheten har. Det som beskrives i standardene som omhandler tilsiktede handlinger er ment som en framgangsmåte som virksomheter kan ta utgangspunkt i, men som må tilpasses til deres egne behov og preferanser. Det er uenighet hvorvidt egne framgangsmåter for tilsiktede handlinger er hensiktsmessig. Fagfolk innenfor Safetyfeltet mener ulike begreper og ulik framgangsmåte vil gå imot hensikten i ISO 31 000 om en helhetlig risikostyring. Fagfolk innenfor Securityområdet mener fagfeltene er svært ulike og dermed må behandles ulikt. Dette er derimot lettere sagt enn gjort, da virksomheter må forholde seg til flere ulike fagområder, og det må gjøres prioriteringer angående hvor ressurser skal settes inn. Dersom det skal være ulike system og metoder for å tilnærme seg hver av disse fagfeltene vil det kunne skape forvirring. Det kan virke som om den største utfordringen er kompetanse. Hvert fagfelt vet for lite om det andre fagfeltet. Dette skaper uenighet og misforståelser. Det blir dermed viktig å presisere hva som blir lagt i ulike begreper og perspektiver. Begge fagfeltene har kommet med nyttige innspill, og det ene kunne ikke vært foruten det andre.

Avhandlingen konkluderer med at uavhengig av hvilken framgangsmåte som blir brukt, så må risikobildet presenteres på en nøytral måte, dvs. at risikobildet blir delt inn i ulike kategorier som er like for alle fagfelt, for eksempel; lav, moderat, høy eller ekstrem. Slik kan beslutningstakere sammenligne mellom de enkelte og implementere sikringstiltak der hvor risikoen er størst.

Forord

Arbeidet som ligger bak denne masteravhandlingen har vært spennende, men samtidig krevende da jeg har beveget meg inn på to ulike fagområder; Safety og Security. Jeg er utrolig takknemlig for den hjelp jeg har fått under hele prosessen.

Først og fremst vil jeg takke min veileder fra Universitetet i Stavanger, Sissel H. Jore. En like stor takk vil jeg rette til Knut Erik Fotland og Anders Karlsen fra Safetec, samt Stig Sandal fra GDF Suez for godt samarbeid og gode faglige innspill. Jeg vil også takke Roy Stranden og resten av informantene som har vært villige til å dele informasjon slik at man sammen kan gjøre et forsøk på å utvikle mer kompetanse på dette området.

Stavanger, 16. Juni 2014

Anne Egeli

Figurer, tabeller og vedlegg

Terminologi

Begrep	**Definisjon**
Safety	”*Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter” (NOU, 2000).*
Security	*“Sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging”*
Risiko	*”Uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value” (NOU, 2000).*
Risiko i sikringssammenheng	*”Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen” (NS 5830, 2012).* (Aven, 2010:3).
Verdi	*”Ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som forvalter eller drar fordel av ressurser”* (NS 5830, 2012).
Trussel	”Mulig uønsket handling som kan gi negativ konsekvens for sikkerheten til personer eller virksomheter” (NS 5830 2012).
Sårbarhet	*”Manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning”* (NS 5830, 2012).

1 INNLEDNING

1.1 Motivasjon for valg av tema

Mange vestlige land mener at terrorisme utgjør en stor sikringsutfordring (Jore og Njå, 2010). Med sikring menes *"sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging"* (NOU, 2000). Terrorangrepene i New York 11. september 2001, førte til en endret persepsjon av risikoen for tilsiktede hendelser, og flere tiltak ble dermed iverksatt for å forsøke å hindre slike angrep i framtiden (Jore, 2012). Hendelser som blant annet bombingen i regjeringskvartalet og skytingen på Utøya 22. juli 2011, samt gisseltakingen på In Amenas gassfasilitet januar 2013 er hendelser som har understreket dette behovet. Terrorisme i sammenheng med risikobegrepet og Securityfeltet generelt har dermed fått et økende fokus. Med unntak av hendelsen som fant sted 22. juli, er Norge et land med relativ liten historie av terrorisme. De norske myndighetene har likevel beskrevet nødvendigheten av å beskytte kritisk infrastruktur mot tilsiktede handlinger. Risikostyring og risikoanalyse er et viktig verktøy i forebyggingsarbeidet (Jore, 2012). Det økte fokuset på terrorisme og risiko i samfunnet generelt gjelder også for petroleumsvirksomheten (St.meld. Nr.12, 2005-2006). Petroleumsnæringen har alltid hatt behov for beredskap og beskyttelse mot viljestyrte handlinger, men hendelsene som er nevnt ovenfor har gitt temaet ekstra stor oppmerksomhet.

> *"Hendelser i nyere tid både i Norge og internasjonalt er grufulle eksempler på hvor viktig det er at selskapene kjenner trusselbildet og har nødvendige systemer og god beredskap på plass"* - Tilsynsdirektør i Ptil, Finn Carlsen (Midttun, 2013:11).

Ifølge Harel (2012) kan det tenkes at oljebransjen er et attraktivt mål for terrorister. I tillegg påstår Relf og Stubblefield (2000) at voldshandlinger mot oljebransjen eskalerer på verdensbasis. Noen årsaker til dette er ifølge dem at multinasjonale oljeselskap har kontorer rundt omkring i hele verden hvor mange blant annet er lokalisert i områder hvor kjente terroristgrupper hører til og i regioner som er preget av politisk og økonomisk opprør. Som et symbol på velstand og makt vil oljeindustrien ha lett for å bli utsatt for politiske og/eller miljømessige kampanjer. Mange menneskerettighetsgrupper og venstreorienterte geriljasoldater klandrer oljeinntektene for å avle korrupsjon. Gjennom å angripe petroleumselskaper ønsker de å få redusert strømmen av oljepenger og dermed tvinge reformer og/eller velte korrupte regimer. I tillegg til at industrien blir et attraktivt mål for flere

er petroleumsindustrien også svært sårbar for terrorhandlinger og kriminalitet, blant annet fordi avsidesliggende oljefelt og rørledninger kan strekke seg hundrevis av mil og dermed bli vanskelige å forsvare, og fordi offshore installasjoner som på grunn av beliggenhet og avstand fra land kan bli svært vanskelige å beskytte (Harel, 2012 og Relf og Stubblefield, 2000).
Selv om det ikke er utført terrorangrep mot norsk sokkel, og få i verden på generell basis, kan offshore innretninger være aktuelle mål dersom en aktør har intensjon og kapasitet (Arnesen, Bjørgo og Mærli, 2005). En aktør kan ha intensjon om å utføre terrorangrep mot en offshore installasjon på norsk sokkel blant annet fordi olje og gassproduksjon er en viktig kilde til energi og inntekt for Norge selv, i tillegg til at eksport av petroleumsprodukter også har betydning for Europas forsyning.

Et terrorangrep mot oljevirksomhet kan ha katastrofale følger og ramme verdier som mennesker, økonomi, miljø og omdømme. Petroleumsindustrien utgjør viktig infrastruktur og på grunn av sin høye profil og dets globale operasjoner i kombinasjon med det brede spekteret av trusler, må industrien beskytte seg mot angrep fra terrorister ved å sysselsette sikkerhetsprosedyrer og opprettholde et høyt nivå av sikringsbevissthet (Relf og Stubblefield, 2000). Petroleumsindustrien har godt rykte på seg når det gjelder ”*sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter”* (NOU, 2000), og har velutviklet analysemetodikk på dette området. Engen, m.fl., (2013) konkluderer med at HMS-regimet for petroleumsvirksomheten fungerer overveiende godt. Det ble derimot ikke gjort en vurdering av Security, og det er uavklart om det fungerer like godt. Terrorhendelsene som nevnt ovenfor har ført til diskusjoner om behov for spesifikk analysemetodikk for Securityfeltet. En diskusjon som også er tatt opp av forskningsmiljøer rundt om i verden. Det har blitt utviklet noen standarder som omhandler sikring, men som enda ikke har blitt godkjent, og som dermed går under betegnelsen prNS5831 og prNS5832. Sistnevnte beskriver en metodikk for analyse av tilsiktede handlinger, men det er delte meninger i hvilken grad denne bør benyttes eller ikke.

1.2 Problemstilling

Utgangspunktet er at vurdering og analysering av risiko for intenderte handlinger fører til en rekke utfordringer og problemstillinger som skiller seg fra de ikke-intenderte uønskede hendelsene. Det diskuteres hvilken metodikk som bør anvendes og i hvilken grad sannsynligheter kan brukes for å uttrykke usikkerheten. Jeg vil derfor undersøke de ulike analysemetodikkene som blir brukt av oljeselskap og relevante myndigheter og vurdere i

hvilken grad sannsynlighet kan eller bør bli benyttet i disse analysene. På grunn av motivasjon og bakgrunn for valg av tema lyder min problemstilling som følger:

Hvordan analyseres risiko for terror i petroleumssektoren og av relevante myndigheter, og i hvilken grad kan sannsynlighet brukes i disse analysene?

Problemstillingen genererer tre spørsmål:

- Hva er fordelene med bruk av sannsynlighet?
- Hva er ulempene med bruk av sannsynlighet?
- Eksisterer det alternativer, hvis ja hva er styrkene og svakhetene?

For å svare på avhandlingens problemstilling må jeg se på følgende forskningsspørsmål:

- Dagens status: Hvilke analysemetodikk brukes av petroleumsselskap og relevante myndigheter i Norge i dag på Securityfeltet?
- Hva er oljeselskapene og de relevante myndigheter sitt syn på eksisterende metodikk, samt bruk av sannsynlighet?

I tillegg blir det relevant med en presentasjon av informantenes faglige ståsted, som vil finne sted i avhandlingens metodekapittel, se tabell 2.

1.3 Avgrensninger

Security og Safety er to engelske begreper som på norsk ofte oversettes til Sikring og Sikkerhet. De norske og engelske ordene vil bli brukt om hverandre. Begrepet Security innebærer flere ulike typer kriminelle handlinger, som for eksempel: piratvirksomhet, tyveri, sabotasje, spionasje og terrorisme. Avhandlingen har fokus på terrorisme, og Securitybegrepet brukes dermed med forbehold om denne avgrensningen. Jeg har avgrenset meg til bare å innhente empiri fra oljevirksomhet og relevante myndighetsaktører, blant annet fordi oljesektoren har god erfaring med utarbeidelse av risikoanalyser for Safety. Oljebransjen samarbeider likevel med myndighetsaktører som har Security som faglig ståsted, og dermed blir det også nødvendig å ta med de for å få et mest mulig helhetlig bilde. Når det er sagt vil mye av det som blir beskrevet kunne benyttes for andre typer av kriminelle handlinger og for andre virksomheter enn petroleum.

1.4 Oppbygning

Etterfulgt av innledningen tar kapittel to for seg konteksten som besvarelsen tar utgangspunkt i. Videre vil kapittel tre presentere teorier som ses på som nødvendig for å gi et tilstrekkelig svar på problemstillingen. Kapittel fire redegjør for hvilken metode som blir brukt for å gjennomføre innsamlingen av empirisk data. En presentasjon av funn fra intervjuene finner sted i kapittel fem. Drøfting av funn opp mot det teoretiske rammeverket finner sted i kapittel seks. Tilslutt vil besvarelsens redegjør for konklusjoner og tanker om videre forskning.

2 KONTEKST: RELEVANTE MYNDIGHETER OG TILHØRENDE LOVVERK

Det blir i avhandlingens kapittel fem presentert analysemetodikk som brukes av petroleumssektoren og av relevante myndigheter. Derfor vil det være nyttig å se litt på hvem disse myndighetsaktørene er. Gjennomgangen starter med tre myndigheter som har et særskilt ansvar for petroleumssektoren. Noen av aktørene nedenfor er ikke representert i denne avhandlingen, dette gjelder Olje- og Energidepartementet, Norsk olje og gass, Politidirektoratet og E-tjenesten. Årsakene til dette er en av følgende:

- At de ikke hadde mulighet til å stille til intervju.
- At jeg på grunn av tidspress måtte velge de myndighetene jeg mente var mest relevant.

Olje og Energi departementet (OED)

OED har det overordnede ansvaret for petroleumsvirksomheten på norsk kontinentalsokkel.

Petroleumstilsynet (PTIL)

I 2004 ble oljedirektoratet delt inn i to organ; Oljedirektoratet (OD) og Petroleumstilsynet (Ptil). Formålet var å skille ressursforvaltning og forvaltning av sikkerhet innen petroleumssektoren. Petroleumstilsynet er underlagt Arbeidsdepartementet og har tilsyns- og regelverksansvar for helse, miljø og sikkerhet både på land og ved offshorebaserte anlegg (St. Meld. Nr. 22, 2007-2008). Petroleumsloven har en alminnelig bestemmelse om beredskap § 9-2, i tillegg ble det i 2013 opprettet og delegert til Ptil en spesifikk paragraf for sikring, § 9-3 - Beredskap mot bevisste anslag. Paragrafens første del lyder som følger:

> *"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."*

Det er ikke gitt noen utdypende forskrifter eller bestemmelser spesielt med hjemmel i §9-3, men denne paragrafen må ses i sammenheng med forskriftene om helse, miljø og sikkerhet – Aktivitetsforskriften, innretningsforskriften, rammeforskriften, styringsforskriften, teknisk og operasjonell forskrift - som er hjemlet i Petroleumsloven (1996) og retningslinjer fra norsk olje og gass. I Petroleumstilsynets HMS-regelverk blir aktørene pålagt å analysere sin egen

virksomhet. De må kartlegge hvilke farlige situasjoner som kan oppstå og utvikle seg, samt hvilke konsekvenser ulike scenarioer kan gi.

Norsk Olje og Gass

Norsk olje og gass er en interesse- og arbeidsgiverorganisasjon for petroleumsselskaper som ble etablert i 1988. De arbeider blant annet med å utvikle retningslinjer når det gjelder både sikkerhet og sikring. Retningslinje 091 - for sikring av forsyninger og materiell i olje- og gassindustrien (Norsk olje og gass, 2003) vil være relevant. Denne retningslinjen inneholder blant annet anbefalinger om hvordan sikringsarbeidet skal organiseres. Formålet med retningslinjen er å oppnå en samordnet praktisering av virksomheters krav til sikring av forsyninger og materiell til oljeindustrien. Den skal bidra til å legge til rette for en robust og tilfredsstillende grunnsikring ved normaltilstand og gi råd ved behov når det oppstår endringer i sikringsnivået. Rettsreglene er ikke formelle og bindende, men utgjør anbefalinger, råd og veiledning for hvordan man kan oppnå et tilfredsstillende sikkerhet- og sikringsnivå (Norsk olje og gass, 2014). Norsk olje og gass har etablert et sikringsnettverk, hvor alle operatørene på sokkelen møtes, og hvor stort fokus blir lagt på hvilke utfordringer intenderte handlinger utgjør for petroleumssektoren (Seglem og Myrset, 2013).[1]

Direktoratet for samfunnssikkerhet og beredskap

Direktoratet for Samfunnssikkerhet og beredskap (DSB) er et direktorat som er direkte underlagt Justisdepartementet. Deres primær oppdrag er å understøtte Justisdepartementets samordningsansvar på tvers av alle departementenes ansvarsområde. Det betyr blant annet at de har ansvar for å framskaffe kunnskaps- og beslutningsgrunnlag for politikkutforming i Norge, når det gjelder samfunnssikkerhet og beredskap. DSB skal ha en generell oversikt over risiko og sårbarhet i samfunnet. De skal være pådrivere i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser (Regjeringen.no).[2] DSB har også blitt pålagt, av Justisdepartementet, å ta for seg tilsiktede hendelser. Justisdepartementet er opptatt av at DSB utfører analyser av sårbarhet i det moderne samfunnet, sårbarhet mot kjente risikofenomen og trusler, men også mot ukjente hendelser.

[1] www.aftenbladet.no/energi/--Oljeselskapene-trener-lite-pa-terror-3111252.html#.U51
[2] http://www.regjeringen.no/nb/dep/jd/dep/underliggende-etater/direktoratet-for-samfunnssikkerhet-og-be.html?id=279674

Nasjonal sikkerhetsmyndighet (NSM)

NSM er en forebyggende sikkerhetstjeneste underlagt Forsvarsdepartementet. Deres rolle er å ha oversikt over ulike samfunnsverdier og føre tilsyn med virksomheter som omfattes av sikkerhetsloven, som er det regelverket de forvalter (Sikkerhetsloven, 1998). I utgangspunktet gjelder dette forvaltningsorganer, og dermed ikke petroleumssektoren. Formålet med loven er å beskytte skjermingsverdige objekter og informasjon mot tilsiktede handlinger som terrorisme. Skjermingsverdige objekter og informasjon må beskyttes da de har betydning for nasjonens sikkerhet (Stålesen, 2011). NSM har utarbeidet en forskrift § 17 - om objektsikkerhet som er hjemlet i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven, 1998), som innebærer at hvert departement skal avgjøre hvilke virksomheter innenfor sitt myndighetsområde som innehar skjermingsverdige objekter. Da skal sikkerhetsloven gjelde også for dem. Slik kan likevel objekter innen petroleumsvirksomheten bli regulert i henhold til loven. Det har vært diskutert mellom Nasjonal sikkerhetsmyndighet (NSM) og Olje- og energidepartementet (OED) om olje- og gassinstallasjoner bør være skjermingsverdige objekter eller ikke. Olje- og energidepartementet har ikke utpekt disse som et slikt objekt og dermed ikke anerkjent at loven gjelder for dem (Helgesen, 2013). Det vil si at de mener at ingen olje-og gass installasjoner trenger ekstra terrorbeskyttelse. NSM er skeptiske til at OED ikke mener det trengs å følge sikkerhetsloven på dette feltet *"Etter vår mening er landets olje- og gassinstallasjoner helt klart vital nasjonal infrastruktur som bør sikres"* - Avdelingsleder Carsten Rapp i NSM (Helgesen, 2013).[3]

Politidirektoratet (POD)

Politidirektoratet (POD) er underlagt Justisdepartementet og er en sentral aktør for å planlegge og å sikre samfunnsviktig infrastruktur og andre skjermingsverdige objekter som kan være utsatt for en trussel. Når det gjelder terror skal hovedfokuset ligge på forebygging og risikobasert politiarbeid. Et av deres mål er å forsøke å avverge at terrorister planlegger eller på annen måte støtter terroraksjoner i eller utenfor Norge (Stålesen, 2011).

Politiets sikkerhetstjeneste (PST)

PST er underlagt justisdepartementet og er en viktig sikringsrådgivende bidragsyter som har fokus på forebygging av blant annet terrorhandlinger. PST har ansvar for å utarbeide strategiske analyser som innebærer graderte og offentlige trusselvurderinger. Dette skal øke

[3] www.tu.no/petroleum/2013/09/02/ingen-olje--og-gassinstallasjoner-trenger-ekstra-terrorbeskyttelse

virksomheters innsikt og forståelse for utviklingstrekkene i det nasjonale trusselbildet (NTB). Ved å kjenne til det nasjonale trusselbildet kan virksomheter etablere best mulig sikringstiltak (pst.no).[4] PST bistår også blant annet ulike aktører i oljenæringen med mer konkrete og spesifikke trusselvurderinger. Disse vurderingene blir brukt i risikoanalyser av kriminelle handlinger; herunder også terrorisme. Deres arbeidsoppgaver er hjemlet i Politiloven § 6 som omhandler trusselvurderinger og sikkerhetsråd (Politiloven:1995;2013). Videre er all deres virksomhet knyttet opp mot sikkerhetsloven, med forskrifter.

Etterretningstjenesten (E-tjenesten)

E-tjenesten er Norges sivile og militære utenlands etterretningstjeneste, og har koordinerende og rådgivende ansvar for all etterretningsvirksomhet i Forsvaret. PST og E-tjenesten samarbeider tett og har en felles analyseenhet som blant annet ser på transnasjonale trusler rettet mot Norge og norske interesser i og utenfor Norge (St.meld. Nr. 29, 2011-2012). E-tjenestens rammer er regulert i Lov om Etterretningstjenesten (1998).

[4] www.pst.no/om/

3 TEORI

3.1 Terrorisme

Terrorisme er en tilsiktet handling. Utøvelse av terrorhandlinger er en alvorlig kriminalitet med forgreininger som ofte går på tvers av landegrenser (Pst.no).[5] Begrepet er omdiskutert, mange har en vag antakelse om hva terrorisme er, men mangler en mer klar og presis definisjon (Hoffman, 2006). Vanskelighetene med å definere begrepet har vært et tema i mange tiår for blant annet FN og for nasjonale og internasjonale organer som jobber med terrorbekjempelse (Schmid, 2004 i Jore, 2012). Man kan se en økende konsensus om hva begrepet innebærer blant både forskere og myndigheter (Bjørgo, 2005). Hoffman (2006) diskuterer ulike definisjoner og mener mange av dem er mangelfulle. Han nevner derimot Oxford English Dictionary (OED) sin definisjon som fokuserer på terroristen mer enn selve handlingen i seg selv, og mener denne skiller seg ut som mer tilfredsstillende av årsaker som blir beskrevet under:

> *"As a political term: a. Applied to the Jacobins and their agents and partisans in the French Revolution, esp. to those connected with the Revolutionary tribunals during the "Reign of Terror," b. Any one who attempts to further his views by a system of coercive intimidation; spec, applied to members of one of the extreme revolutionary societies in Russia"- (*Hoffman, 2006:2).

Hoffman (2006) mener denne definisjonen er mer hjelpsom fordi den introduserer leseren til forestillingen om terrorisme som et politisk konsept. Dette påstår han er helt avgjørende for å forstå en terrorist sin motivasjon, og er en viktig egenskap for å skille terrorisme fra andre typer av tilsiktede handlinger. Han hevder videre at i den mest aksepterte og moderne bruken av begrepet, så er terrorisme fundamentalt og iboende politisk. Det handler også om streben etter og bruk av makt for å oppnå politisk endring. Terrorisme innebærer vold og trussel om vold for å oppnå et politisk mål. OED har utvidet definisjonen, ved å legge til følgende:

> "Anyone *who attempts to further his views by a system of coercive intimidation"*
>
> (Hoffman, 2006:3).

[5] http://www.pst.no/trusler/terrorisme/

Dette påpeker en annen fundamental karakteristikk ved terrorisme, nemlig at det er en planlagt, kalkulert og systematisk handling. Sikkerhetslovens definisjon av terrorhandlinger dekker mye av det som står ovenfor:

> *"ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer og eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål" (Sikkerhetsloven, 1998).*

Denne avhandlingen tar utgangspunkt i sikkerhetslovens definisjon i og med at den inkluderer mange av aspektene som ligger i begrepet terrorisme, den kommer fra en pålitelig kilde og er en lov som er kjent av samtlige informanter som er representert i denne besvarelsen.

Ifølge Bjørgo (2005) er terrorisme overlagt vold mot sivile for å skape psykologisk frykt blant folk utover de som er direkte utsatt. I tillegg til frykt fører det til at mennesker kan føle seg sårbare, nervøse, forvirret, usikre og hjelpeløse. Jore (2012) påstår at enkelte mennesker vil føle en form for frykt, selv om flere ser på sannsynligheten som liten. Konsekvenser av et terrorangrep kan være svært alvorlige; tap og skade av liv, materielle skader, samt økonomiske tap. Selv om konsekvensene kan være svært ødeleggende, er det ikke den faktiske skaden eller drepingen som er selve formålet. Ødeleggelsen er ifølge Bjørgo (2005) ment for å oppnå andre mål. Likevel er ikke valg av målgruppe vilkårlig. Det er strategiske mål som er relatert til hvem, hvor og når de skal slå til. Disse instrumentelle intensjonene gjør at det er verdt å benytte seg av risikostyringsprinsippene og metodikk for analysering av trusselen som finnes (Jore, 2012). Terrorisme har etter terrorangrepene 11. september 2001 blitt sett på som en katastrofal risiko som truer demokrati, nasjonal sikkerhet og kritisk infrastruktur. Dermed må altså samfunnet beskyttes ved å forebygge at terrorhandlinger gjennomføres og å forberede seg på angrepene dersom de likevel skulle oppstå

Ifølge Relf og Stubblefield (2000) kan terrorister deles inn i tre ulike kategorier:

- Rasjonelle terrorister som undersøker mål og muligheter for å avgjøre hva som vil fremme en sak. En kost-nyttevurdering blir utført for å evaluere omfang av et angrep og dets potensiale for å oppnå et intendert mål.
- Psykologiske terrorister som er motivert av utilfredshet med livet og personlige prestasjoner. De skiller ikke mellom rett og galt; syn utenfra deres gruppe er fullstendig grunnløs og er oppfattet som å være basert på onde motiver. Det er ingen nåde eller tvetydighet under et angrep.

- Terrorister som er motivert av kultur, nasjonalisme, religion, samt rase er spesielt dedikert til deres sak. Mange mennesker er ikke fullstendig klar over graden kultur kan motivere oppførselen og den potensielle faren disse gruppene utgjør. Trusler mot en kultur som en terrorist identifiserer seg med kan trigge ekstrem aggresjon. Terroristangrep som ellers ville blitt sett på som ekstraordinær handling i desperasjon, blir i den kulturelt motiverte terroristens sinn sett på mer som en plikt.

Relf og Stubblefield (2000) påpeker også muligheten av at det kan være "insidere" som ønsker å sabotere eller eventuelt utføre et terrorangrep.

Historikk: Terror mot oljevirksomhet

Ifølge globale undersøkelser blir petroleumssektoren sjelden angrepet (Kjøk og Lia, 2001). Kjøk og Lia har utarbeidet en rapport på vegne av Forsvarets forskningsinstitutt hvor de gjør en undersøkelse av terror- og opprørsangrep på petroleuminfrastruktur fra 1968 – 1999. De har i dette arbeidet brukt databasen ITERATE,[6] hvor de har samlet 262 tilfeller av terror- og opprørsangrep eller angrepsforsøk mot petroleuminfrastruktur. I rapporten til Kjøk og Lia (2001) hevdes det at nye Security-trusler kan dukke opp på kort varsel til tross for de få tilfellene som er registrert. Et nylig eksempel som støtter deres påstand er gisseltakingen på In Amenas gassanlegg i Algerie januar 2013.

Offshore

Det har vært få suksessfulle terrorangrep på offshore oljeplattformer til nå. Kjøk og Lia (2001) har bare registrert noen få angrep, hvor to av dem inntraff i Nigeria. I juni 1999 ble en oljeplattform i Harcourt havnen i Niger-Delta regionen stormet av fire tungt bevæpnede ungdommer. Plattformen ble påført skader, et helikopter ble kapret og tre ansatte ble kidnappet. I august 1999 ble tre ansatte kidnappet fra en annen oljeplattform i regionen, men uten å komme til skade. Det blir ifølge Kjøk og Lia (2001) sett på som et worst-case scenario for Norsk oljeproduksjon dersom en oljeplattform i Nordsjøen skulle bli kapret av en terrorist. Nigeria er så vidt Kjøk og Lia (2001) vet det eneste landet som har opplevd at en offshore petroleumplattform har blitt kapret. Kapringen fant sted i juli 2000, og er dermed ikke med i deres statistiske undersøkelse. 35 bevæpnede unge menn i Nigeria brukte en robåt for og nå to oljeplattformer utenfor kysten. De klarte å ombordstige riggene og ta 165 oljearbeidere som gissel. De krevde at selskapet Shell ansatte flere personer fra Nigeria, og at de måtte betale et

[6] ITERATE står for "Attributes of Terrorist Events," og er en omfattende database av internasjonal terrorisme som dekker perioden 1922 – 1999. Datasamlingen før 1968 er mindre systematisk og består bare av 14 av de 262 samlede tilfellene.

gebyr til det lokale samfunnet for å utnytte deres petroleumsressurser. Shell inngikk en avtale med gisseltakerne og gislene ble dermed frigjort etter fire dager. Det har ifølge Kashubsky (2011)[7] også blitt utført to terrorangrep mot offshore installasjoner i den Persiske Gulf, hvor selvmordsbåter er tatt i bruk.

3.2 Safety og Security

Sikkerhet er et begrep som kan ha flere ulike betydninger i ulike situasjoner. De engelskspråklige betegnelsene ”Safety” og ”Security” blir ofte brukt for å skille mellom to aspekter av sikkerhet (Rausand og Utne, 2009; Piètre-Cambacédès og Chaudet, 2010). Det framkommer av Stålesen (2011) at flere teoretikere er enige om at en tydelig forklaring og definisjon av Safety og Security er viktig for å unngå misforståelser. For å svare på avhandlingens problemstilling blir det dermed sentralt å forklare forskjellen mellom disse begrepene. NOU (2000:24) definerer begrepene slik som beskrevet nedenfor:

- **Safety**: ”*Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter”*
- **Security:** *“Sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging”*

Som man ser ligger forskjellen i om skaden er påført med vilje (tilsiktet/villet) eller ikke (utilsiktet). Eksempler på utilsiktede hendelser er naturkatastrofer og tekniske svikt. Eksempler på tilsiktede handlinger er sabotasje og terrorisme. Ifølge Rausand og Utne (2009) kan man gjerne oversette Safety til trygghet og Security til sikring. Securityregimet står ifølge Stålesen (2011) overfor andre risikostyringsutfordringer enn Safetyregimet og de intenderte handlingene vil kreve andre styringsmekanismer. Risikoanalyse er en del av risikostyringsprosessen, det vil dermed være andre utfordringer i en analysesammenheng for sikringsrisiko. Albrechtsen (2003) har sammenlignet Safety og Security hvor han har et fokus på årsaker, trusler og farer, tap, omgivelser, relevans, samt usikkerhet. Han påpeker at det er en likhet mellom dem ved at begge begrepene tar utgangspunkt i et ønske om beskyttelse mot farer og trusler slik at man kan være trygge og sikre, men hevder at det er flere forskjeller enn likheter.

[7] http://ro.uow.edu.au/thesis /3662/

Tabell 1: Forskjellen mellom Security og Safety (Albrechtsen, 2003:13).

	Security	**Safety**
Causes	An incident is most often a result of one person or a groups's will	An incident is most often a result of human behaviour in combinition with the environment
Causes	Often planned actions	Often unplanned
Causes	Criminal acts	Criminal acts (Working environment Act)
Causes	Mainly malicious acts	Seldom, if ever, malicious
Causes	Mainly deliberate acts with a wish of wanted output/consequence of the act	Mainly deliberate acts without a wish of a wanted output and accidental incidents
Threats/Hazards	External and internal human threats	Internal human threats
Threats/Hazards	Threats are not always observable, tangible and proximate	Hazards are observable, tangible and proximate
Loss	Loss is mainly related to physical assets and information	Loss is related to human injuries/death and reliability o findustrial assets
Surrounding	Reflects the state of society through its structures, economical situation, lawabidingness and moral	Includes physical and environmental conditions – not only humans and society
Relevance	Relevant for a wide range of companies	More relevant for the industry and transporting sector
Uncertainty	High degree of uncertainty and low degree of knowledge about threats within	

Flere av karakteristikkene i forbindelse med Security gjør at analyseprosessen fort kan bli litt mer utfordrende. Dermed blir det vanskelig å gjøre en analyse på samme måte som for Safety-hendelser. Dette har ifølge (Aven, 2013) blant annet bakgrunn i:

- At det er viljestyrte og planlagte handlinger hvor trusselaktøren har en intensjon og ønsker å oppnå et mål. Trusselaktørene er rasjonelle, kalkulerende, fleksible, samt tilpasningsdyktige individer.
- Hendelsene er preget av lite gjentakelse, det er lite empirisk data, og ved hvert tilfelle forsøker trusselaktøren å gjøre noe nytt med det formål om å skremme og overraske. Dermed er trusselen preget av stor grad av uforutsigbarhet.

3.3 Black Swan teorien

"Black Swan" var opprinnelig en metafor for det helt umulige eller helt usannsynlige, helt til en oppdagelsesreisende fant ut at det levde sorte svaner vest i Australia. Nassim N. Taleb utviklet på bakgrunn av dette en teori hvor han beskriver tre egenskaper som må være oppfylt for at hendelsen kan betegnes som en Black Swan hendelse (Taleb i Aven og Krohn, 2013).

1) Det må være en uforutsett hendelse som kommer som en overraskelse og som dermed er preget av mye usikkerhet
2) Konsekvensene må være høye og alvorlige
3) Det må i etterkant av hendelsen kunne være mulig å se hvordan hendelsen kunne inntreffe.

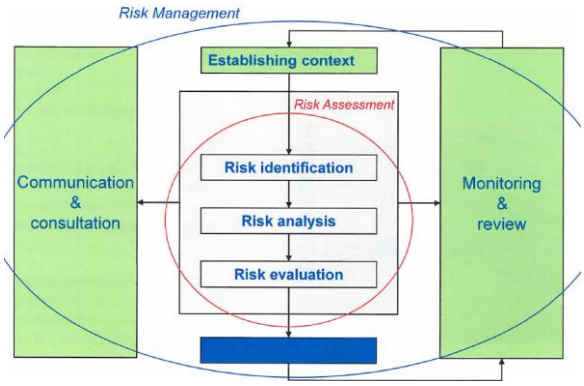
Ikke alle kriminelle handlinger kan defineres som "sorte svaner." Noen, som terrorangrepene i USA 11. September 2001 og massakren på Utøya 22. Juli 2011 kan sies å oppfylle disse kravene og dermed betegnes som Black Swan hendelser. Bombeangrepet på regjeringskvartalet samme dag som hendelsen på Utøya derimot var på mange måter tenkelig ettersom det var ulike faresignaler på forhånd. En kan da stille spørsmålet hvorfor det da ikke var satt inn flere sikringstiltak. Ifølge Aven har hendelser som blir ansett som bestående av svært lav sannsynlighet for å oppstå, ofte en tendens til å bli bli ignorert eller neglisjert i en risikovurdering eller risikostyringsprosess fordi en ikke er villig til å investere tid og penger i å beskytte seg mot slike (Aven og Krohn 2013). For å vurdere, og forsøke å styre og kontrollere risiko for uforutsette hendelser, hevder Aven og Krohn (2013:2) at det er behov for å se utover sannsynlighet og ta i bruk et bredere risikoperspektiv.

> "*We also need methods that can be used for the practical assessment and management of these types of events and situations. This is a huge research challange"* (Aven og Krohn 2013:2).

For å forstå hva som menes med et bredere perspektiv må man først se på risikostyringsprosessen på generell basis, samt tilnærming til risiko med et tradisjonelt perspektiv.

3.4 Risikostyringsprosessen i Safety kontekst

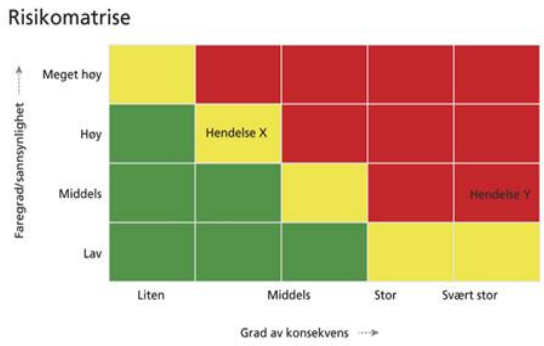
Risikostyringsprosessen handler om å forebygge eller redusere konsekvenser av en uønsket hendelse, identifisert av en risikovurdering gjennom å velge hensiktsmessige tiltak (Aven og Renn, 2010). Oppgaven med å velge tiltak er lokalisert hos beslutningstaker. Risikostyringsregimet bygger altså på antakelsen om at en organisasjon eller virksomhet har den nødvendige kompetansen for å vite hvilken type risiko virksomheten kan bli utsatt for, slik at ideelle beslutninger kan bli tatt for å oppnå et optimalt sikkerhetsnivå (Jore og Moen, 2014). Hovedutfordringen med risikostyring er tvetydigheten som ofte kan være framtredende. Tvetydigheten kan være relatert til risikovurderingens relevans, mening og implikasjon. Den kan være relatert til hvilke verdier som ønskes beskyttet, hvor man må vurdere hvilken risiko som er akseptabel, tolererbar eller uakseptabel. Tolererbar risiko kommer mellom akseptabel og uakseptabel risiko, og her må det gjøres videre vurdering og prioritering (Aven og Renn, 2010). Også i en vurdering av sikringsrisko må organisasjoner avgjøre om risikoen er så alvorlig at det er behov for å implementere tiltak eller ikke. Generelt gir ikke risikostyringstilnærmingen mye veiledning angående hvordan beslutninger skal fattes, og i hvilken grad risikoen er akseptabel eller ikke (Jore og Moen, 2014). Balansen mellom kost-nytte har ofte avgjørende betydning for i hvilken grad risikoreduserende tiltak er berettiget eller ikke (Aven & Renn, 2010). Jore og Moen (2014) hevder at det blir enda mer komplisert når det gjelder sikring, blant annet fordi det er knyttet høy grad av usikkerhet til slik type risiko. Det politiske aspektet- og håndteringen av risikoen er preget av stor grad av tvetydighet, samt at de fleste organisasjoner mangler kunnskap om Security og virkningen av sikringstiltak. I tillegg er de fleste vurderinger og beslutninger angående Security klassifisert. Organisasjoner i en beslutningskontekst vil ofte ha mangel på informasjon om hvordan andre organisasjoner har ordnet deres sikringssystem. Siden risikostyringstilnærmingen ikke er en praktisk veiledning og ikke gir noen klare retningslinjer for hva et hensiktsmessig sikringsnivå, antar Jore og Moen (2014) at mange organisasjoner i Norge sliter med å tilpasse seg dette nye regime. Nedenfor vises til en modell av risikostyringsprosessen slik den blir presentert i ISO 31000, en vel anerkjent standard innenfor risikostyringsfaget.



Figur 1: Risikostyringsprosessen (ISO 31000).

3.4.1 Tradisjonell klassisk tilnærming til risiko

Den tradisjonelle klassiske måten å framstille risiko på i en analysesammenheng er en teknisk-naturvitenskapelig tenkemåte der risiko blir estimert ut fra sannsynlighet x konsekvens (Aven og Renn, 2010). Risikoanalyse er et steg i risikostyringsprosessen hvor en skal identifisere og analysere initierende hendelser, gjøre en årsaksanalyse, konsekvens- og sårbarhetsanalyse. Analysen har som formål å skape innsikt om risiko i forhold til en gitt aktivitet eller et gitt system. Usikkerhet blir kvantifisert og behandlet ved bruk av estimater, og modeller blir lagt for å angi hva som er riktig sannsynlighet og forventning. En kommer frem til ulike risikotall eller risikokategorier som beskriver risikoen (Aven og Renn, 2010). Risikomatrise brukes i denne sammenheng ofte som en presentasjon av risikobildet, slik at man lettere skal kunne prioritere risikoreduserende tiltak (Rausand og Utne, 2009).

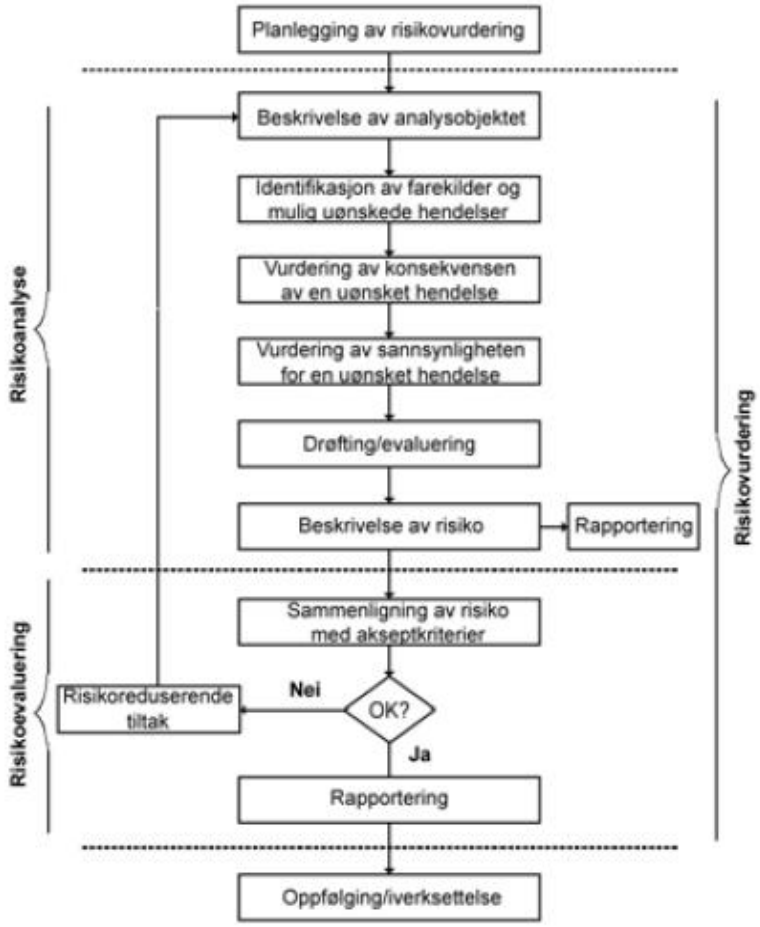


Figur 2: Eksempel på risikomatrise (St.meld. Nr.15, 2011-2012).[8]

Figuren ovenfor er et eksempel på en risikomatrise, hvor risikobilde basert på sannsynlighet x konsekvens fremstilles. Rødt område er uakseptabelt der produksjonen må stanse øyeblikkelig dersom tiltak ikke iverksettes. Grønt område er akseptabel risiko der tiltak ikke nødvendigvis

[8] http://www.regjeringen.no/nb/dep/oed/dok/regpubl/stmeld/2011-2012/meld-st-15-20112012/5.html?id=676544

må implementeres. Gult område befinner seg mellom disse absolutte skillene og nærmere vurdering må gjøres (Rausand og Utne, 2009). Matrisen fargelegges basert på hvilke akseptkriterier en virksomhet har for risiko. For risikoaverse vil det være flere røde og gule områder. For risikovillige vil det være mer grønne og gule områder.



Figur 3: Forenklet figur av risikoanalyseprosessen (NS 5814).

3.4.2 En bayesiansk tilnærming til risiko

Innenfor risikoanalyse og risikostyring har fokus tidligere vært på teknisk-naturvitenskapelig tilnærming til risiko. Fagmiljøet har de senere årene lagt til grunn et bredere perspektiv fordi førstnevnte syn er for smalt, ved at risiko blir beskrevet så klart og strengt. Mange forskere er pådrivere for alternative semi-kvantitative eller kvalitative metoder som fokuserer på

sårbarhet, fleksibilitet, resiliens, samt robusthet (Jore og Njå, 2010). Flere forskere mener at nye metoder må til for å analysere terrortrussel eller videreutvikle de allerede eksisterende metodene som finnes innenfor risikostyringsfeltet (Jore, 2012; Leveson, 2004). Dette fordi terrortrussel ikke kan behandles på samme måte som tekniske svikt. Jore og Njå (2010) anbefaler å ha en Bayesiansk tilnærming til terrorisme i en analysesammenheng. Ifølge dette perspektivet er risiko bare en presentasjon av noen sin vurdering av usikkerhet. I motsetning til den teknisk-naturvitenskapelige tilnærmingen, er all snakk om sannsynlighet betinget av analysegruppens bakgrunnskunnskap. Bakgrunnskunnskap må derfor alltid bli gransket siden det gir grunnlag for evalueringen (Aven, 2013). Antakelsen bak tilnærmingen er at risikoanalysen vil utgjøre grunnlag for diskusjon og debatt omkring sikring og ikke en presentasjon av sannheten. Aven (2013) hevder at risikokonseptet ikke bør begrenses til bare sannsynlighet, da hans definisjon av risiko anses å være litt bredere og mer fleksibelt:

> *"Risk refers to uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value" (Aven og Renn, 2010:3).*

Dersom en skal benytte seg av Safetymetodikk på Securityområdet vil risiko assosiert med terror ifølge Aven og Renn (2010) referere til usikkerhet om og alvorligheten av konsekvensene av angrepet. I analysen beskrives risikoen og usikkerhet uttrykkes (Aven og Renn, 2010). Man kan ifølge Aven (2013) kunne bruke kunnskapsbasert-, subjektiv sannsynlighet for å uttrykke usikkerheten ved at en er opptatt av å beskrive og redegjør for bakgrunnsinformasjonen som sannsynlighetene bygger på. Slik vil flere aspekter bli fanget opp i analysen. Aven og Krohn (2013) foreslår noen ideer basert på fire grunnleggende pilarer, for hvordan man bør tenke i denne konteksten:

- En passende risikokategorisering for forståelse, vurdering og styring av risiko som er i tråd med ideene.
- Grunnleggende teori, prinsipper og metoder for risikovurdering og styring i tråd med denne kategoriseringen, som dekker for eksempel prinsipper for behandling av usikkerhet slik som forsiktighetsprinsippet.[9]
- Konsepter og ideer fra kvalitetsstyring relatert til ulike typer variasjon og som understreker viktigheten av kontinuerlig forbedring

[9] Forsiktighetsprinsippet er en grunnleggende norm innenfor risikostyring som sier at forsiktighet skal være det ledende prinsipp når det er knyttet usikkerhet til hva som er konsekvensene (Aven, 2007).

- Konseptet om Collective Mindfulness inkluderes i studiene om HRO-teorien,[10] og beskriver en mental tilstedeværelse for få en økt forståelse, og i større grad ha mulighet til å oppdage uforutsette risiko. Mindfulnessbegrepet blir dermed et nyttig rammeverk i arbeid med forebygging av terror. Begrepet inkluderer punktene nedenfor:
    - *Opptatthet av feil:* For å få til en suksessfull risikoanalyse, må listen av scenarioer studeres og en sjekk må bli utført i forhold til om midler/tiltak er iverksatt, slik at de uønskede utfallene som beskrives i scenarioene kan unngås. Identifikasjon av scenarioer er et grunnleggende steg i alle risikovurderinger. Å være sensitiv til signaler om farer og ulykker er i tråd med det nye risikoperspektivet som har fokus på uforutsette og overraskende hendelser. En beskrivelse av risiko i et sannsynlighetsbasert risikoperspektiv vil ikke være like sensitiv til forandringer i kunnskap.
    - *Motstand mot forenkling:* Dette betyr at vi ikke bør basere bedømmelsen av risiko på enkle verktøy som sannsynlighet x konsekvens. Dette gjøres ofte ved fremstilling av risikobildet i risikomatriser. Risikomatriser kan være en måte å starte en vurdering på, men er ikke tilstrekkelig for å få et risikobilde med kvalitet. Forenklinger kan føre til blindsoner, slik at sannsynligheten for overraskelser øker.
    - *Sensitivitet for operasjoner:* Det er viktig å være sensitiv til hva som skjer gjennom analyseprosessen, for eksempel om ekspertene som er med i analyseprosessen er preget av bias,[11] om det er maktspill ved at noen kommer til og ikke andre, slik at risikoen dermed kan bli vurdert på en mest mulig nøytral måte. Videre må det undersøkes om informasjonen som framkommer er troverdig og hvilken grad av usikkerhet som forbindes med informasjonen.
    - *Engasjement for resiliens:* Dette handler blant annet om hvordan man kan møte trusler og usikkerhet. Collective Mindfulness gjør at en er preget av forventninger som handler om forutsigelse og forebygging av potensielle farer før de inntreffer.

[10] High reliable organization (HRO) teorien ble utviklet etter detaljerte studier av pålitelige organisasjoner som klarer å forebygge ulykker eller håndtere dem om de oppstår. Ifølge teorien vil god planlegging gi et sikrere system og en sikrere organisasjon (Rausand og Utne, 2009).
[11] Systematiske feilvurderinger (Njå, m.fl, 1998).

- *Respekt for ekspertise:* En ekspert er en person som har mye kunnskap på sitt fagområde, men ikke nødvendigvis på andre. Det er viktig at det er eksperter representert i analyseprosessen på alle områder.

3.5 Sannsynlighet og usikkerhet

Som nevnt ovenfor er terrorisme preget av svært mye usikkerhet. Både på grunn av trusselaktøren som har en intensjon og kapasitet, som er tilpasningsdyktig og fleksibel, samt på grunn av mangel på historisk data og erfaring. Det er viktig å være bevisst på dette slik at man i analyseprosessen kan ta hensyn til denne usikkerheten. Aven (2007) mener at ledere er i stand til å forholde seg til denne usikkerheten, men at problemet ligger i at analytikere ikke legger stor nok vekt på usikkerheter og at presentasjonsformen av analyseresultatene ikke har vært godt nok gjennomtenkt. Usikkerhetsvurderinger kan ofte være mangelfulle på grunn av mangelfull forståelse av helheten i problemstillingen blant analytikere og andre fagpersoner. Dermed er utfordringen ifølge Aven (2007) å presentere usikkerhet på en hensiktsmessig måte, slik at beslutningstakere får best mulig underlag for sine beslutninger.
Ifølge Flage og Aven (2009) kan en benytte seg av tre indikatorer når en skal vurdere usikkerhetene i analysene

- Tilgang på relevante data og erfaringer
- Forståelse av hendelsen som analyseres
- Enighet blant ekspertene som deltar i risikoanalysen

Aven og Renn (2010) viser til et skille mellom to ulike kategorier av usikkerhet og tilhørende måte å sette sannsynlighet:

3.5.1 Aleatorisk usikkerhet og frekvenstolket sannsynlighet

Aleatorisk usikkerhet er en stokastisk usikkerhet og reflekterer tilfeldige variasjoner i en populasjon, forekomst av hendelser og utvalgets representativitet. Den Aleatoriske usikkerheten reflekteres ifølge Aven og Renn (2010) som en relativ frekvenstolket sannsynlighet, hvor man kan uttrykke brøkdelen av ganger en hendelse inntreffer når en vurderer en uendelig populasjon av lignende situasjoner eller scenarioer. Aven (2013) betegner denne sannsynligheten $P_f(\mathrm{A})$. Siden risikoen for terror må baseres på kvalitativ kunnskap og ikke statistikk er den aleatoriske usikkerheten ikke særlig relevant.

3.5.2 Epistemisk usikkerhet og subjektiv sannsynlighet

Epistemisk usikkerhet oppstår på grunn av manglende kunnskap (Aven og Renn, 2010). Analytikere som skal gjøre en vurdering av risiko for terrorhandlinger mangler ofte kunnskap og informasjon, dermed vil vurderingene være preget av stor grad av epistemisk usikkerhet. Det kan blant annet være mangel på kunnskap om hvilke mennesker som utgjør en trussel (hvem som har intensjon og kapasitet), hvilke mål som er attraktive for terroristen, og når de eventuelt vil slå til. Igjen avhenger dette av hvilket perspektiv man har på risiko og usikkerhet (Aven, 2003). Den epistemiske usikkerheten uttrykkes ifølge Aven og Renn (2010) av subjektiv sannsynlighet, som er et subjektivt mål av usikkerhet betinget av bakgrunnskunnskap *(K)*. En subjektiv sannsynlighet uttrykker analytikerens grad av usikkerhet om hva utfallet vil bli. Hvis du sier at sannsynligheten er ti prosent, sammenligner du usikkerheten med det å trekke en bestemt kule opp av en urne hvor det ligger ti kuler (Aven og Renn, 2010). I dette perspektivet snakker man ikke om en korrekt sannsynlighet, og dermed risiko, Sannsynligheten er subjektiv. Det vitenskapelige med perspektivet er en systematisering av kunnskap som finnes om fenomenet, samtidig som det er en læringsprosess. Denne måten å uttrykke usikkerhet på kan ses i sammenheng med det bayesianske perspektivet. Aven (2013) betegner denne sannsynligheten P (AIK). Å beskrive bakgrunnskunnskap og identifisere usikkerhet er viktig fordi usikkerhet kan være skjult i bakgrunnskunnskapen som sannsynlighetene bygger på (Aven, 2013). Njå, m.fl. (1998) beskriver noen utfordringer med å sette subjektive sannsynligheter. Det grunnleggende problemet/utfordringen er å overføre subjektive vurderinger fra eksperter og analytikere til tall, altså å kvantifisere på bakgrunn av subjektivitet. En annen utfordring er at ekspertene som setter sannsynlighetene kan ha ulike meninger og komme fram til ulike resultater. Det blir derfor viktig å klargjøre uoverensstemmelser. En tredje utfordring er at sannsynlighetene kan være den samme i en situasjon hvor du har mye og pålitelig kunnskap, og en situasjon hvor du ikke har det. Derfor bør man ifølge Aven (2013) beskrive og identifisere de antakelsene som sannsynlighetene er basert på, med tanke på både sensitivitet og usikkerhet. Styrken på kunnskapen som er lagt til grunn for sannsynlighetstallene er viktig (Aven og Krohn, 2013). Dersom fokus bare ligger på å beskrive og vurdere sannsynlighet alene uten bakgrunnskunnskap vil det kunne mislede beslutningstakere.

Aven (2013) beskriver også bruk av unøyaktige sannsynligheter, som innebærer å sette generaliserte sannsynligheter ved å bruke et intervall som beskriver nedre sannsynlighet og øvre sannsynlighet.

3.5.3 Strategisk og probabilistisk usikkerhet

Golany, Kaplan, Marmur og Rothblum (2007) viser til et skille mellom probabilistisk usikkerhet og strategisk usikkerhet, hvor han presenterer ulike metoder for å tilnærme seg dem. Han påstår at sannsynlighetsteori kan benyttes på førstnevnte, men for strategisk usikkerhet vil spill-teori være mer egnet. Spill-teori handler om en forestilling av et ikke-samarbeidende spill mellom angriper og forsvarer. Ved strategisk usikkerhet bør det tas utgangspunkt i full konflikt, i den betydning at en trusselaktør ønsker å oppnå skade eller tap av verdien til forsvarer. "Zero-zum game" er et uttrykk som vanligvis brukes for å fange opp de konflikterende interessene mellom partene. På bakgrunn av at trusselaktøren ofte er rasjonell og kalkulerende og har mulighet til å samle informasjon fra åpne kilder, bør det også tas utgangspunkt i at trusselaktøren har full informasjon og vet mesteparten av målets sårbarheter. Ifølge Ericson og Doyle (2004) vil trusselens natur i kombinasjon med mangel på data være en påminnelse på begrensningene til risikovurderinger og risikostyring i forbindelse med terrorisme. Aven (2013) er enig i at sannsynlighet ikke er et perfekt redskap, da man aldri kan vite med absolutt sikkerhet hva framtiden vil bringe. Han mener likevel ikke at vi må glemme sannsynlighet helt og at man må ta i bruk subjektive sannsynligheter dom nevnt ovenfor.

3.6 Risikopersepsjon

Risikopersepsjon er menneskers subjektive oppfattelse av risiko, som bygger på egen erfaring og informasjonsgrunnlag (Pettersen og Engen, 2010). Sosial og kulturell bakgrunn, samt erfaringer vil blant annet bidra i vurderingene og påvirke hvordan risiko oppleves og forstås (Renn, 2008). Denne teorien blir dermed relevant i forbindelse med en tilnærming til risiko som anerkjenner subjektivitet. Risikopersepsjon kan ha stor betydning innen sikringsanalyser ettersom det er mangel på empirisk data og historikk, og dermed i større grad preget av eksperters subjektive oppfatninger. Renn (2008) hevder at menneskelig atferd ikke blir drevet av fakta, men av persepsjon.

3.7 Ekspertvurderinger

For fenomener som er preget av lite empirisk data vil det være større behov for å benytte seg av eksperters subjektive vurderinger. For å sikre kvalitet på vurderingene er det behov for riktig ekspertise. (Njå, m.fl., 1998) påpeker at man må skille mellom ulike grader av ekspertise, for slik å plukke ut de rette ekspertene. Dreyfus og Dreyfus (1986) har utviklet ulike ferdighetsnivå i utviklingen fra en nybegynner til en ekspert, blant annet:

- En kompetent person som har en analytisk og faktabasert fremgangsmåte til problemer og hvordan disse kan løses.
- En dyktig person som klarer å skille mellom de fakta som er viktigst og hvilke som kan komme i bakgrunnen. Denne personen forstår problemer intuitivt og løser det derfra på en analytisk måte.
- En ekspert har en intuitiv tilnærming til både problemet og løsningen. Han har også evne til å reflektere kritisk over sin egen intuisjon.

En kombinasjon av kunnskap om fenomenene som analyseres, om modellene som finnes, samt en risikoforståelse vil være idealet. Det er den samlede kompetansen til risikoanalytikeren og eksperten som betyr noe, godt samarbeid og god kommunikasjon er dermed nøkkelbegreper. Njå m.fl. (1998) mener det er viktig å være oppmerksom på ekspertenes begrensninger. Noen eksperter kan for eksempel misbruke ekspertstemplet og makten dette innebærer og som en følge uttale seg om mer enn det som er vedkommendes kompetanse, ofte kreves det derimot ulik kompetanse. En annen begrensning er at ekspertvurderinger kan kreve mye tid og ressurser. Eksperter vil alltid være subjektive i sine vurderinger, og det vil dermed være naturlig for dem å bruke ulike heuristikker[12] når de angir sannsynlighet. Dette er nødvendigvis ikke et problem så lenge eksperten er bevisst denne tendensen. Uten å være bevisst kan det i verste fall føre til systematiske og alvorlige feiltolkninger. Gjennom samtaler med ekspertene bør risikoanalytikere forsøke å avdekke overkonfidens og heuristikker (Njå m.fl., 1998).

Noen eksempler på vanlige heuristikker er:

- *Tilgjengelighet:* Hendelser man er godt kjent med eller som ofte er blitt omtalt i lignende situasjoner som den man analyserer har lett for å komme i fokus.
- *Ankring og justering:* Man justerer vurderinger fra funn og informasjon som kommer fram i prosessen ut fra et spesielt utgangspunkt, som for eksempel tidligere erfaring.

[12] Tommelfingerregler

- *Representativitet:* En ekspert vurderer sannsynlighet ved å sammenligne sin kunnskap om et fenomen med den stereotypiske oppfatningen av dette fenomenet. Jo mer samsvar, desto mer sikker blir eksperten i sin vurdering.

Det bør fremgå av analysen eller diskusjonen rundt analysen hvilke heuristikker og menneskelige faktorer som kan ha påvirket resultatene fra analysen. Det må gjøres en avveining mellom det å benytte flere eksperter for å få helhetlige vurderinger eller individuelle eksperter for å få konsistente vurderinger. Ved bruk av flere er det helt avgjørende at ekspertene snakker noenlunde samme språk for at analyseresultatene skal være mest mulig gyldige (Njå, m.fl. 1998).

Før prosessen med å sette sannsynligheter starter er det visse ting som bør være klargjort og anerkjent overfor de involverte ekspertene:

- *Introduksjon til temaene:* For eksempel hva analysen skal brukes til, omfanget og kompleksitet, begrensninger og antakelser, samt hvorvidt det er tvetydighet i problemdefinisjonen.
- *Konkretisere problemet og bestemme informasjonsbehovet:* Ekspertene bør evaluere hvorvidt modellene og verktøyene som brukes i analysen bør bli utvidet, revidert eller avvist.
- *Gjøre ekspertene kjent med sannsynlighetsbegrepet*: Det vil være behov å samkjøre sannsynlighetsforståelsen og sette intuitiv sannsynlighet på relevante hendelser for analysen.

3.8 Verdi, Beskytter, Trusselaktør (APT) teorien

I 1997 lagde Giovanni Manunta en universell teori om sikkerhet mot tilsiktede uønskede handlinger som skal gjelde for alle bransjer og faglige ståsteder (Stranden, 2013). Teorien skiller sikkerhet mot tilsiktede handlinger fra blant annet sikkerhet mot teknologiske og naturlige ulykker. Teorien til Manunta er basert på tanken om at Security er en funksjon av tilstedeværelsen og samspillet mellom en verdi (Asset), en beskytter (Protecter) og en trusselaktør (Threat) i en gitt situasjon (Si). Stranden (2013) presenterer dette slik:

$$S = (V, B, T)\ Si.$$

Alle faktorene må være tilstede for at en sikringskontekst (S) skal eksistere. Uten en verdi er det ikke noe som trenger beskyttelse, uten en trussel er det ingen grunn til å beskytte verdien og uten en beskytter er det ingen som forsøker å oppnå sikkerhet. I en sikringskontekst, er det behov for sikringstiltak. De ulike faktorene må dermed identifiseres og beskrives, for å vurdere hvor og hvilke tiltak som trengs iverksatt. Det blir i praksis nødvendig å inkludere disse tre elementenes interaksjon med omgivelsene, da de ikke eksisterer isolert, men samhandler med hverandre. Situasjonsbegrepet blir brukt for å beskrive kompleksiteten av omstendigheter som kontinuerlig påvirker de tre elementene. Det eksisterer en dynamisk tilstand som hele tiden utvikler seg i forskjellige retninger. Trusselaktøren og beskytteren justerer seg konstant til hverandre. Stranden (2013) eksemplifiserer med kappløpet mellom trusselaktøren og beskytter, der trusselaktøren hele tiden forsøker å utvikle nye metoder og utnytte teknologi til å overkomme sikringstiltak, mens beskytteren hele tiden forsøker å holde følge med trusselaktøren eller å være ett skritt foran. Situasjonen vil også endres over tid. Stranden (2013) viser til et eksempel hvor en virksomhet fikk mindre penger til å bruke på sikkerhet som en følge av finanskrisen i 2008. APT-teorien introduserer dermed behovet for å følge med på hvordan trusselaktøren utvikler seg innenfor blant annet intensjon og kapasitet. Dette krever etterretningsarbeid, som er en systematisk måte å identifisere hva slags informasjon som trengs, samle inn denne informasjonen, dermed analysere og videreføre resultatet til dem som skal ta beslutninger om justering av tiltak. I hovedsak blir etterretningarbeid utført av PST og E-tjenesten, men ifølge Stranden (2013) kan også ledere og rådgivere som er ansvarlige for sikkerheten i en virksomhet driver etterretning. Her vil det derimot være en stor forskjell i hvilke lovhjemler de ulike aktørene har for innhenting og lagring av slik informasjon.

3.9 Oppsummering av teori:

Sikringsrisiko er preget av stor grad av usikkerhet blant annet på grunn av mangel på erfaring og historisk data, samt at trusselaktøren har en intensjon og kapasitet. Dette fører til at man må se bort ifra frekvensbasert sannsynlighet. Avhandlingen tar derfor utgangspunkt i en bayesiansk tilnærming til risiko som anbefalt av Jore og Njå (2010). Sannsynligheter er i denne tilnærmingen et resultat av en persons subjektive vurdering av usikkerheten. Ved lite historisk data og statistikk er analysene i større grad enn for høyfrekvente hendelser, avhengig av eksperters subjektive vurderinger. Mennesker har ulik forståelse og oppfatning av risiko, blant annet på bakgrunn av ulik informasjonsgrunnlag og erfaring, samt på grunn av

forskjellig kompetanse og bakgrunn. Det blir dermed viktig å beskrive bakgrunnsinformasjonen og forutsetningene som analysen baseres på. Avhandlingen har en risikobasert tilnærming til sikringsrisiko, men dette må også ses i sammenheng med APT-teorien som beskrevet ovenfor, for å få et helhetlig bilde av fagfeltet. Videre vil jeg undersøke hvordan petroleumssektoren og relevante myndigheter analyserer sikringsrisiko og i hvilken grad sannsynlighet kan brukes.

4 METODE

Vitenskapelig metode refererer til prosedyrer og tilnærminger for å innhente og analysere datamateriale (Holter og Kallevik 1982). Aubert (1985) i Hellevik (1994:14) ser på metode som: *"en fremgangsmåte, et middel til å løse problem og komme frem til ny kunnskap."* Metodevalget mitt skal vise hvilke egenskaper jeg vektlegger for å komme til bunns i min problemstilling. Analyse av sikringsrisiko har fått et økt fokus de siste par årene, men slik har det imidlertid ikke alltid vært og det er dermed ikke like utviklet som Safetyfeltet. Med bakgrunn i dette har jeg valgt å bruke kvalitativ metode fordi i motsetning til kvantitativ metode som omhandler tall og statistikk, innebærer kvalitative metoder dybdeforståelse av fenomenet som studeres. Nedenfor vil jeg beskrive hva dette innebærer og hvordan det har blitt gjennomført.

4.1 Intervju

Jeg valgte å benytte meg av intervju som metode i datainnsamlingen fordi jeg mener at det vil være best egnet for å svare på avhandlingens problemstilling. Dette mener jeg fordi ved intervju får man mulighet til å gå i dybden og dermed få en bredere forståelse. Ifølge Kvale (1997) brukes det kvalitative forskningsintervju når man er ute etter å få kjennskap til erfaringer og opplevelser, altså den subjektive oppfatningen om fenomenet som studeres. Jeg ønsket å få en bredere forståelse, fordi jeg hadde svært lite kunnskap om dette på forhånd. En årsak til dette er fordi i samfunnssikkerhetstudiet fokuseres det i større grad på analyse av ikke-intenderte uønskede hendelser og svært lite på analyse av tilsiktede handlinger. Jeg måtte derfor opparbeide meg innsikt og forståelse, og syntes da intervju var beste måten å oppnå dette på. Ved en fortsettelse av denne undersøkelsen kunne jeg derimot tenke meg å bygge videre på kunnskapen jeg har tilegnet meg underveis, og da kunne spørreskjema eventuelt blitt tatt i bruk.

Intervjuene ble gjennomført halv-strukturert (Kvale, 1997). Dette innebærer at jeg i forveien hadde formulert formålet med undersøkelsen. Jeg hadde utarbeidet en intervjuguide, hvor jeg fokuserte på ulike tema, og hadde under de enkelte temaene formulert ulike spørsmål som jeg tok utgangspunkt i. Jeg var likevel ikke bundet til å følge denne til punkt og prikke, og hadde dermed rom for improvisasjon. Selv om intervjuene ikke var fullt strukturerte, var de heller ikke ustrukturerte. Ifølge Kvale (1997) vil det være mest relevant å bruke halvstrukturerte intervju når fokuset er et bestemt tema, slik at man får de mest relevante og gyldige svarene

på problemstillingen. Intervjuguiden bør ifølge Svensson og Starrin (1996) utvikles på bakgrunn av aktuell litteratur og teoretisk rammeverk. Jeg måtte derfor sette meg inn i fenomenet som skulle undersøkes på forhånd for å øke min forståelse, slik at jeg skulle ha et godt utgangspunkt for å stille gode spørsmål, og ikke minst for å vite hvem jeg burde intervjue.

Utvelgelse av informanter

Siden jeg ikke har vært ute etter å generalisere har jeg ikke brukt statistiske metoder for å velge ut respondanter. Det finnes ingen standard metode for utvelgelse i kvalitative undersøkelser, man må likevel passe på at informantene velges ut slik at funnene i størst mulig grad er preget av gyldighet (Kvale, 1997). Ugyldige data kan ødelegge avhandlingens troverdighet. Jeg satt meg som nevnt ovenfor inn i gjeldende teori og litteratur og så på hvem som hadde uttalt seg om tema i diverse dokumenter. Eksempler på slike dokumenter er den årlige trusselvurderingen til PST og det nasjonale risikobildet utarbeidet av DSB. Dette var dermed med på å styre min utvelgelse av informanter. Ved å gjøre dette sikret jeg at intervjuobjektene var relevante for min problemstilling. Jeg startet med å intervjue myndigheter med kompetanse og faglig innsikt innen Security og analysemetodikk for å få et mer overordnet bilde av terrorisme og hvordan dette fenomenet kan analyseres. Deretter beveget jeg meg inn på petroleumssektoren og så på hvordan de gjennomførte sine analyser. Jeg merket godt til den såkalte ”snøballeffekten” som innebærer at planlagte intervjuer ofte kan føre til ikke-planlagte intervjuer, ved at jeg ble henvist videre av informantene til andre eksperter (Jacobsen, 2005). Nedenfor vises en oversikt over avhandlingens informanter.

Tabell 2: Oversikt over informanter

Hvem	Faglig ståsted	Hvor	Varighet
Tre Representanter fra DSB	Safety, noe Security	Telefonintervjuer	Ca. en time med hver representant
En Representant fra NSM	Security	Telefonintervju	Ca. en time
En representant fra PST	Security	Intervju hos PST i Oslo	Ca. en og en halv
To representanter fra Petroleumstilsynet	Safety, noe Security	Hos Petroleumstilsynet i Stavanger	Ca. en og en halv time
En representant fra Statoil	Security og risikoanalyse	Hos Statoil i Oslo og i Stavanger	Ca. en og en halv time hver gang
En representant fra Talisman-Energy	Security og risikoanalyse	Hos Talisman-energy i Stavanger	Ca. en og en halv time
To representanter fra GDF Suez	Safety og Security	Hos GDF Suez i Stavanger	Ca. 45 min
To representanter fra konsulentselskapet Proactima	Safety og risikostyring	Hos Proactima sine kontorer i Stavanger	Ca. en time
Morten Bremer Mærli, representerer seg og sitt ståsted	Fysikk, risikokommunikasjon, doktorgrad fra NUPI med atomterrorismetematikk	På hans arbeidssted, på Stortinget i Oslo	Ca. en time
Roy Stranden som representerer seg og sitt ståsted (har også brukt litteratur fra Stranden)	Tidligere ansatt i PST. Security-bakgrunn. Driver egen forskning: www.proakt.no	Telefonsamtale	Ca. en og en halv time totalt

4.2 Etiske betraktninger

Det ble viktig for meg å opparbeide tillit, slik at informasjonsinnsamlingen kunne være preget av mest mulig gjennomsiktighet. I et forsøk på å oppnå dette presenterte jeg meg selv på forhånd før intervjuet, der jeg blant annet beskriv kort meg selv, hva jeg studerer, samt litt praktiske opplysninger som tid på intervju og anonymisering av svar om ønskelig. Kvale (1997) beskriver tre etiske regler man bør jobbe ut ifra.

1) *Informert samtykke* - At informanten deltar på frivillig basis og er kjent med oppgavens formål. For å ta hensyn til dette informerte jeg i starten av intervjuet hva avhandlingen min gikk ut på og hva jeg ønsket å oppnå med den. Jeg spurte også om deres samtykke til å ta opp intervjuet. En av informantene ønsket ikke dette, noe som ble tatt hensyn til.

2) *Konfidensialitet* - At svarene til informantene ikke blir offentliggjort på en slik måte at de kan avsløre identiteten deres, dersom de ikke ønsker dette selv. For å ta hensyn til dette slettet jeg lydopptakene så fort jeg var ferdig med transkribering. To av informantene ga klart uttrykk for at anonymitet ikke var nødvendig.
3) *Konsekvenser* - Konsekvensene av en intervjustudie bør vurderes med tanke på ulempe og fordel for personen som blir intervjuet.

4.3 Gjennomføring av intervjuet

For at det skulle være praktisk for informantene møtte jeg dem på deres arbeidssted eller gjennomførte et telefonintervju dersom det var nødvendig.

Telefonintervju

Det finnes både fordeler og ulemper med telefonintervju (Sander, 2014). Det er en rask og effektiv metode, tid og penger kan spares. Ulempene er at man ikke har mulighet for visuell fremstilling, ikke kontroll over informantene sine omgivelser inkludert muligheten for støy, samt tekniske problemer som for eksempel dårlig dekning.

Personlig oppmøte

Det finnes også fordeler og ulemper med gjennomføring av intervju. Man får en viss kontroll over omgivelsene og man har mulighet til å oppfatte ikke-verbal kommunikasjon. Informanten kan lettere oppnå tillitt når han kan sette et ansikt på den som intervjuer. Ulemper er at det er tidkrevende og kan føre til utgifter i forbindelse med reising. Det kan også være mer krevende å finne tid som passer både intervjuer og informant.

4.4 Dataanalyse

Intervjuene ble tatt opp på bånd, samtidig som det ble notert. Jeg transkriberte intervjuene fra muntlig til skriftlig form. Dette var tidkrevende, men svært nyttig da jeg satt meg godt inn i funnene. En utfordring her kan være å oversette dialekt til bokmål (Kvale, 1997), men jeg er av den oppfatning at dette gikk fint. Jeg har benyttet meg av en deduktiv analyse. Der jeg har fulgt Kvales (1997) tre analysenivåer:

1) Selvforståelsesnivået: Her gjorde jeg et forsøk på å se saken fra informanten sin side uavhengig av mitt teoretiske ståsted.

2) Common-sense nivået: I denne fasen så jeg på ulike mønstre på tvers av de forskjellige informantene. De informantene som fulgte samme mønster ble dermed strukturert sammen og hevet opp på en bredere forståelsesramme enn første nivå.
3) Det teoretiske nivået: Her koplet jeg mine funn mot avhandlingens teoretiske rammeverk.

4.5 Metodiske begrensninger og utfordringer

Behov for døråpnere

Johannessen og Tufte (2006) beskriver såkalte *"døråpnere"* som kan bidra til å komme lettere innpå informantene. Jeg har underveis i forskningsperioden vært i dialog med Safetec, hvor jeg har hatt mitt eget kontor, samt med GDF Suez. Jeg ser på dem som mine *"døråpnere"* da de har hjulpet meg og komme i kontakt med noen av informantene, slik som Statoil og Talisman-Energy. I tillegg har min veileder fra Universitetet i Stavanger hjulpet meg med å komme i kontakt med representanter fra PST, NSM, samt DSB. Da jeg forsøkte å komme i kontakt med aktører på egen hånd var det i noen tilfeller vellykket, mens andre ganger ikke. Dette viser hvor viktig det er å ha noen kontakter, såkalte *"døråpnere"*. Det at ikke alle ønsket eller hadde mulighet til å stille til intervju kan ha påvirket avhandlingens validitet ved at en gjerne ikke får samlet inn all relevant og nødvendig informasjon for å besvare problemstillingen, noe som kan føre til at man ikke får dekket helheten (Kvale, 1997).

Sensitivt tema

En annen begrensning er at fenomenet som undersøkes er sensitivt. Dette er blant annet fordi dersom forebygging og forberedelser i denne sammenheng skal ha en hensikt, så er det av interesse for de enkelte aktørene å gradere en del av informasjonen. Svarene jeg har fått fra de ulike representantene kan være preget av dette. På bakgrunn av dette er det en mulighet for at jeg ikke har fått like utfyllende svar som jeg kanskje kunne fått ved undersøkelse av et annet fenomen.

Snøballeffekten

Som nevnt ovenfor har avhandlingen vært preget av den såkalte snøballeffekten (Jacobsen, 2005). Det vil si at jeg er blitt henvist til informanter ut fra hvilken kompetanse de har om fenomenet som studeres, og fra dem har jeg blitt henvist videre til andre relevante aktører. Dette kan være en svakhet ved avhandlingen ved at det er en mulighet for at informantene har henvist til andre som deler samme syn som dem. Slik kan det oppstå en skjevhet i

informasjonsinnsamlingen der ikke alle sider av en sak blir dekket. Jeg mener likevel avhandlingen representerer forskjellige syn og meninger, blant annet fordi jeg har dratt inn uavhengige fagpersoner, relevante myndigheter, samt et konsulentselskap i tillegg til petroleumsselskapene. Jeg har heller aldri hatt som formål å generalisere eller å si noe om en statistisk fordeling i en befolkning, målet har hele tiden vært å diskutere og drøfte bruken av sannsynlighet i analyse av sikringsrisiko. Slik kan gjerne avhandlingen inspirere til videre diskusjon og på den måten videreutvikle forståelsen og kompetansen på feltet.

Antall oljeselskap

På grunn av tidsmessige begrensninger er det grenser for hvor mange intervju som kan bli gjennomført. Intervjuer er tidkrevende blant annet på grunn av omfattende etterarbeid som transkribering og analysering. Det hadde kanskje styrket avhandlingen min om jeg hadde hatt med informanter fra flere oljeselskap. Jeg har likevel fått svært interessante funn ved å trekke inn andre relevante aktører. Jeg anså disse aktørene som viktige og relevante for min undersøkelse fordi de samarbeider med petroleumsselskapene, og innenfor et godt sikkerhet- og sikringsarbeid er et helhetlig syn og forståelse viktig (Njå m.fl., 1998). Det kan også tenkes at for mange intervju ville ført til mindre tid og dermed redusert kvaliteten på analysen av intervjuene, og det er kvalitet som er formålet med en kvalitativ analyse, ikke kvantitet (Kvale, 1997).

Eget ståsted

Det er mange tilnærminger til Security, denne avhandlingen dreier seg om en risikobasert tilnærming, og dermed vil mye av teorien som er brukes være basert på litteratur fra samfunnssikkerhetstudiet. Dette er litteratur jeg oppfatter som troverdig, men som kan skape en ensidig profil i avhandlingen. For å unngå dette har jeg også forsøkt å sette meg inn i litteratur på Securityfeltet. Pettersen og Engen (2010) hevder at ulik erfaring, kunnskap og risikosyn vil føre til at identifisering av risiko blir forskjellig. Jeg har vært bevisst på dette og dermed forsøkt å forholde meg nøytral til begge fagfeltene.

Noe jeg ville gjort annerledes?

De første intervjuene ble gjennomført med representanter fra Securityfeltet og med myndigheter som har et mer overordnet bilde. Dersom jeg skulle gjort noe annerledes ville jeg også intervjuet noen fra Safetyfeltet litt tidligere, slik at jeg ikke ble ”fanget” av en side av saken. Selv om det var vanskelig å bevege seg inn i to ulike fagområder, så mener jeg at jeg taklet dette bra og reflekterte kritisk over funn fra begge felt.

4.6 Styrker med avhandlingen

Til tross for at jeg har hatt behov for døråpnere og vært preget av snøballeffekten, mener jeg at jeg har presentert flere forskjellige syn fra ulike representanter og at avhandlingen dermed er preget av mangfoldighet. Til tross for tidsbegrensninger synes jeg at jeg har fått gjennomført mange intervju, samtidig som jeg har sørget for kvalitet i både analysen og presentasjonen av funnene. Det er også en styrke at jeg har intervjuet uavhengige fagpersoner, relevante myndigheter, konsulentfirma og forskjellige petroleumsselskap. Sistnevnte har godt rykte på seg når det gjelder HMS innenfor Safetyområdet (Arbeidsdepartementet, 2013), og de relevante myndighetene har utdanning og særskilt kompetanse innenfor Security. Samarbeid og tverrfaglighet er viktig for å få et helhetlig bilde.

4.7 Oppsett av funn

Funnene er delt inn etter avhandlingens to forskningsspørsmål som må ses i sammenheng med deres faglige ståsted, jf. Tabell 2, kap 4.1.

- Hva er dagens status: Hvilke analysemetodikk brukes av Oljevirksomhet og relevante myndigheter i Norge i dag på Securityfeltet?
- Hva er oljeselskapene og de relevante myndigheters syn på eksisterende metodikk?

Ikke alle informantene utarbeider risikoanalyser. Deres syn er likevel presentert da de har kompetanse innen sikring, arbeider med det, samt samarbeider med aktører som utarbeider egne analyser. Avhandlingens problemstilling er preget av større mangfoldighet og er blitt belyst i større grad ved at disse bidragene er tatt i betraktning. Bidragene fra informantene har gitt svar på problemstillingen i ulik grad, og det har vært uenigheter. Jeg påstår likevel at etter en vurdering og analyse av informantenes svar, sett opp mot hverandre og det teoretiske rammeverk, så vil funnene belyse problemstillingen på en god måte.

5 EMPIRI

Nedenfor presenteres hvordan analyser av risiko for tilsiktede uønskede handlinger blir gjennomført av petroleumsselskap og relevante myndigheter. Det må klargjøres at analyse og vurdering har motsatt betydning for DSB og PST. For PST er vurdering en del av analysen, for DSB er det motsatt. Dette er viktig å understreke, slik at misforståelser kan unngås. Denne avhandlingen tar som DSB utgangspunkt i at analyse inngår i en vurdering. Samtlige av informantene ser behovet for å identifisere og beskrive verdier, trusler og sårbarhet, men er uenige om vi trenger to ulike metoder og om vi må se bort fra sannsynlighet. En nærmere gjennomgang av hvordan disse de tre faktorene forsøkes avdekket vil fremkomme. Tilslutt, vil en gjennomgang av representantenes syn på eksisterende metodikk og bruk av sannsynlighet finne sted.

5.1 Hva er dagens status, og hvordan analyseres risikoen for terror?

5.1.1 Relevante myndigheter

Standard Norge

Det finnes tre standarder som spesifikt tar for seg beskyttelse mot tilsiktede uønskede handlinger, ofte referert til som 5830-serien. NS 5830 som ble godkjent i 2012, er den eneste av standardene beskrevet under som er blitt godkjent til nå, dermed betegnes de to andre som prNS.

- Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi (NS 5830)
- Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til risikohåndtering (prNS 5831)
- Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til risikoanalyse (prNS 5832)

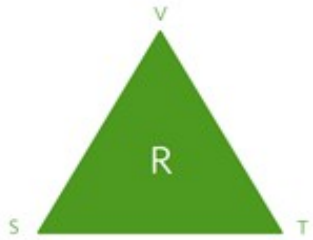
PST har vært en av de sentrale aktørene i arbeidet med å utvikle ny metode for å vurdere risiko knyttet til tilsiktede handlinger. Roy Stranden forteller at arbeidet med standardene startet med en revidering av to veiledere om beskyttelse mot terrorhandlinger som var utgitt

av NSM som den ene og PST og Politidirektoratet som den andre. Begge disse var gradert og forholdsvis lite kjent. Justisdepartementet bestemte da at det skulle utgis kun en veileder som skulle være ugradert. Dette arbeidet hadde pågått i to år når Roy Stranden startet i PST, hvor han fikk som oppgave å bidra i dette arbeidet. PST tok en ledende rolle fordi dette var noe som Stranden og hans samarbeidspartner prioriterte høyt. De to var de eneste med en akademisk bakgrunn innen sikkerhet og fikk dermed en ledende rolle i arbeidet. I praksis skrev de om alt som var blitt gjort tidligere. Noe av årsaken til det var fordi de mente kvaliteten på det som ble gjort tidligere var for dårlig. Stranden sier videre at de gjennom deres veiledning til private og offentlige virksomheter så hva de opplevde som kaotiske tilstander hvor de ikke klarte å kommunisere på grunn av manglende felles plattform, i tillegg til at flere slet med å gjennomføre risikoanalyser av kriminelle handlinger. Alle risikoanalysene som var gjort hadde brukt en Safety tilnærming og resultatene var svært dårlige, da de ikke belyste relevante faktorer på en god måte. Parallelt med denne prosessen hadde det startet et arbeid i Standard Norge med å undersøke hvorvidt det fantes noen relevante standarder innenfor kategorien kriminalitet. Da Stranden og samarbeidspartneren ble klar over dette arbeidet og ble klar over at det var mangler, så de at det var mer hensiktsmessig å overføre arbeidet de holdt på med i PST til Standard Norge. Det var først en liten rasktarbeidende gruppe som skulle lage utkastene, videre ble de sendt ut på høring til en større referansegruppe før de tilslutt gikk ut til offentlig høring. Deltakerene fra gruppen var blant annet representanter fra PST, NSM, Næringslivets sikkerhetsråd, Statoil, Forsvarsbygg og Standard Norge. Flere andre har også vært med i ettertid, men primært er det Stranden og samarbeidspartneren som har stått for det faglige innholdet i tillegg til å drive prosessen fremover. Arbeidet har startet en egen dynamikk som nå resulterer i flere standarder innen samme serie og som er tett koblet sammen. Til tross for at prNS 5831 og prNS 5832 ikke er godkjent er de kjent av alle informantene, det er derimot ulike syn i hvilken grad den bør benyttes. Representanten fra PST hevder at en av årsakene til at den ikke er blitt godkjent er på grunn av uenigheter i forbindelse med termonologi og framgangsmåte, han nevner DSB som eksempel.

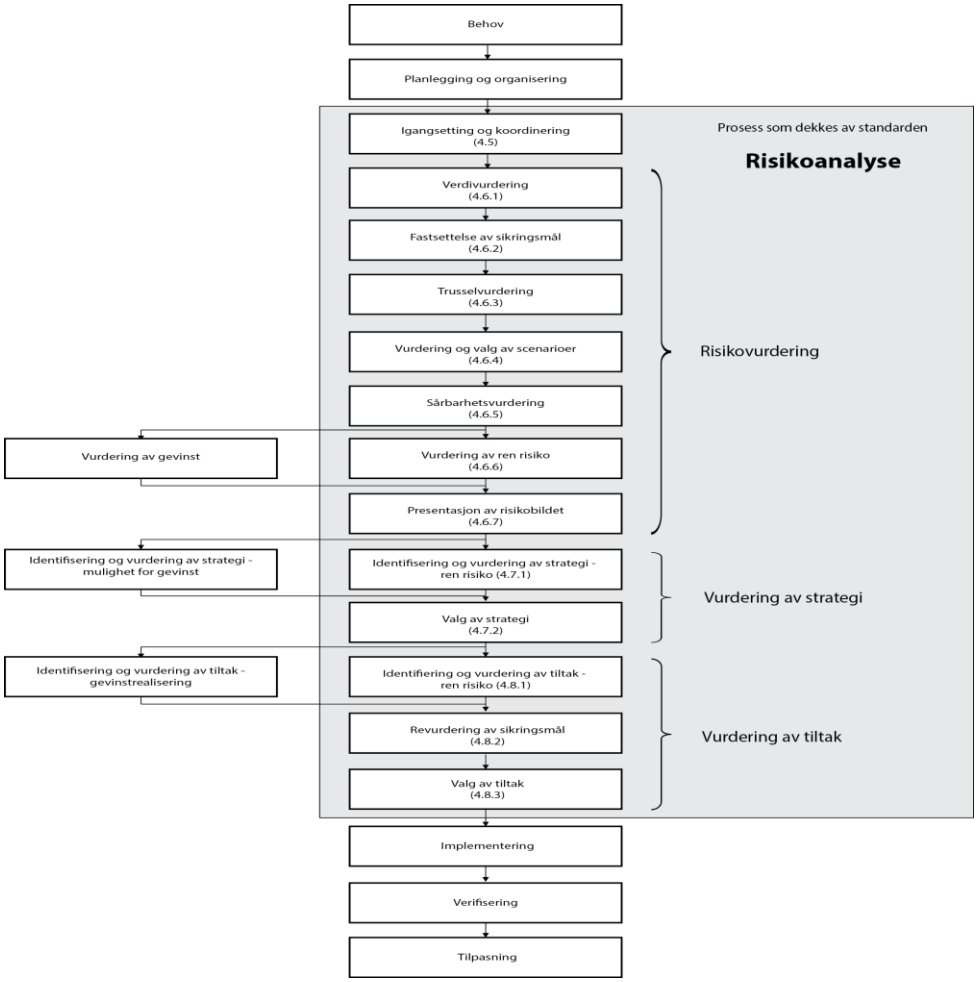
> *"DSB mener at de har et slags eierforhold til dette med risikoanalyse" Representant fra PST.*

Det framkommer av standarden at en risikoanalyse må innebære en vurdering av verdi, trussel og sårbarhet. Figur 4 "Risikotrekanten" blir presentert i PST, NSM og PODs veileder, og

viser til forholdet mellom de tre faktorene. En reduksjon i en av dimensjonene vil medføre en mindre totalrisiko, og en økning i en av dimensjonene føre til økt totalrisiko. Figur 5 viser et flytdiagram av analyseprosessen fra prNS 5832, som baseres på trekanten.

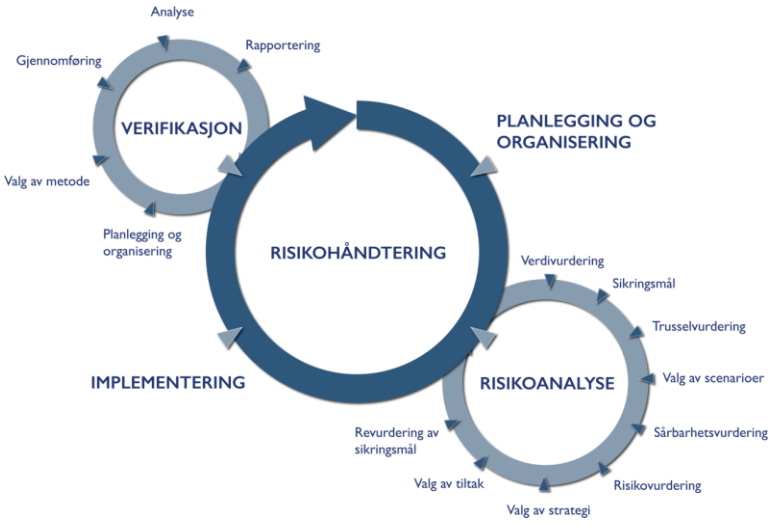


Figur 4: Risikotrekanten (PST, NSM, PODs veileder)



Figur 5: Flytdiagram av analyseprosessen slik det blir presentert i prNS 5832

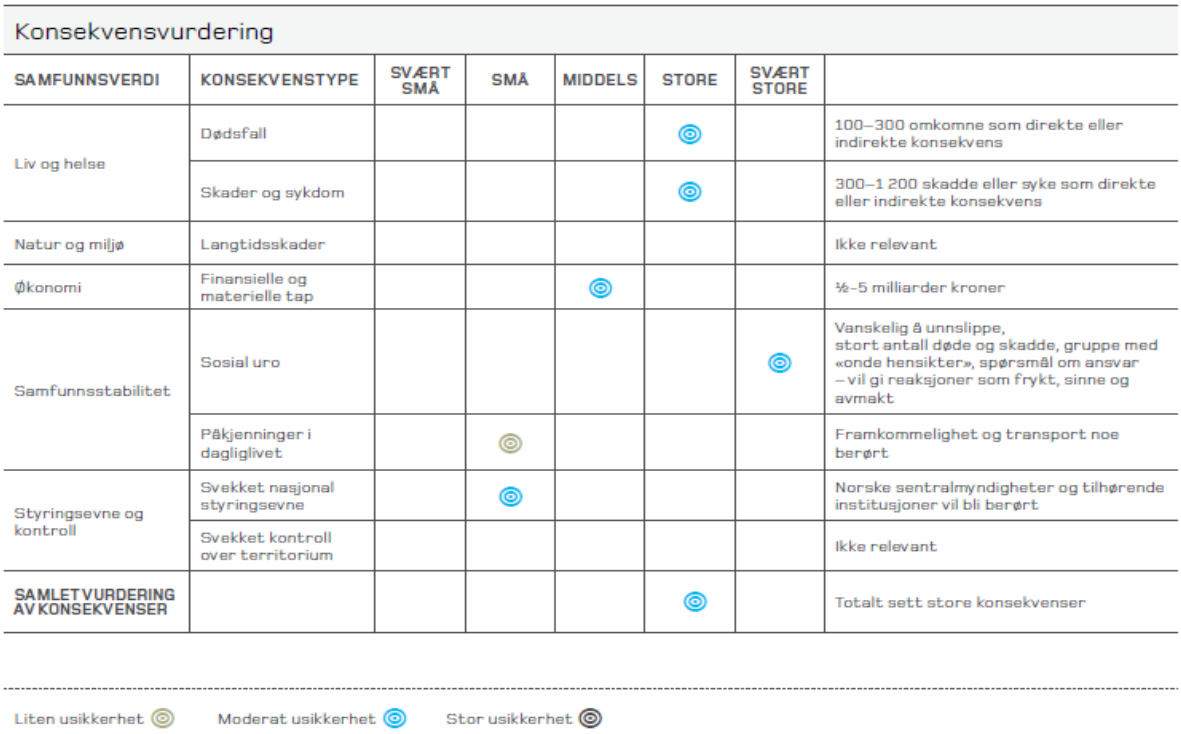
Roy Stranden har utarbeidet en risikoanalyse med bakgrunn i prNS 5832, som kan bli brukt som et eksempel for å få frem ulike momenter ved vurderinger og gjennomføringen av en risikoanalyse for kriminelle handlinger, se vedlegg 3. Figuren under er en fremstilling av risikohåndteringsprosessen som han jobber ut fra.



Figur 6: Risikohåndteringsprosessen (Roy Stranden).

Direktoratet for samfunnssikkerhet og beredskap (DSB)

DSB som organisasjon har en ulik metodisk tilnærming til risiko og som nevnt ovenfor er de ifølge representanten fra PST uenig angående terminologi og metodikk. DSB gjør sitt arbeid med utgangspunkt i ISO 31000. De ser på konsekvenser og usikkerhet. Der usikkerheten er i henhold til hvor sannsynlig det er at en hendelse vil inntreffe og usikkerhet i forbindelse med konsekvensene av angrepet. DSB har altså en ulik definisjon på risiko enn PST og NSM. DSB utarbeider hvert år et nasjonalt risikobilde. I risikobildet for 2013 har de inkludert et scenario som går på terrorangrep i et byområdet. I utgangspunktet hadde de benyttet seg av samme tilnærming til risiko også her, sannsynlighet x konsekvens. Det ble for denne hendelsen satt en sannsynlighet på 0,01. Dette vekte skarpe reaksjoner fra blant annet PST og NSM, noe som gjorde at sannsynlighetstallet ble fjernet. DSB ser nå bare på konsekvens og usikkerhet i forbindelse med konsekvensene. Dette blir presentert i en tradisjonell risikomatrise, uten å sette sannsynlighet.



Konsekvensvurdering

SAMFUNNSVERDI	KONSEKVENSTYPE	SVÆRT SMÅ	SMÅ	MIDDELS	STORE	SVÆRT STORE	
Liv og helse	Dødsfall				◎		100–300 omkomne som direkte eller indirekte konsekvens
	Skader og sykdom				◎		300–1 200 skadde eller syke som direkte eller indirekte konsekvens
Natur og miljø	Langtidsskader						Ikke relevant
Økonomi	Finansielle og materielle tap			◎			½–5 milliarder kroner
Samfunnsstabilitet	Sosial uro					◎	Vanskelig å unnslippe, stort antall døde og skadde, gruppe med «onde hensikter», spørsmål om ansvar – vil gi reaksjoner som frykt, sinne og avmakt
	Påkjenninger i dagliglivet		◎				Framkommelighet og transport noe berørt
Styringsevne og kontroll	Svekket nasjonal styringsevne		◎				Norske sentralmyndigheter og tilhørende institusjoner vil bli berørt
	Svekket kontroll over territorium						Ikke relevant
SAMLET VURDERING AV KONSEKVENSER					◎		Totalt sett store konsekvenser

Liten usikkerhet ◎ Moderat usikkerhet ◎ Stor usikkerhet ◎

Figur 7: Risikomatrise med konsekvens og usikkerhet (DSB, 2013).

DSB konkretiserer usikkerheten ved å vurdere kunnskapsgrunnlaget som ligger til grunn for konsekvensvurderingene. Dette går på resultatenes sensitivitet med tanke på endringer i forutsetningene som ligger til grunn for scenarioet, for eksempel endring i tidspunkt på døgnet, værforhold og lignende.

Usikkerhetsvurdering

INDIKATORER PÅ KUNNSKAPSGRUNNLAGET	FORKLARING
Tilgang på relevante data og erfaringer	Forskning og tilgang på noe data og erfaringer fra tilsvarende hendelser, blant annet i Midtøsten og Afghanistan, og tidligere hotellhendelser.
Forståelse av hendelsen som analyseres (hvor kjent og utforsket er fenomenet)	Terrorangrep vurderes som et godt kjent og utforsket fenomen sammenlignet med øvrige type hendelser som er analysert i NRB.
Enighet blant ekspertene (som har bidratt i risikoanalysen)	Ingen store uenigheter blant ekspertene
Resultatenes sensitivitet	
I hvilken grad påvirker endringer i forutsetningene konsekvensanslagene?	Type håndvåpen, eksplosiver og mål, hvorvidt eksplosjonene medfører at bygninger raser sammen, tidspunkt på døgnet og kriseinformasjonen som gis er kritiske forutsetninger for konsekvens-vurderingene. Resultatenes sensitivitet vurderes derfor som *moderat*.
Samlet vurdering av usikkerhet	Usikkerheten vurderes å være *moderat*.

Figur 8: DSBs vurdering av usikkerhet (DSB, 2013).

5.1.2 *Petroleumsselskap*

GDF Suez

GDF Suez har ingen analysemetodikk spesifikt for terrorisme og andre tilsiktede handlinger. De har en liste med forskjellige typer risikoanalyser som i utgangspunktet blir brukt i forbindelse med Safety hendelser, og som er basert på sannsynlighet x konsekvens. Hazid og Hazop er to eksempler. Representantene forteller at de har planer om å oppdatere analysearbeidet i forbindelse med Security i løpet av året, spesielt for beredskap. Det virker som det er uklart om en egen Securitymetodikk for analyse skal utarbeides.

Statoil

Statoil brukte tidligere den tradisjonelle teknisk-naturvitenskapelige risikoanalysen på alle uønskede hendelser, både Safety og Security. Etter hvert så Statoil behovet for andre metoder. En årsak til det var blant annet gisselsituasjonen på gassanlegget In Amenas i Algerie. På bakgrunn av dette har Statoil utviklet et nytt styringssystem for Security og en ny metodikk for analysering og vurdering av sikringsrisiko som tredde i kraft ved årsskiftet 2013/14. Metodikken til Statoil er veldig lik framgangsmåten som anbefales i Standard prNS 5832, men med litt forskjellig begrepsbruk. Statoil ser på sikringsrisiko som en funksjon av trussel, sårbarhet og konsekvens. Han under streker at konsekvens er det samme som verdi, konsekvensen av at verdien blir skadet eller tapt. For eksempel skade eller tap av mennesker, økonomiske tap, miljømessig skade, eller skade på omdømme til virksomheten. Roy Stranden støtter dette og sier det er to sider av samme sak, hvor konsekvens er en annen måte å vurdere verdi på. Representanten fra Statoil sier at de har fått inspirasjon fra Department of Homeland Security i USA og American Petroleum Institute, som ser på Security risk som en funksjon av formelen: Threat x vulnerability x Consequence. Det er en semi-kvantitativ metode hvor de ut fra en subjektiv vurdering setter en score fra en til ti på hver av de tre faktorene og hvor den totale scoren utgjør den totale risiko. Statoil benytter seg altså av tall og kvantifisering basert på en kvalitativ vurdering, slik at de kan sammenligne ulike risikobilder. Riskobildet blir så plassert inn i ulike risikonivå; Lav, moderat, høy, ekstrem. Statoil bruker kategoriseringen av ulike nivå som PST opererte med tidligere, men som de nettopp gikk bort ifra på grunn av vanskeligheten med å sette et nasjonalt risikonivå.

Tabell 3: Ulike risikonivå

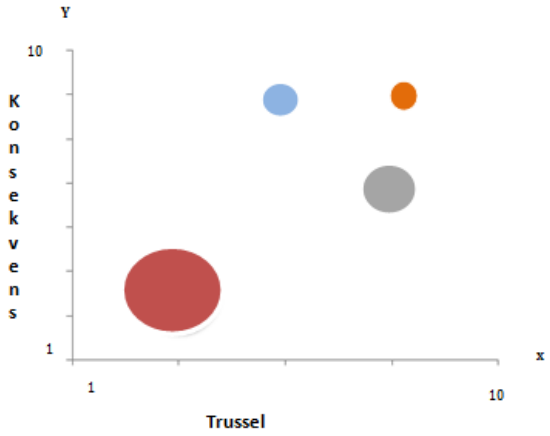
Lav	En eller flere aktører kan ha intensjoner om, men trolig ingen kapasitet til å ramme bestemte interesser. Det foreligger en mulig, men lite sannsynlig trussel.
Moderat	En eller flere aktører kan ha intensjoner om og kapasitet til å ramme bestemte interesser. Det foreligger en mulig trussel.
Høy	En eller flere aktører har intensjoner om og kapasitet til å ramme bestemte interesser. Det foreligger en generell og uspesifisert trussel.
Ekstrem	En eller flere aktører har intensjoner om og kapasitet til å ramme bestemte interesser. Det foreligger en spesifikk og overhengende trussel.

På bakgrunn av dette har de tilpasset en egen risikoanalyse for sin virksomhet bestående av følgende faser:

- Verdivurdering
- Trusselvurdering
- Risikovurdering (sårbarhet, scenariomodellering)

I tillegg har Statoil et kapittel om usikkerhet og begrensninger. Usikkerheten blir beskrevet på en fullstendig kvalitativ måte, uten noen som helst tall og kvantifisering. Representanten fra Statoil sier at det er stort sett i trusselvurderingen det er mye usikkerhet, og at scoren som er satt der vil stige ved økt usikkerhet. Det vil alltid være begrensninger i forhold til en risikovurdering. Representanten fra Statoil nevner at det kan ha med tid og tilgjengelighet å gjøre eller at du ikke har fått snakket med riktige personer. Representanten sier at begrensningene er veldig viktige, slik at ikke folk får inntrykk av at en har kontroll over informasjon som en ikke har tilgang til. For å unngå å villede noen må begrensninger beskrives.

Statoil tar i bruk et boblediagram som en måte å framstille de tre dimensjonene; trussel, sårbarhet, konsekvens. Y-aksen representerer konsekvensene, X-aksen representerer trusselen og de ulike boblene representerer størrelsen på sårbarhetene. Nedenfor er et enkelt eksempel, det er ikke slik Statoil sitt ser ut. Ofte vil det innenfor de ulike aksene være forskjellige farger, som i en risikomatrise, for at det lettere skal kunne leses av hva som er høy og lav risiko. I utgangspunktet er det likevel størrelsen på boblene som har størst betydning, da disse kan påvirkes av virksomhetene.



Figur 9: Egenprodusert figur av et boblediagram, kun for å illustrere et eksempel.

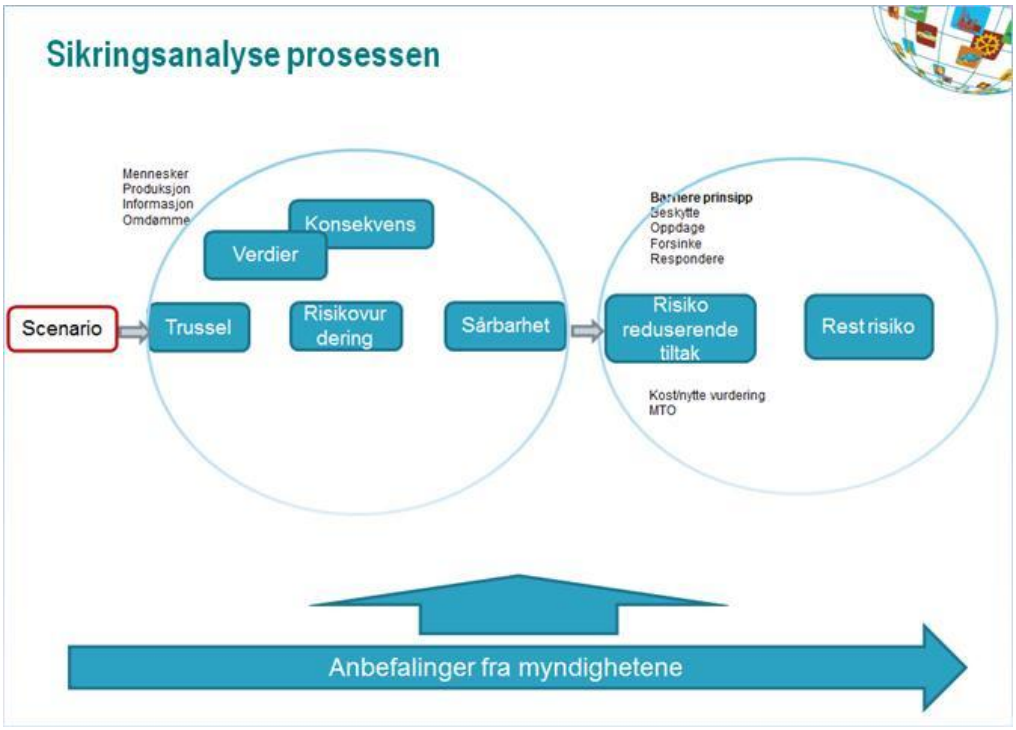
Den røde boblen viser stor sårbarhet, men liten trussel og konsekvens. Den orange boblen derimot viser lav sårbarhet, men høy trussel og konsekvens. Det vil kanskje være den grå boblen som bør reduseres først, da sårbarhetene og konsekvensene er moderat, men trusselen høy. Dette vil likevel være en vurdering som kan være forskjellig fra person til person.

Når Statoil skal presentere resultatene av sikringsanalysen må de prøve å konvertere det inn i den totale risikostyringen, slik at beslutningstaker kan prioritere å håndtere det som er mest utsatt eller farligst først. De plasserer kvantifiseringene de har kommet fram til i en matrise for å få en lignende presentasjon slik som Safetyrisiko, litt forskjeller vil det derimot være. De ser blant annet på framgangsmåten i FEMA 452 ”A how-to guide to mitigate potential terrorist attacks against buildings” (2005), se vedlegg 2.

Talisman-Energy

Talisman-Energy har en metodikk som ligner Statoil sin og tar utgangspunkt i risikotrekanten; Verdi, trussel og sårbarhet, se figur 4. De baserer risikoanalysen på mulige scenarioer basert på en vurdering av verdi (konsekvens av bortfall), trussel og sårbarhet. På hver av de enkelte faktorene settes et kvalitativt tall. De gjennomfører videre en såkalt "Self-riskassessment" hvor de tar utgangspunkt i en hazid-analyse som er en velbrukt risikoanalyse på Safetyfeltet. I deres "Self-Riskassessment" settes et kvalitativt tall på hvor sannsynlig/mulig et anslag kan være, basert på subjektive vurderinger av verdi, trussel, sårbarhet fra kvalifiserte eksperter. Dette blir gjort for å kunne sammenligne og sette sammen Security og Safety risiko. Sannsynligheten og konsekvensen kan bli et tall mellom en og fem slik at total risikoen kan være opp til 25. Totalscore over syv vil bli sett på som uakseptabelt og være innenfor det røde området i risikomatrisen, som de bruker for å presentere risikobildet. Talisman-Energy har også ulike kategorier av risikonivå, lav, moderat, høy og ekstrem. De sitter tilslutt igjen med to risikobilder:

- Før mitigerende tiltak
- Etter mitigerende tiltak



Figur 10: Laget av representant fra Talisman-Energy som viser deres prosess. Ut fra trussel, sårbarhet, gjøres en kvalitativ vurdering som det settes tall til.

5.1.3 Konsulentselskapet Proactima

Konsulentfirmaet Proactima følger ISO 31000 og ser på både konsekvens og sannsynlighet/usikkerhet. Det første Proactima gjør når de arbeider med sikringsanalyser for oljeselskap er å sette seg inn i selskapets risikostyringssystem. Deretter definerer de omfang av analysen. Etter de har gjort en verdivurdering, henter de trusselvurderinger hvor de tar utgangspunkt i offentlig tilgjengelig informasjon og ser på hvordan trusselbilde er for selskapet som er deres kunde. Verdi og trusselvurderingen er to produkter proactima tar inn i forkant av analysemøte. I analysemøtet gjennomfører de, slik som Talisman-Energy, en hazid analyse. Der de ser på hvilke hendelser de er utsatt for, hvilke scenarioer som kan oppstå, for dermed å gjøre en risikovurdering. De foreslår videre tiltak, og ser på sårbarhetene i etterkant av iverksatte tiltak. De har en sammenstilling av elementer fra hvert fagområde ved at de trekker inn verdi, trussel og sårbarhet i allerede eksisterende framgangsmåte. De mener å ivareta det som står beskrevet i NS 5830-serien, men følger framgangsmåten som presenteres i ISO 31000, ved at de har med verdi og trussel vurdering i forkant av riskoanalysen. De lager ikke nye systemer, de benytter seg av det som allerede finnes. De bruker samme erfaring, kompetanse og system som for Safetyområdet. De har en helhetlig og enhetlig tilnærming til risiko.

5.1.4 Oppsummering

NS 5830-serien har ulike begreper og beskriver en annen framgangsmåte enn ISO 31 000, NS 5814 og NORSOK Z-013. Både Statoil og Talisman tar utgangspunkt i disse standardene, men har egne systemer for å integrere det i resten av risikostyringen, hvor de bruker elementer både fra Safety og Security. De vurderer verdi og trussel, ser på ulike scenarioer og dermed hvor de er sårbare. Deretter gjør de en kvantifisering av de enkelte dimensjonene for å beskrive hvor lav eller høy verdien (konsekvens av bortfall av verdien), trusselen og sårbarhetene er, slik at den totale scoren kan plasseres i et totalt risikonivå. Slik kan de sammenligne ulike risikobilder og dermed prioritere ressursbruk og tiltak. Proactima gjør mye av det samme, men følger framgangsmåten som beskrives i ISO 31000. Representanten fra proactima mener bruk av egen metode på Securityområdet som kommer med helt andre begreper og framgangsmåter, vil føre til en risikostyringprosess som ikke er helhetlig.

5.2 Verdi, trussel og sårbarhet

Det er ulike måter å gå fram i et forsøk på å avdekke verdi, trussel og sårbarhet. Nedenfor presenteres de ulike framgangsmåtene som nevnt av representantene.

5.2.1 Verdi/konsekvens ved bortfall av verdi

I prNS 5832 står det at en må identifisere, definere, vurdere og rangere de verdiene som må beskyttes relatert til et terrorangrep. Verdivurderingene må videre brukes for å prioritere bruken av ressurser i en sikringssammenheng. Verdiene vil være helt avgjørende for hvilke sikringsmål som blir satt for å fjerne eller redusere risikoen. Representanten fra Direktoratet for samfunnssikkerhet og beredskap (DSB, 2013) understreker at det må tas hensyn til ulike rammebetingelser og perspektiver når verdiene defineres, som for eksempel lover, egne målsetninger og forhold til omgivelsene. Det anbefales av alle informantene å samarbeide med relevante aktører, få fram flere synspunkt i en workshop. Dette er også noe som blir understreket i en trussel og sårbarhetsvurdering. Ifølge Roy Stranden er det avgjørende å starte med verdiene for å kunne gå videre i prosessen.

> *"Start med verdiene, som er grunnlag for hver fornuftig bruk av ressurser for å sikre noe (...) Om du ikke vet verdiene som skal sikres kan du ikke gjennomføre en god trusselvurdering, og for å kunne gjennomføre sårbarhetsvurderingen må du først ha gjort verdi og trusselvurdering. Her er det et avhengighetsforhold. Om dette gjøres i en annen rekkefølge vil du finne opp trusler og scenarioer som kanskje ikke er relevante og som du ikke bør bruke tid på" - Roy Stranden*

5.2.2 Trusselvurdering

Det fremkommer av prNS 5832 at det må gjøres en selvstendig trusselvurdering etter en identifisering av verdiene, hvor det da blir sett på trusselaktører som kan ramme de identifiserte verdiene. En trussel bestemmes ifølge Morten B. Mærli av hvem som ønsker å oppnå hva, med hvilke midler og hvilke mål. Faktiske trusler oppstår derimot ikke før noen har intensjon og kapasitet til å gjennomføre et angrep. Videre påstår han at en trusselaktørs risikotaking vil øke ut fra hvor betydelige verdiene er for han, dvs. at verdiene må skape interesse hos trusselaktøren. Dersom ikke verdiene vekker interesse eller er betydelige for trusselaktøren mener Mærli at risikoen vil være lavere for virksomheten som eier verdiene. Det er ikke alltid tilfelle hevder Roy Stranden, da verdiene ikke nødvendigvis trenger å være målet for trusselaktøren, men et virkemiddel for å oppnå et annet mål. Dersom dette er tilfellet vil fokuset på beskytterens verdi være underordnet. For virksomheten som ønsker å beskytte

sine verdier vil dette være likegyldig i og med at tap er tap uansett om man er et tilfeldig mål eller primærmål. Verdiene kan imidlertid være svært attraktive for trusselaktør samtidig som risikoen kan være neglisjerbar, dersom angriper ikke har kapasitet til å gå gjennom angrepet. Kapasitet i form av blant annet kompetanse, ferdigheter og utstyr eller verktøy. Det understrekes av representanten fra Statoil og likevel å holde et øye med trusler som er lave, for å sørge for at trusselen ikke stiger uten at det blir fanget opp av virksomheten.

Trusselvurdringens formål

Ifølge prNS 5832 kan en trusselvurdering ha to formål i en sikringsmessig kontekst:

1) Å identifisere trusselaktørene og deres framgangsmåter for å dimensjonere grunnsikringen og beredskapstiltakene.
2) Tidlig varsling slik at eventuelle beredskapstiltak kan iverksettes for å motstå et potensielt angrep.

Etterretningsmetodikk

PST og Etterretningstjenesten bruker etterretningsmetodikk for informasjonsinnhenting i et forsøk på å avdekke trusselen for Norge, hvor PST ser på nasjonale forhold og Etterretningstjenesten internasjonale forhold. I ansvarsområde er det en tydelig ansvarsfordeling mellom dem, men Roy Stranden påpeker at metoden de bruker er ganske lik, bortsett fra at er at E-tjenesten har mer kapasitet innenfor signaletterretning (SIGINT). Deres årlige trusselvurdering er en analyse av forventet utvikling innenfor deres hovedansvarsområder. Vurderingen retter fokus mot forhold som kan påvirke norsk sikkerhet og skade nasjonale interesser.

> *"En trusselvurdering er en ferskvare (...). Det er en kontinuerlig prosess, som egentlig aldri stopper (...). I løpet av et år kan imidlertid uforutsette hendelser endre vurderingsgrunnlaget, og slike hendelser kan få stor betydning for trusselsituasjonen"*
> *- Representant fra PST*

PST har to måter å vurdere trussel på

1) Strategisk analyse/Et strategisk syn: Ser på historikk og prøver så å se framover med den informasjon i minne.
2) "Current" analyse, det som skjer nå: De miljøene, kapasitetene og den intensjonen miljøene har akkurat nå. Denne type vurdering er for eksempel rettet opp i mot personer, hendelser og arrangementer.

Trusselen kan være lav en dag, men representanten fra PST viser likevel til 22. Juli og sier ”vel trusselen var jo skyhøy og vi så den ikke.” Disse vurderingene baserer seg mye på informasjonsinnhenting og på de strategiske vurderingene som blir gjort.

Trusselindikatorer

Samtlige av avhandlingens informanter prater om intensjon og kapasitet ved en trusselvurdering. De fleste ser på PST sine trusselvurderinger og samarbeider tett med dem. En av representantene fra DSB påstår at de etter hvert har litt evne til å tro og mene noe om kapasitet. De prøver å ha kontroll med blant annet tilgjengelighet på type terrormidler, for eksempel kjemikalier som det går an å lage sprengstoff av. Han påstår videre at det er generelt vanskelig å bygge opp stor kapasitet i Norge uten at det blir oppdaget på en eller annen måte.

”Vi er et lite og ganske gjennomsiktig samfunn.”

Representanten fra PST viser til ulike indikatorer som de tar utgangspunkt i ved en trusselvurdering

A) Tilstedeværelse

Det blir her sett på om det eksisterer trusselaktører i området eller regionen.

B) Kapasitet

Det blir her sett på om trusselaktørene har ressurser og kunnskap til å gjennomføre en handling.

C) Intensjon

Det blir her sett på om det finnes trusselaktører med en intensjon om å gjøre skade.

D) Historikk

Her ser en på om det eksisterer trusselaktører som har gjennomført eller truet med å gjennomføre en slik type handling tidligere.

E) Målvalg

Det vurderes om identifiserte trusselaktører har valgt ut en virksomhet som et mål, blant annet ved å se på hvilke verdier som er attraktive for trusselaktørene og hvorfor.

Statoil har egne ansatte med Security kompetanse som arbeider med trusselvurderinger, men samarbeider likevel også tett med PST. Representanten fra Statoil nevner samme faktorer som PST ved gjennomføring av en trusselvurdering, men er stolte av å legge til en indikator de har utviklet selv.

- **Future anticipated targeting** – Denne indikatoren går på hva trusselaktøren er forventet å gjøre i framtiden. Her tvinges man til å tenke framover og ikke bare se på historikk.

Statoil setter en score fra en til ti på samtlige av faktorene nevnt ovenfor, noe som resulterer i en total trussel. I et sammendrag av trusselen beskriver de hvordan de har kommet fram til det de har kommet fram til. Roy Stranden er skeptisk til å kvantifisere, da det ikke er en matematisk formel som vil gi deg trusselnivået. Han forklarer dette med at det ikke er alle indikatorene som er like viktige alene som de er i kombinasjon med andre, og det er kombinasjonen av de ulike faktorene som er viktig. Denne kombinasjonen fremstiller han i en tabell i risikoanalyseeksempelet han har utarbeidet, se vedlegg 3 (side 14 og 15 i vedlegget). Tabellen vises til under, og må ses i sammenheng med indikatorene beskrevet ovenfor; tilstedeværelse, kapasitet, intensjon, historikk og målvalg.

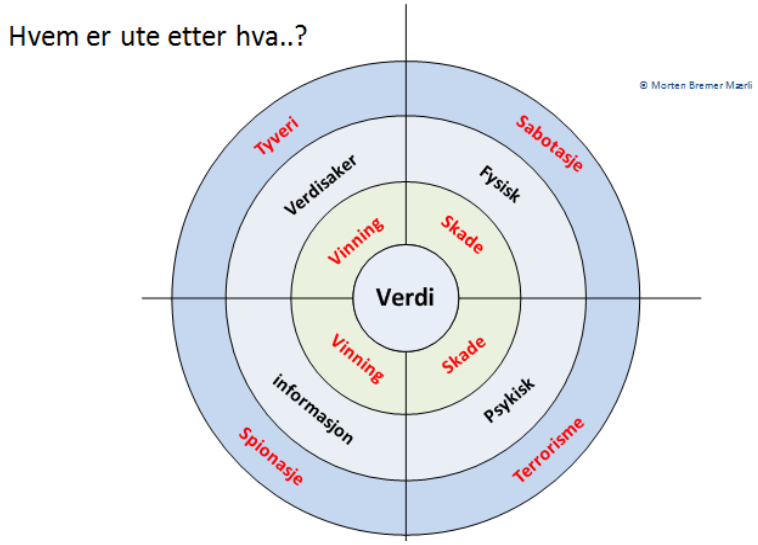
Tabell 4: Kombinasjonen av ulike indikatorer er viktig

Nivå	Beskrivelse
Svært høy	Indikatorene a, b, c og e eller a, b, d og e er til stede.
Høy	Indikatorene a, b, c og d er til stede.
Moderat	Indikatorene a, b, c eller a, b og d er til stede.
Lav	Indikatorene a og b er til stede.
Ubetydelig	Indikatorene a eller b er til stede.

Statoil forsvarer dette med at scoren ikke er basert på gjennomsnitt, men en vurdering av scoren på de ulike indikatorene. Han eksemplifiserer med at det vil være enkelt å gi en total score dersom alle har fått scoren fem. Dersom intensjon har fått ti og resten fem derimot, da må det vurderes mer. Her kommer sammendraget inn i bildet, hvor det gjerne kan komme fram at intensjon bør vektlegges mer enn kapasitet, noe som kan ha sammenheng med at til tross for at trusselaktøren ikke har evne, vil det gjerne bli utført forsøk om og om igjen. Dette må ses i sammenheng med representanten fra Statoil sin understreking av å holde et øye også med trusselaktører som ikke har stor kapasitet, for å sørge får at en fanger opp dersom den skulle stige. På bakgrunn av dette påstår representanten fra Statoil at man kan ha en viss formening om hvem trusselaktøren er, hvor trusselaktøren er og hva han kan komme til å gjøre. Dette utgjør et godt grunnlag for å lage scenarioer i risikovurderingen.

Totalscoren på trussel, blir plassert innennfor ulike trusselnivåer, såkalt ”level of threat (LOT)”. Intensjon og kapasitet er indikatorene som blir vektlagt i størst grad av Statoil.

Morten B. Mærli har utviklet en modell som man kan ta utgangspunkt i når verdien er identifisert. Her kan man se på hvilke trusselaktører som finnes og hva de er interessert i. Du har tyver, sabotører, spioner og terrorister. Intensjonen kan være vinning, informasjon, psykisk og fysisk skade. Han synes modellen er ryddig og grei å bruke og skaper en spennende vinning/skade problematikk. Det fremkommer tydelig av modellen at terrorister er ute etter å gjøre psykisk skade mot en verdi.



Figur 11: Tilsiktede kriminelle handlinger og tilhørende intensjon, utviklet av Morten B. Mærli.

Tabellen nedenfor kan brukes for å finne ut av verdiens attraktivitet overfor trusselaktøren. Summen av disse antakelsene vil ifølge Mærli ha stor betydning for om et mål kan bli ansett som attraktivt, og dermed føre til en økt sannsynlighet for å være et mål for trusselaktøren. En må tenke på hva som skal til for at en verdi vil være spennende og interessant for noen trusselaktører. En petroleumsvirksomhet har flere installasjoner, det bør da gjøres en spesifikk vurdering for hver enkelt. De ulike punktene i tabellen vil ikke nødvendigvis være like relevant for alle virksomheter, slik at noen tilpasninger må gjøres.

Tabell 5: En framgangsmåte for å vurdere verdien eller målets attraktivitet, utviklet av Morten B. Mærli.

	SYMBOL	PERCEIVED AVAILABILITY			POTENTIAL HARM			POTENTIAL GAIN	
ASSET	VALUE	PROTECTION	PREVALENCE	PASSAGE	CASUALTIES	ECONOMY	PEOPLE	SPECIFIC SALEABILITY	GENERAL SALEABILITY
WEIGHT	0	0	0	0	0	0	0	0	1
A1	Low	High	High	Low	High	Low	High	High	High
A2	High	Low	High	High	High	High	High	High	High
A3	Low	Low	Low	Low	Low	Low	Low	Low	Low
A4	High	High	High	High	High	High	High	High	High
A5	Low	Low	High	High	High	High	High	High	High
A6	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium
A7	Low	Low	High	High	High	High	High	High	High

- Er det skade eller vinning?
- Har verdien stor symbolverdi for terroristen?
- Hvordan er tilgjengeligheten (availability)?

- Utbredelse (Prevalence): Hvor mange tilsvarende verdier finnes. Empire State building er for eksempel en verdi med stort symbol og som det bare finnes en av.
- Tilkomst (Passage): Er den lett eller vanskelig å få tak i/komme seg til?
- Beskyttelsesnivå: Er det implementert sikringstiltak?

Tabell 6: Eksempel på vurdering av et mål sin attraktivitet overfor en trusselaktør

Eksempel: Objektet som studeres er en offshore installasjon i Barentshavet.

- Har målet symbolverdi? For noen kan det kanskje symbolisere penger og velstand.
- Mål: Terroristen kan være ute etter vinning (for eksempel miljøaktivister som ønsker å vinne kampen mot forurensning eller terroristen som ønsker å utøve frykt).
- Utbredelse: Ser på antall offshoreinstallasjoner som eksisterer i området det er snakk om. Offshoreinstallasjonene kan da sammenlignes.
- Hvordan er tilkomsten? Det kan være svært vanskelig å komme seg til en plattform med eksplosiver og diverse. Retningslinjen 091 til Norsk olje og gass har regler for tilkomst til installasjoner. Det blir utført flere kontroller. Det er ulike sikkerhetssoner rundt plattformen. Det kan likevel være insidere som er ute etter å sabotere.
- Beskyttelse: Olje- og Energidepartementet har ikke utpekt offshore installasjoner som skjermingssverdige objekter, da de mener offshore plattformer ikke har behov for ekstra terrorbeskyttelse, se s. 16 under NSM.

5.2.3 Sårbarhetsvurdering

Sårbarhet kan forstås som forhold som reduserer eller begrenser evnen til å motstå aksjoner mot mål hvor verdiene finnes. Eksempler kan være alt fra ulåste dører til utro tjenere. Virksomheten må ta for seg innretningen og finne ut hvor de er sårbare, understreker Mærli. Når det gjelder offshore installasjoner må det ikke kun bli sett på plattformen der ute, også helikoptertrafik, supplybåter, basen og lignende er viktig. Det er ifølge Nasjonalt risikobilde (DSB 2010) opprettet ulike forhold som kan påvirke sårbarheten, og som dermed må tas med i en sårbarhetsvurdering. Sårbarheten avhenger blant annet av i hvilken grad trusselaktørene kan forutse iverksatte sikringstiltak. Trusselaktøren kan samle indikatorer og sette sammen den kritiske informasjonen som trengs for å gjøre angrepet til en suksess. Trusselaktørene kan studere og identifisere en virksomhet sine sårbarheter ved og for eksempel utnytte de ansatte som informasjonskilder eller ved å se på bilder. Bilder kan inneholde flere lag med informasjon og vil da være ekstremt verdifulle for angrepsteamet. Radio trafikk, telefon, fax og e-mail har også potensial for å bli utnyttet og er dermed faktorer som må være med i en sårbarhetsvurdering.

”Deter, detect, delay and deny”

I en sårbarhetsvurdering må man ifølge Mærli se på hvilke systemer man har for de fire prinsippene; deter (avskrekke), detect (oppdage), delay (forsinke) og deny (benekte). Disse prinsippene er ifølge Stranden, hentet fra en militær tilnærming hvor hovedprinsippet er at sikkerhet er et null-sum spill, altså kun en vinner.

> *“Angrepsviljen til en terrorist avhenger som regel av deres antakelser om sine egne evner ved eksisterende sikringstiltak (…) Har du høye piggtrådgjerder vil trusselaktøren kanskje velge det objektet som ikke har det (…) I petroleumsindustrien er det sjeldent terrorister angriper fasiliteter som er godt nok sikret” – Morten B. Mærli*

Mærli hevder at trusselaktøren vil anse verdier med stort skadepotensiale som mer interessante. Mål som fra utsiden virker svært godt beskyttet er da gjerne mindre attraktive, og dersom han ikke har en tro på at angrepet vil bli vellykket, vil det gjerne være større sjanse for at trusselaktøren trekker seg tilbake. I de fleste tilfeller vil terrorister altså slå til hvor sårbarhetene til en virksomhet er større enn deres evne til å avskrekke trusselaktøren eller forsvare seg mot tilsiktede uønskede handlinger. Roy Stranden mener det er farlig synsing å tenke at en trusselaktør vil trekke seg fra å gjøre et angrep bare fordi det er godt sikret. Dette begrunner han med at tankegangen hvor man vurderer trusselaktøren ut fra hva man mener er

rasjonelt eller fornuftig ikke vil passe for alle trusselaktører. Det passer kanskje for dem som bare er ute etter økonomisk vinning, men det vil ikke fungere dersom trusselaktøren er ideologisk motivert, mentalt forstyrret eller desperat.

> *"Et eksempel på dette er angrep på amerikanske ambassader både i fredlige land, men spesielt i konfliktområder som for eksempel Afganistan og Kabul. Her har de erfart mange angrep og da er jo ambassaden beskyttet av hundrevis av soldater i tillegg til at ambassaden ligger inne i ISAF-HQ sin leir. Du blir ikke bedre sikret enn det!"- Roy Stranden*

Hvis trusselaktør ikke blir avskrekket må de andre systemene forsøke å hindre at angrepet blir suksessfullt. Uten system for å oppdage trusselaktøren øker muligheten for at han vil komme forbi en hindring, fordi da kan han bruke all tiden han trenger. Mærli eksemplifiserer med David Toska, en av NOKAS ranerene, som brukte hele natten på å bore seg gjennom et tak til en gullsmed, fordi det ikke var deteksjonssystem. Mærli mener det er viktig at man får en "detect" før en "delay" slik at det utgjør en nytte ved at en får mulighet til å stoppe trusselaktøren. Motsatt er det ikke nødvendigvis slik at målet som er mest sårbart er det som blir angrepet. Ifølge Stranden vil en målrettet trusselaktør gå etter målet han har bestemt seg for i forkant, og blir ikke styrt av om målet er lett tilgjengelig eller ikke.

Scenariomodellering

Representanten fra PST sier at man kan teste sårbarheter ved scenariomodellering.
Statoil gjør dette i sin tredje fase; risikovurdering, hvor de ser på identifiserte verdier og trusler opp mot ulike scenarioer og tilhørende konsekvenser. De legger inn konsekvens i forhold til en personell, en finansiell og miljømessig vurdering. De vurderer ulike scenarioer og forsøker å finne ut hvor de er mest sårbare. Statoil har en rekke faktorer de vurderer sårbarhet i forhold til, blant annet gjelder dette; alternative mål, fysisk beskyttelse, prosedyrer, profil. Her ser de også hvilke tiltak de kan iverksette for å redusere sårbarheten. De gjør så samme prosess om igjen med de nye tiltakene inkludert i scenarioet, da spesielt med tanke på trusselaktørens intensjon og kapasitet. PST ser også på hvor effektive de nåværende sikringstiltakene vil være i å hindre et vellykket angrep. Statoil lager scenarioer basert på hver enkelte trusselaktør som er identifisert, fordi ulike trusselaktører kan ha ulik kapasitet. Ved å se på scenarioer mot ulike trusselaktører vil du kunne luke ut de som har lavere intensjon og kapasitet og som ikke er like viktig med tanke på mitigerende tiltak. Representanten fra Statoil understreker derimot at selv om en trussel er lav må en likevel ta de med videre og følge dem hele tiden og ha kontroll på om den øker. At en trussel er lav er ikke et godt nok

argument i seg selv for og ikke ta den med videre, nettopp fordi sårbarheten og konsekvensen kan være høy. Representanten hevder videre at dersom trusselen øker, må sårbarhetene reduseres, slik at virksomheten kan oppnå mer kontroll. En av kritikken Statoil fikk i In Amenas rapporten var at *"det burde ringt noen bjeller."*

> *"Vi trodde nok ikke at vi var så sårbare pga militære styrker, men dersom vi ser på fasiten i ettertid, vil jeg si at trusselen var lav, så har den økt uten at vi klarte å fange det opp"* - Representant Statoil.

Scenarioene til PST og Statoil baseres på:

- Kunnskapen de besitter som analytikere.
- Historikk/hendelser nasjonalt og internasjonalt
- Pst nevner også strategiske vurderinger og her og nå vurderinger basert på interne og internasjonale vurderinger som de har tilgang til om for eksempel kapasitet.
- Representanten fra Statoil nevner også at de forsøker å sette seg inn i trusselaktørens hode ved at de tenker ut fra angripers synspunkt og beveger seg slik de selv ville gjort i dette scenarioet om de var trusselaktøren. "Man bør være dyktig å kjenne fienden, vite hvor man er svak og hvor sårbarhetene ligger, dette må dermed beskrives så godt som mulig" Statoil ender opp med en automatisert score, som forteller hva risikoen er.

5.3 Syn på eksisterende metodikk og bruk av sannsynlighet

5.3.1 Egne metoder for Safety og Security

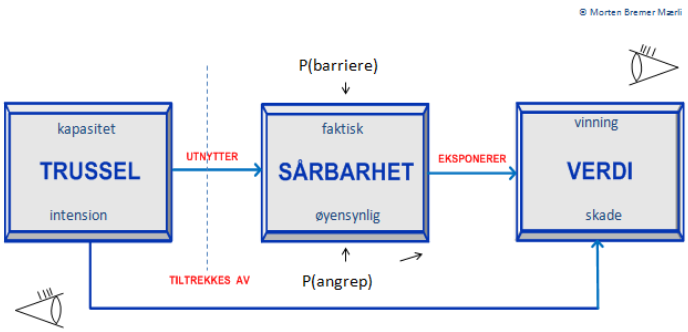
Det er uenighet om det bør være egne metoder for Security og Safety og hvorvidt sannsynlighet kan være en del av metodikken. Funnene tyder på at fagfolk innenfor Securityfeltet ønsker ulike metoder, og fagfolk innenfor Safety mener metodikken bør være noenlunde den samme for å sikre helhetlig risikostyring. PST og NSM mener også man trenger egne metoder for å analysere terror trussel. Dette begrunner de med vanskeligheten eller umuligheten ved å bruke sannsynlighet blant annet på grunn av mangel på historisk data, trusselens natur eller faren for å utnytte tallmateriale. PST jobber mye med å få deres metodikk, den nye standarden inn i den totale virksomhetsstyringen, men representanten hevder det er vanskelig og utfordrende fordi virksomheter da må si noe kvalitativt og plassere det inn i noe kvantitativt. Han innrømmer at de ikke har funnet noen løsning på det.

”Nei vet du hva, dette vrir jeg hjernen min på nesten hver dag. Jeg er nok ikke smart nok til å komme fram til noe” - Representant fra PST

Alle informantene utenom representanten fra Proactima og en av GDF Suez sine representanter sier ved flere anledninger i intervjuet at vi ikke kan bruke sannsynligheter for om et angrep vil oppstå. Jeg tolker det som at PST og NSM er de som er sterkest imot sannsynlighetsbegrepet. Det er derimot flere som likevel snakker om og bruker sannsynlighet i ulik grad i sine analyser. Dette skal vi komme til senere. Først skal vi se på hvorfor informantene mener at vi ikke kan bruke sannsynlighet på dette området. Morten B. Mærli mener forskjellen er så stor mellom Safety og Security, slik at man ikke kan ha samme metodikk, samt at man må se bort ifra sannsynlighet.

”Tror du skal være forsiktig med å gjøre en analyse samtidig, det er to verdener”- Morten B. Mærli

Han mener vi bør følge det som står i prNS 5832 ved å gjøre en vurdering av verdi, trussel og sårbarhet. Han begrunner hvorfor ved å vise til en egenprodusert modell:



Figur 12: Modell som viser hvorfor man ikke kan bruke sannsynlighet for om angrep vil oppstå (Morten B. Mærli).

En trusselaktør (T) har en kapasitet og intensjon. Trusselaktøren kan utnytte en operatør sin sårbarhet (S) for å eksponere en verdi eller objekt (Konsekvens). Verdien har noen egenskaper som gjør den interessant og attraktiv for trusselaktøren fordi det er et potensial som er knyttet til at det kan gi skade på verdien eller vinning for trusselaktøren, alt etter hva han er ute etter å oppnå, se figur 11 og tabell 5. Det er altså en tiltrekning der som er med på å styre angrepssannsynligheten P (A). De har en antakelse om sårbarheten og kan enten bli avskrekket og tror ikke at de vil klare å gjennomføre et angrep eller de kan se muligheten og

gjør så en kost-nyttevurdering av verdien. En kost-nyttevurdering vil da gå på deres antakelse om måloppnåelsen mot innsatsen og kostnadene som blir lagt i angrepet. Alt dette ligger altså bak angrepssannsynligheten og ifølge Mærli kan man ikke si noe om denne fordi det er noe som trusselaktøren eier.

> ”Virksomheter kan ikke ha kontroll på trussel, det er en ferskvare. Det de må gjøre er å si at de skal beskytte seg mot den og den type trussel.” - Morten B. Mærli

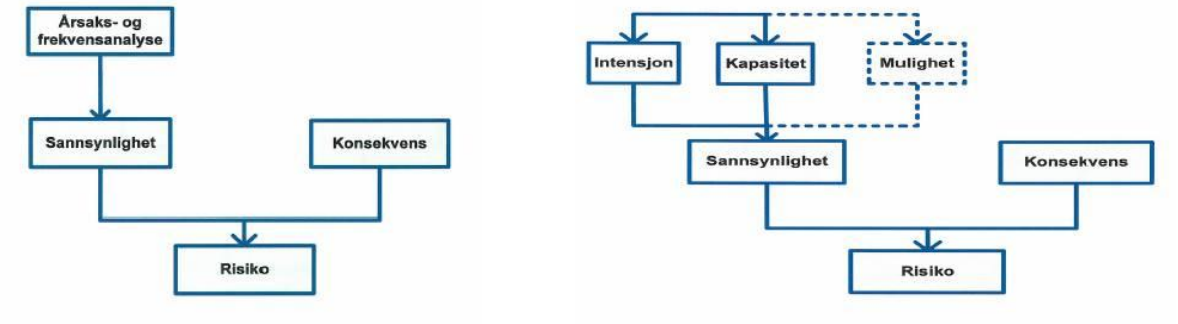
Vi må derfor, påpeker han videre, ta utgangspunkt i at P (A) = 1, som i 100 prosent. Man må altså gå ut ifra at det vil skje. Nedenfor vises til et sitat, før en gjennomgang av informantenes argumenter mot bruken av sannsynlighet.

> *”På sikringssiden må du bare erkjenne at det er en mulighet for at dette kan skje, uavhengig av sannsynlighet. Trenger ikke prøve å tallfeste den på en måte. Du kan ikke prøve å regne deg vekk fra at dette er en mulighet” - Representant fra Ptil.*

5.3.2 Argumenter mot bruken av sannsynlighet

> *”Alt koster penger. Dersom en ikke har noen hendelser å vise til så er det vanskeligere å få ressurser (…) Nå viser det seg tilslutt at glemmer du statistikken og sannsynligheten, da er det eksempler på at ting kan skje” - Representant fra Ptil*

Ifølge representanten fra NSM foregår det en stor metodediskusjon i en del fagmiljøer i forhold til bruken av historiske data og statistikk på sikringsområdet.



Figur 13: Forskjellen på Safety risik (t.v.) og Security risiko (t.h.) (Morten B. Mærli).

Figur 13 viser forholdet mellom Safety og Security risiko. Ved analyse av Safety risiko kan det gjøres en årsaks - og frekvensanalyse, og på bakgrunn av det bli sagt noe om

sannsynligheten. Mens for Sikringsrisiko kan man ikke gjøre en årsaks- og frekvensanalyse, der må man se på trusselaktørens intensjon, kapasitet og mulighet. Mærli påstår at man ikke kan anslå sannsynlighet på intensjon og kapasitet. Mulighet kan en operatør bidra med å styre ved å sette inn sikringstiltak, dermed er det mulig å anslå sannsynlighet for om et forsøkt angrep gitt at det finner sted, vil være vellykket.

> *"Det blir meningsløst å prøve å basere seg på statistikk, en frekvens av tilsiktede hendelser over tid" - Representant fra DSB.*
>
> *"Selv om du legger inn en form for kalkulasjoner i et datasystem, vil den ene hendelsen, være så lite signifikant, at den vil ikke statistisk gi noe godt ut av det. Du får nok et tall som er ganske lite vil jeg tro" - Representant fra Ptil*
>
> *"Snakker man om lavfrekvente hendelser, vil du jo alltid få et lavt tall. Naturlig nok. Slik at beslutningsgrunnlaget vil bli feil" - Representant fra PST*

Som sitatene ovenfor beskriver vil beslutningsgrunnlaget bli feil dersom det fastsettes sannsynlighet basert på historisk data, i den forstand at tallet som kommer fram vil være svært lavt, dermed vil det ikke bli prioritert ressurser til å implementere sikringstiltak. Representanten fra PST eksemplifiserer med terrorscenarioet til DSB i det nasjonale risikobildet hvor det ble sagt at det var en sannsynlighet på 0,01 per år over 10 000 år. Han stiller seg undrende til hvordan de kom fram til dette tallet, og lurer på om de i det hele tatt vet det selv. I tillegg stiller han seg kritisk til hva det egentlig betyr. PST var med og kvalitetssikret dette og de klarte å fjerne tallet som var blitt satt. Hadde det blitt satt inn i en NS 5814 metodikk ville man ifølge representanten fra PST fått at et resultat hvor det overhode ikke fantes noen fare for terrorisme i Norge. Det ville blitt så lavt at man ikke hadde trengt å ta hensyn til det. Hvis vi tenker tilbake på 22. Juli og bombeangrepet på regjeringskvartalet, så er det mye som tyder på at folk anså sannsynligheten som liten. Hadde sannsynligheten blitt sett på som høy derimot, hadde nok gata blitt sperret med en gang. Representanten fra NSM sier at verdien av et objekt kan være så viktig og konsekvensene av et eventuelt angrep mot disse vil være så høye at en må sikre objektet uansett. Det spiller ingen rolle hvilken sannsynlighet hendelsen nevnt overfor hadde for når det skjer må en være forberedt.

”Dersom man skulle satt sannsynlighet på 22. Juli så ser man at hele metodikken faller på sin egen urimelighet, fordi situasjonen kan endre seg drastisk. ”det er i mine øyne, (derfor) helt umulig (…) Nei, vil ikke tenke på sannsynligheter, veldig vanskelig begrep å bruke” - Representant fra PST

"Trusselbilde endrer seg konstant” - Representant fra PST

En annen årsak til diskusjonen om bruk av sannsynlighet i forbindelse med terror er at trusselen er tilpasningsdyktig. En trussel kan endre seg svært raskt for eksempel på grunn av et sikringstiltak som har blitt iverksatt. Sannsynligheten for angrep bestemmes/eies av trusselaktørene hevder Mærli som nevnt overfor.

”Man har å gjøre med trusler, og da må man i stedet for tradisjonelle sannsynlighet x konsekvens gå inn og vurdere å ha oversikt over faktisk intensjon og kapasitet til faktisk eksisterende aktører” – Representant fra DSB.

”Dette med sannsynlighet funker ikke (…) Det er ikke slik du forutser hendelser basert på menneskelig rasjonalitet” - Representant fra Statoil

”Du må bare glemme å tro at du skal kunne skrive ned og planlegge at det er akkurat dette som kan skje, hvor og når. Det går ikke” - Representant fra Ptil

Historisk sett ser man ved terrorisme at det ene angrepet ikke kommer en gang til, det er en ny sak. Terroristen ønsker å skape frykt og ønsker ikke å bli hindret i å utføre angrepet. Som et resultat av dette kommer angrepene ofte på en uventet måte til et uventet tidspunkt. Videre hevder representanten fra Ptil at å sette sannsynligheter for at dette skal kunne skje bare vil være en avsporing. Sannsynlighet med bakgrunn i historisk data og statistikk fører til at en ofte ser på hva forrige trusselaktør prøvde på og gjør oss på den måten alltid klare til forrige krig, hevder representanten fra Statoil. Man kan da glemme at motparten tenker ut noe nytt og da kan man ofte havne bak. Her blir det nyttig med scenariomodellering som mange av representantene nevner at de gjør og bruk av ekspertvurderinger i et forsøk på å forutse hva som kan skje i framtiden, og ikke bare basere seg på hva som har skjedd i fortiden. Dette tar også Statoil hensyn til når det ser på ”future anticipated targeting, se s. 56.

”Du kan ikke bruke sannsynlighet på trusselen, men muligheten for barrierebrudd eller suksessfullt angrep”- Morten B. Mærli

Dette gjøres ved å se på verdiens attraktivitet som nevnt ovenfor, se tabell 5. Da må en tenke hvilke spesifikke trusselaktører som er interessert i spesifikke mål. Mærli forklarer hvordan vi kan sette sannsynlighet for suksessfullt angrep eller barrierebrudd ved bruk av samme figur

som han mener viser hvorfor vi ikke kan sette sannsynlighet for om angrep vil oppstå, se figur 12. Operatøren som illustreres øverst til høyre på figuren må se på sine verdier og sårbarheter. Dette er noe som operatøren vil eie ifølge Mærli. Det er her skille går mellom P(A) og P(B), som er sannsynligheten for barrieresvikt. Operatøren kan sette inn tiltak for å redusere sårbarheten. Man kan sette sannsynlighet på dette området fordi denne sannsynligheten er avhengig av investering i sikring eller sårbarhet. Her kan man ifølge Morten B. Mærli kjøre workshops og scenarioer med utgangspunkt i at operatøren har en trusselaktør som ønsker å angripe. Representanten fra Proactima foreslår å bruke et hendelsestre for å si noe om sannsynligheten for om et angrep blir suksessfullt. Mærli framstiller dette ved hjelp av noen formler.

Risiko = Sannsynlighet (P) x Konsekvens (C).
Safety Risik = P (frequency) x C (arbitrary).
Security Risk = P (Intensjon, kapasitet) x C (Optimized)

Risk = Threat x V(X) = P (I, K) x P (barrier) x L (X)

Formelen ovenfor står for: Risko = trusselen x sårbarheten til verdien = Sannsynligheten for angrep x Sannsynligheten for barrieresvikt x Tap av verdi.

5.3.3 Like metoder for Safety og Security

DSB mener de nye standardene som omhandler tilsiktede handlinger har snudd opp ned på terminologi og framgangsmåte enn hva de er kjent med fra blant annet ISO 31 000 som er blitt en anerkjent standard innenfor risikostyringsfaget, se figur 1. Rerepsentanten fra Proactima er enig i at NS 5830-serien går i mot ISO 31000, og reagerer sterkt på at standardene har snudd opp ned på betydningen av risikovurdering og risikoanalyse, at de har innført ny definisjon av risiko og innført nye begrep, som for eksempel ren risiko. Å komme med nye standarder er ikke alltid bra hevder han videre og begrunner med at det blir vanskelig å forholde seg til mange ulike systemer. Dette påstår han bidrar til å ødelegge intensjonen med den helhetlige og enhetlige risikostyringen slik det anbefales i ISO 31000

> *"Jeg er litt skeptisk fordi vi har ISO 31000 som legger til rette for at du kan få til en helhetlig risikostyring i virksomheten, så kommer det en NS som på en måte gjør noe helt annet (...). Det oppstår da et skille mellom Safety og Security, der Security blir en boks stående alene, en egen verden, noe som fører til at resultatet en kommer fram til blir vanskelig å implementere i resten av risikostyringen" - Representant fra Proactima*

Han er enig i at man må se på verdi, trussel og sårbarhet, men han skjønner ikke hvorfor det skal distanseres fra resten av risikostyringen. Han er bekymret over at den nye standarden krever en helt ny kompetanse og risikoforståelse i virksomhetene. Dette mener han vil være problematisk når det allerede jobbes så mye med å få en helhetlig risikostyring i virksomhetene til å fungere. Dersom sikringsrisiko blir separert fra resten av sikkerhetsstyringen, tror han eierskapsfølelsen vil forsvinne. Han hevder det er viktig at de ansatte har eierskap til analysen, slik at den blir brukt i etterkant av selve analyseprosessen. Det er synd dersom analysen ikke blir brukt når det ofte går mye ressurser med i et analysearbeid. Ved å være bevisst på omfang av analysen og beskrivelse av analyseobjektet, samt fylle inn elementer der det kreves, så vil den eksisterende metodikken som finnes på Safety hendelser dekke mye av intensjonen med prNS 5831 og prNS 5832.

> ”Den nye standarden beskriver hvilke tiltak som er fornuftige å iverksette og det er jo det vi gjør i andre deler av risikostyringen også. Det som står i den nye standarden blir egentlig ivaretatt gjennom den tradisjonelle risikostyringen” - Representant fra Proactima

Hos GDF-Suez fikk jeg litt ulike innfallsvinkler på spørsmålene jeg stilte. Representanten med bakgrunn i tradisjonell risiko tenkning mener man kan bruke de tradisjonelle analysene, beskrive kontekst og dermed si noe om sannsynlighet og konsekvens. Representant med Securitybakgrunn er klar over prNS 5832 som blir beskrevet nedenfor og ser behovet for å ha en egen metodikk som avdekker verdi, trussel og sårbarhet.

Statoil og Talisman har utviklet deres egen metodikk hvor de bruker elementer fra Safety og Security. De vurderer både verdi, trussel, sårbarhet og gjør med utgangspunkt i dette en risikoanalyse hvor de i workshops kommer fram til scenarioer. Statoil har klokketro på deres nye styringssystem for Security og mener boblediagrammet de framstiller risikoen på åpner opp for gode diskusjoner og illustrerer en del gode problemstillinger. Talisman-Energy mener de ikke har kommet like langt på Security som for Safety, men de inkorporerer begrepet mer nå enn før i deres Safety and Security risk Assessment. Mærli tror ikke det går an å lage en modell som sammenkopler Security analyse og Safety analyse. Du blir bare nødt å ha et ledelsessystem som fanger opp begge.

5.3.4 Argumenter for bruk av sannsynlighet

> *"Du kan alltid snakke om sannsynlighet uansett"- Representant fra konsulentselskapet Proactima*

Det er bare snakk om hvilken bakgrunnsinformasjon du har påstår han. Du kan ha god og sterk eller svak og dårlig bakgrunnsinformasjon. Dersom man kjenner området man jobber i, for eksempel vet hvilke trender og trusselaktører som finnes, hvilke selskap som blir rammet og hvilken risikoprofil man har så kan man si noe om sannsynlighet, sannsynlighet som et mer kvalitativt begrep. Han ser nytten av å se på trussel, verdi og sårbarhet, men de mener han er komponenter i sannsynlighetsdimensjonen. Hvis man har en høy trussel og er sårbar samtidig som man har verdier som er attraktive, så betyr det at sannsynligheten er høyere. Man trenger ikke statistikk for å skjønne det hevder han. Det er likevel en form for sannsynlighet. Informantene som mener vi ikke kan bruke sannsynlighet har selv snakket om dette, men likevel sier de at det blir feil å snakke om sannsynlighet for sikringsrisiko.

> *"Det er et eller annet jeg ikke forstår, hvorfor det skal være så kontroversielt å bruke subjektive sannsynligheter" Representant fra Proactima.*

Det å skylde på mangel på historisk data blir feil ifølge representanten fra Proactima. Innenfor Safety og Storulykke problematikk er det heller ikke har mye data. Han kommer med et eksempel at han nå jobber med storulykker i Nordsjøen, blant annet alvorlige gasslekkasjer. Den siste store ulykken der var Piper Alpha i 1988.

> *"Vi har ikke data vi heller. Vi er i samme situasjon, men fordi om du ikke har data så kan du likevel snakke om sannsynlighet. Du trenger ikke data for å snakke om sannsynligheten. Der tror jeg de misforstår litt. (...) Man må snakke om sannsynlighet for å kunne prioritere hvor man skal få ressurser til å sette inn tiltak" – Representant fra Proactima*

Mærli, PST og flere av de andre informantene har snakket om dette med at det kan være større sjanse for at en verdi blir utsatt for angrep enn en annen, og at høy sårbarhet reduserer verdiens attraktivitet, osv. Dette kan tolkes som indirekte sannsynlighet. Representanten fra Proactima tror egentlig at man tenker mer likt enn de (som er i mot sannsynlighet på) tror. Til tross for at han er veldig sikker i sin påstand om at man kan bruke sannsynlighet, kan han ikke si akkurat hvordan, slik at man kommer i mål. Han mener en må sette seg sammen og se på det på tvers, og slik komme fram til en framgangsmåte. Videre påpeker han at man må ha

fokus på endring av trender. Først da kan man lage oss et godt bilde av hvilke hendelser som er relevant for en virksomhet eller ikke.

5.3.5 Tvetydige svar

I starten av intervjuene er både PST, NSM, DSB, Ptil, Statoil, Talisman-Energy, samt en av representantene fra GDF helt klare på at man ikke kan bruke sannsynlighet. Noen virker likevel litt mer usikre etterhvert eller bruker andre begreper som kan forbindes med sannsynlighet, slik som blant annet; muligheten, sjansen for og rimelig. Et eksempel er en av representantene fra DSB, som sier:

> *"Det vi ønsker å forholde oss til er det vi kaller rimelige verstefall scenarioer, men vi diskuterer ikke egentlig sannsynlighet for terrorisme for å si det sånn" - Representant fra DSB.*

Det virker som at flere på en indirekte måte bruker og tenker sannsynlighet, til tross for at de sier de ikke gjør det. Representanten fra PST er klar over dette problemet og viser til svakheter ved det norske språk, da det bare finnes ett ord for sannsynlighet, i motsetning til de engelskspråklige begrepene "Probability" som ofte refereres til matematisk sannsynlighet og "Likelihood" som refereres til en mer hverdagslig sannsynlighet.

Vanskelig å prioritere uten sannsynlighet

Representanten fra PST ser at det kan bli vanskelig å prioritere og å gjøre avveininger om hvor en skal sette inn ressurser til sikringstiltak når en ikke bruker sannsynlighet og hevder at vi i stedet for må være ekstremt gode til å skrive. Representanten fra DSB er også usikker hvordan en på best mulig måte vurderer mest relevante og rimelige scenarioer når det ikke er satt noe sannsynlighetstall. Videre kan representanten fortelle at de baserer seg mye på verdivurderingene som kommer fra PST. En av representantene snakker om dominerende diskurs og ulike tolkninger av risikofenomen når de skal vurdere hva som er rimelige scenarioer eller ikke. Skytinga på Utøya 22. Juli 2011 kom litt utenfor den dominerende diskurs påstår han.

> *"Å forberede oss på det uventede er en kjempe utfordring (...) Greia er å forstå de diskursene vi er en del av selv og prøve å gå utenfor det" – Representant fra DSB*

Mest sannsynlig og Worst-Case scenario

Til tross for at informantene sier at de ikke bruker sannsynlighet er et vanlig skille blant flere av dem mellom scenarioer som er mest sannsynlige og scenarioer som beskriver ”worst-Case”. DSB ser kun på Worst-Case scenario som har lav sannsynlighet for å inntreffe, men som vil få høye konsekvenser. Dette er en avgrensning de gjør i det nasjonale risikobilde. Worst case scenarioer skal for DSB være rimelige, realistiske og tenkelige. Rimelig i den forstand at det har skjedd før enten i Norge eller andre land, det skal kunne skje i morgen eller i dag. For å kunne si noe om dette har de ulike avgrensningskriterier om hva som faller innenfor og utenfor. Noen eksempler på forutsetninger er at hendelsen skal kunne medføre tverrsektorielle konsekvenser og håndtering, ekstraordinær myndighetsinnsats og hvis mulig og relevant skal scenarioene bygge på tidligere hendelser. Det er nyttet stor usikkerhet til Worst-Case scenarioer siden det finnes lite data og liten erfaring. Statoil prioriterer det som er farligst og som de kaller dominerende risiko. Da er det det scenarioet som gjelder og som må jobbes med først. Når de har fått det ned vil en ny dominerende risiko fremkomme. Representanten sier at det er opp til hver enkelt virksomhet som skal ta risikoen og prioritere mellom disse to alternativene. Basert på hvilke scenarioer en prioriterer vil en komme fram til ulike sikringstiltak. Denne avgjørelsen må bli tatt basert på virksomhetens verdier. Representanten fra Petroleumstilsynet sier at virksomhetene må forsøke å veie dette og gjøre kost-nytte vurderinger.

> *”Hvis du mener at verdiene dine er så viktige for deg og samfunnet, vel da er det verstefallsteorien du må gå etter, fordi konsekvensene ved tap er så ekstrem at du må beskytte deg mot verstefall (…) Vi prøver å nivellere det veldig for å gi våre kunder en form for gyllen middelvei” Representant fra PST.*

6 DRØFTING AV FUNN OPP MOT TEORI

Security kan på mange måter ses på som et ja eller nei spørsmål, med det menes at enten har du det eller ikke. Utfordringen er at i den virkelige verden, så er det ikke så lett. Selv om du jobber med og prioriterer sikkerhet så er virkeligheten slik at dette bare er en av flere ting som må tas hensyn til. Et sentralt spørsmål blir dermed hvordan du kan balansere mellom begrensede ressurser og ubegrensende forventninger (Stranden, 2013). Her kan en risikobasert tilnærming til usikkerhet være en mulig måte å håndtere dette på. En risikovurdering blir nødvendig for at beslutninger om prioritering av ressurser kan tas.

6.1 To overordnede framgangsmåter for risikoanalyse og vurdering

Funnene mine viser at det er to overordnede måter å gjøre analyser og -vurderinger av sikringsrisiko i Norge. På den ene siden har du ISO 31000 som beskriver risikostyringsprosessen innenfor Safetyfeltet, samt NS 5814 som inneholder forslag til framgangsmåte for risikovurdering. På den andre siden har du innenfor Securityfeltet en rekke standarder, som enda ikke er godkjent, men som blant annet beskriver en tilnærming til risikohåndtering, samt krav til risikoanalyse for tilsiktede uønskede handlinger. Standardene som gjelder tilsiktede handlinger presenterer en rekke ulike begreper og framgangsmåter som er ukjente blant fagfolk innenfor Safetyområdet og som skiller seg fra de anerkjente standardene de er vandt til å bruke på alle slags type risikoer. En viktig forskjell er analyse- og vurderingsbegrepet. Ifølge prNS 5832 vil en risikovurdering inngå i en risikoanalyse, men for NS 5814 vil en risikoanalyse inngå i en risikovurdering. Framgangsmåten er annerledes ved at NS 5814 identifiserer farer og uønskede hendelser før konsekvens (eller verdi). prNS 5832 vurderer konsekvens i forbindelse med bortfall av verdi før trusler (farer) og deretter utarbeides scenarioer eller identifikasjon av uønskede hendelser. I tillegg avvises bruk av sannsynlighet i prNS 5832. De nye standardene for tilsiktede handlinger, er kjent blant alle informantene, men i ulik grad. Det er uenighet hvorvidt det bør være en egen standard spesifikt for sikring som viser til helt andre begreper og framgangsmåter. Jeg oppfatter at den største og mest intense uenigheten og diskusjonen lander på i hvilken grad sannsynlighet kan brukes i en analyse/vurdering av terror.

6.2 Ulemper med sannsynlighet i forbindelse med analyse av sikringsrisiko

Mine funn viser at det er flere karakteristikker ved sikringsrisiko og spesielt terrorisme som gjør at en ikke bør benytte sannsynlighet i en analysesammenheng. Disse karakteristikkene blir også beskrevet av Albrechtsen (2003). Terrorisme innebærer mye strategisk og epistemisk usikkerhet. Renn (2008) påstår at usikkerhetsmomentet fordrer store krav til hvordan risikoen bør vurderes og bearbeides.

En kort oppsummering av mine funn som beskriver hovedårsakene til den store graden av usikkerhet:

1) Mangel på historisk data, samt at usikkerheten ofte må håndteres før en har klart å innhente tilstrekkelig informasjon.
2) Trusselaktørene er ofte rasjonelle og kalkulerende, samt tilpasningsdyktige og fleksible.
3) Trusselaktørene er uforutsigbare i forhold til tid og sted. De gjennomfører uforutsette aksjoner i den hensikt å forårsake betydelige skade og/eller dødsfall.

6.2.1 Mangel på historisk data

Innenfor områder hvor man har masse historisk data vil det være mulig å ta i bruk statistisk og matematiske kalkulasjoner for å fastsette en sannsynlighet. Dette gjelder for eksempel i forbindelse med trafikkulykker. På grunn av det empiriske materialet vil det være mulig å benytte mer presise sannsynligheter, basert på ulike kalkulasjoner. På bakgrunn av det kan det uttrykkes med stor grad av sikkerhet omtrent hvor mange bilulykker som vil inntreffe i løpet av et år. Ingen kan si noe sikkert om framtiden, men det vil være mye relevant data som gjør at prediksjonene som blir gjort kan ses på som pålitelige. Dersom en skulle brukt de få historiske dataene som eksisterer i forbindelse med terrorhandlinger mot petroleumssektoren ville sannsynligheten blitt svært lav, noe som igjen ville påvirket risikobildet. Til tross for at konsekvensene hadde blitt vurdert som store, ville sannsynligheten ført til at risikoen ble nærmere ubetydelig. En slik tilnærming til risiko framstilles ofte i en risikomatrise. Slik vil beslutningstaker få en oversikt over både sannsynlighet, konsekvens og dermed den totale risiko. Aven og Krohn (2013) påpeker at hendelser som blir ansett som svært usannsynlige, har en tendens til å bli ignorert eller neglisjert i en risikovurdering. Dette tenker jeg kan føre til at beslutningstakere ikke vil være villige til å investere tid eller penger i å beskytte seg mot

noe som mest sannsynlig ikke vil finne sted. Et resultat av det er at ressurser til iverksetting av sikringstiltak ikke blir prioritert. Sikkerhet er som nevnt ovenfor bare en av mange områder som må tas hensyn til. Risiko har ikke bare en nedside, men også en oppside. Det vil si en mulighet for gevinst (Stranden, 2013). Eksempler på gevinst er økonomisk fortjeneste, eller friheten til å gjøre hva man vil. Fremstilles sannsynligheten som svært liten, kan det tenkes at beslutningstaker vil foretrekke oppsidene ved risikoen, ved å unngå et betydelig pengebruk på sikringstiltak og ved å unngå begrensninger av den enkeltes frihet, slik som informanten fra Talisman understreket:

"Vi vil ikke ha kamera på toalettet"

Dette kan ses i sammenheng med påstenden til Aven og Renn (2010) om at balansen mellom kost-nytte ofte har en avgjørende betydning for i hvilken grad risikoreduserende tiltak blir sett på som berettiget eller ikke. Jore og Moen (2014) hevder dette blir enda mer komplisert i forbindelse med sikring på grunn av den høye graden av usikkerhet. Terrorangrepet på regjeringskvartalet, 22. Juli 2011 og gisseltakingen på gassanlegget In Amenas i Algerie, 16. Januar 2013 er to eksempler hvor det ikke var iverksatt tilstrekkelige sikringstiltak, noe jeg tolker har bakgrunn i en antakelse om svært lav sannsynlighet.

Nå må det sies at risikoanalysefaget har utviklet seg veldig fra 1970-tallet. Ved svært usikre risikoer ser man bort fra frekvens og matematiske kalkulasjoner som en måte å fastsette sannsynlighet. Renn (2008) grupperer risikoer i ulike kategorier; enkle, komplekse, usikre og tvetydige, hvor de tre sistnevnte betegnes som systemisk risiko. Eksempler på enkle risikoer er trafikkulykker og butikktyveri. Man kan rimelig godt forklare årsak-konsekvens forholdet dersom en beruset person kjører bil og krasjer. Piper Alpha og massakren som fant sted 22. Juli derimot er eksempler på systemisk risiko. Renn (2008) hevder at man må tilnærme oss slike risikoer på ulike måter. Den Bayesianske tilnærmingen til risiko understreker at sannsynlighet ikke er en objektiv sannhet eller en korrekt sannsynlighet, men en subjektiv vurdering som blir gjort med basis i eksisterende bakgrunnskunnskap. Dersom en ser sannsynlighet på denne måten, som subjektiv og kunnskapsbasert, uten bruk av kalkulasjoner og statistikk, vil det likevel være utfordringer knyttet til bruken. En utfordring er dersom det settes ulike akseptkriterier som det ofte blir gjort i forbindelse med sannsynlighet. Ved fastsettelse av akseptkriterier ligger det et maktaspekt i og med at den som har mest makt kan utnytte sannsynligheten ved å plassere den i en lavere risikokategori enn den kanskje burde

være i, nettopp for å slippe og investere i dyre sikringstiltak. En annen utfordring er dersom det på bakgrunn av eksisterende informasjon blir satt en høy grad av sannsynlighet, og det ikke oppstår noe angrep over lang tid, vil det kunne føre til en falsk oppfatning om at sannsynligheten er feil, dermed blir den fastsatte sannsynligheten kanskje redusert.

Historisk data er likevel ikke så interessant for diskusjonen om sannsynlighet kan tas i bruk, da det ikke er den probabilistiske usikkerheten, men den strategiske usikkerheten som i størst grad avgjør om det er relevant å gjøre prediksjoner om sannsynlighet. Dette kan forklares med at dersom de eksisterende angrepene mot installasjoner har blitt gjennomført når sikringstiltak har vært fraværende, vil ikke nødvendigvis sannsynligheten som kommer fra statistisk materiale ha gyldighet for fremtidige prediksjoner dersom denne forutsetningen endrer seg og tiltak blir iverksatt. Dermed blir punktet som Statoil vurderer ”future anticipated targeting” særlig relevant. Utfordringen her er at det blir vanskelig å se i hvilken grad sikringstiltak fungerer eller ikke, nettopp fordi fravær av angrep ikke er ensbetydende med at tiltakene har vært suksessfulle. Det kan tenkes at virksomheten aldri var et mål for trusselaktøren i utgangspunktet. Jeg er usikker på om den bayesianske tilnærmingen får frem forståelsen av at det ikke nødvendigvis er grad av sårbarhet som avgjør om et angrep blir forsøkt, men hvorvidt trusselaktøren har valgt ut den spesifikke virksomhet som mål. Dersom en virksomhet gjennom hele sin levetid aldri har blitt utsatt for et terrorangrep, betyr ikke det nødvendigvis at verdiene de sitter på ikke er attraktive eller at de har liten sårbarhet og dermed klart å avverge det. Virksomheten kan sitte på store verdier og være svært sårbare, men likevel aldri bli angrepet fordi trusselaktøren gjerne aldri har hatt den spesifikke virksomheten som sitt mål og dermed ikke hadde tenkt å gjennomføre angrep i utgangspunktet. Dette kan skyldes at trusselaktøren ikke har visst om virksomheten eller at andre mål har vært mer attraktive. Bestemmer trusselaktøren seg for å gå for det målet likevel, da vil man se hvor store sårbarhetene egentlig er. Man kan reflektere over i hvilken grad virksomhetene selv kan sitte og styre dette, og i hvilken grad de er prisgitt at noen plutselig velger å angripe dem eller ikke. Problemet er at man aldri kan vite om terroristen slår til i dag, i morgen eller om 50 år. På den måten vil sannsynlighet være lite egnet til å kommunisere budskapet når trusselaktører med en intensjon er involvert.

6.2.2 Trusselens natur

Trusselaktørene har en intensjon og en kapasitet. De ønsker å oppnå et mål og går ofte strategisk fram for å oppnå dette målet. De er i mange tilfeller dermed rasjonelle og

kalkulerende. En terrorist, med unntak av selvmordsbombere, er opptatt av egen sikkerhet, samtidig ønsker alle å lykkes med sitt angrep, dermed vil trusselaktøren veldig ofte selv innhente informasjon fra blant annet åpne kilder. Basert på den innsamlede informasjonen vil de gjerne gjøre egne risikoanalyser og – vurderinger. Dersom trusselaktøren avdekker deres utvalgte mål sine sikringstiltak og blir avskremt, vil sannsynligheten reduseres. Trusselaktøren kan dermed velge å gå for en annen verdi, eller et annet mål. Motsatt vil sannsynligheten øke dersom terroristen avdekker sårbarheter som de kan utnytte. For Safety risiko, slik som teknisk feil eller naturkatastrofe, vil ikke sikkerhetstiltak føre til en forandring i hvordan trusselen/farekilden pålegger systemet risiko. Graden av feil på systemet, eller utfallet av disse feilene kan variere som en følge av tiltak, men det kan ikke selve den initierende hendelsen. Uavhengig av om trusselaktøren får tak i spresifikk informasjon angående sikringstiltak eller sårbarheter, kan informasjon om sannsynligheten som er satt, gitt at de blir avdekket av trusselaktøren, være selvoppfyllende i den forstand at trusselaktøren tolker en høy grad av sannsynlighet som at det er flere sårbarheter som kan utnyttes og at det er attraktive verdier på spill, dermed øker incentivet til å angripe. Dette fører til svært unike egenskaper ved sikringsanalyser i forhold til en analyse av ikke tilsiktede hendelser. I tillegg må det understrekes og tas hensyn til i vurderinger, at ikke alle terrorister er rasjonelle, noen handler i affekt eller er mentalt forstyrret, da skal det ikke mer til enn en uttalelse fra en politiker i media eller en karikaturtegning av en profet som provoserer.

6.2.3 Uforutsigbarhet

Trusselaktøren er som man kan se i avsnittet ovenfor tilpasningsdyktig og fleksibel ved at de kan endre hvordan, hvor og når de skal angripe. Dette gjør at en trussel kan endres raskt, som igjen fører til en økt uforutsigbarhet. Sannsynligheten som er satt i dag, kan være totalt annerledes i morgen. Det vil være utfordrende om ikke umulig for virksomhetene å holde følge med dette. Å sette en subjektiv sannsynlighet basert på bakgrunnsinformasjon, som det ifølge Aven (2013) må bli lagt vekt på, er ikke like enkelt når de fleste virksomheter ofte har svært lite informasjon. Da spørs det hvor pålitelig sannsynligheten som blir satt er. PST og E-tjenesten jobber med dette primært gjennom sitt etterretningsarbeid, men vil likevel ikke ha fullstendig kunnskap om alle eksisterende trusselaktører, deres intensjon og kapasitet, til tross for at flere har trening og erfaring med etterretning og dermed høy grad av kompetanse. Kunnskapen de besitter er i tillegg gradert og vil ikke kunne deles i detalj med virksomhetene. Dette vil ifølge Renn (2008) legge føringer for gangen i risikostyringsprosessen og risikovurderingen/analysen. Virksomhetene har ikke hjemmel i lov til å drive med etterretning

på samme måte som PST og E-tjenesten. Virksomhetenes kunnskap vil dermed alltid være ufullstendig og selektiv, til tross for innsatsen som blir gjort for å innhente mest mulig korrekte data. Petroleumsselskapene må dermed håndtere intenderte hendelser som de har liten eller ingen erfaring med og det finnes ingen oversikt over hva som er framtidens utfordringer (Aven, et. Al, 2008).

6.2.4 Spiller på frykt

Terrorister har blant annet som formål å skape frykt. Ulik risikopersepsjon fører til at denne frykten oppfattes ulikt av forsvarerne, uavhengig av sannsynligheten. Sannsynligheten er større å dø i en bilulykke, likevel frykter flere å reise med fly enn å kjøre bil. Ifølge Jore (2012) vil enkelte mennesker føle en form for frykt til tross for at sannsynligheten er liten, dette kan føre til at sannsynligheten i en risikoanalyse blir vurdert som mye større enn den er. Renn (2008) hevder at menneskelig atferd ikke blir drevet av fakta, men av persepsjon. Noen har personligheter som gjør at de er risikoaverse, som betyr at de har en motvilje til å ta risiko, mens andre er risikosøkende. Eksemplene ovenfor angående terrorangrepet på regjeringskvartalet og gisseltakingen i Algerie viser at de rammede nå har en økt frykt for å bli utsatt for terrorangrep, og sikkerhet blir høyt prioritert. Representanten fra Statoil ser at de burde fulgt trusselnivået mer nøye. I etterkant har de som funnene viser opparbeidet et svært gjennomtenkt styringssystem for Security. Det har i etterkant av hendelsene 22. Juli blitt utviklet nye lover og regelverk, blant annet Petroleumslovens § 9-3 som omhandler bevisste anslag og de nye norske standardene, NS 5830-serien som omhandler beskyttelse mot tilsiktede handlinger. Dette tolker jeg som at det i dag blir lagt betydelig større vekt på andre faktorer enn sannsynlighet. Fryktfaktoren kan også virke inn på trusselaktørene. En trusselaktør kan som nevnt ovenfor bli avskrekket om sikringstiltakene blir for vanskelige å komme forbi, de vil dermed gå videre til neste mål på listen. Frykt perspektivet mener jeg dermed heller ikke blir fanget opp ved bruk av sannsynlighet.

6.2.5 Presentasjon av sannsynlighet

Det kan være en utfordring når sannsynlighet skal kommuniseres til beslutningstaker, da man er prisgitt at mottaker forstår budskapet bak sannsynligheten. Utfordringen er dersom de feilaktig fokuserer på sannsynligheter, da dette vil prege hele vurderingen. Et eksempel er beslutningstakere som sitter på åremål og som kanskje bare tenker kortsiktig. Ved å unngå å bruke sannsynlighet i denne sammenheng kan fokus rettes mot om det er beslutningstaker/beskytter som kan bestemme om angrepet blir gjennomført suksessfullt eller

ikke, ved å innføre tiltak, eller om beslutningstaker er prisgitt at trusselaktøren bestemmer seg for å angripe eller ikke angripe. Det kan tenkes at dette vil ha motsatt effekt ved bruk av trefaktormodellen: verdi, trussel og sårbarhet. Hvis en beslutningstaker får et risikobilde som baseres på høy trussel og sårbarhet virker det mer alvorlig og dermed vil det bli tatt mer på alvor. I tillegg vil et fokus på sårbarhetene føre til at beslutningstaker får en mer eierskapsfølelse til risikoen noe som trolig kan føre til økt innsats mot å forebygge terrorhandlinger.

6.3 Fordeler med bruk av sannsynlighet

At det finnes eksempler på flere Black Swan hendelser innenfor Securityområdet, som gjør bruk av sannsynlighet vanskelig, er ikke til å legge skjul på. Massakren 22. Juli 2011 som nevnt ovenfor og terrorangrepene i New York 11. September 2001 er bare to eksempler. Det er derimot ikke slik at det alltid er nok empirisk data på Safetyområdet heller. Det er flere eksempler på storulykker som oppfyller Black Swan kriteriene og som dermed kan kalles en Black Swan hendelse; Piper Alpha og Alexander Kielland er to av dem. Storulykker innenfor Safety-kontekst er uforutsette hendelser, med lite empirisk data. Likevel følges ofte ISO 31000 og NS 5814 på slike hendelser. Klart uten empirisk materiale har man ingenting å regne på og man kan dermed ikke bruke frekvensbaserte sannsynligheter, men subjektiv-, kunnskapsbasert sannsynlighet er en helt annen sak. Jeg forstår det slik at Aven (2013) mener at dersom man har god bakgrunnskunnskap, kan subjektive sannsynligheter settes også ved tilsiktede handlinger. Noe som også blir understreket av representanten fra Proactima når han sier at dersom man kjenner verdiene, trusselen, sårbarheten og dermed risikobilde, samt at man kan gjenkjenne trender og endring i trender, så vil man ha et godt grunnlag for å si noe subjektivt om sannsynligheten. Sannsynlighet i en bayesiansk tilnærming er vitenskapelig i den forstand at det er en systematisering av kunnskap om fenomenet.

At flere likevel bruker mangel på empirisk data og statistikk som argument for og ikke sette sannsynlighet mener jeg er selvmotsigende på grunn av trusselens overraskende og uforutsigbare natur, som gjerne fører til at den ene hendelsen ikke vil komme en gang til. For terrorisme og andre tilsiktede handlinger er det ikke så interessant med historisk data likevel, fordi en terrorist som vil overraske og slå til på en uforutsigbar måte til et uforutsigbart tidspunkt, vil ikke gjøre det på en slik måte som det er blitt gjort før. Da vil det jo ikke være særlig overraskende. Ifølge Jore (2012) vil disse instrumentelle intensjonene gjøre at det er

verdt å benytte seg av risikostyringsprinsippene og metodikk for analysering av trusselen som finnes.

Fordelen med sannsynligheter er at de, sammen med konsekvensvurdering vil kunne gi en tydelig presentasjon av risikobildet. Ved å se på sannsynlighet, konsekvens og tilhørende usikkerhet kan beslutningstaker gjøre en vurdering av hvor det er mest nødvendig at det settes inn flest ressurser og dermed tiltak, slik at analyseresultatene blir gjort noe med og oppnår sitt formål. Det at analysen blir brukt i ettertid, er helt nødvendig for at risikostyringen skal ha noen hensikt. Beslutningstaker gjør ikke disse analysene selv, dermed vil det uten en form for sannsynlighetstenkning, enten uttrykket som tall eller som en mer kvalitativ måte med en subjektiv vurdering som basis, være utfordrende å gjøre prioriteringer. Det er flere fagområder i en virksomhet hvor det gjennomføres risikoanalyser som tar utgangspunkt i risiko som en funksjon av sannsynlighet og konsekvens og som fremstiller risikobildet i en risikomatrise. Dermed vil det være vanskelig å sammenligne risikobilde for Security med risikobilde på de resterende fagområdene om dette ikke blir gjort også her. Beslutningstakeren har ikke mulighet til å lese gjennom all bakgrunnskunnskapen som finnes på alle de forskjellige risikoene, for alle de forskjellige verdiene. Derfor kan det være mulig for en kvalifisert ekspertgruppe og analytiker å gjøre en vurdering av verdi, trussel og sårhet, slik som det anbefales i prNS 5832 og på bakgrunn av dette si noe om sannsynlighet og konsekvens. La oss ta et eksempel; En analysegruppe bestående av flere eksperter på områder som blant annet risiko og etterretning, kommer fram til etter å ha analysert og vurdert sine verdier og trusselaktører som er relevante for verdiene, at sannsynligheten er 0,5 for akkurat den plattformen, fordi den er i et land hvor det er ustabilt, og et land hvor flere kjente trusselaktørgrupper operer. Plattformen i Barentshavet derimot, har en betydelig lavere sannsynlighet. Dersom konsekvensene vil være de samme blir det dermed klart og tydelig hvor tiltakene må iverksettes.

Neal (2003) hevder at det kreves særskilt kompetanse i forhold til å utarbeide Security-rettede risikovurderinger. Ikke alle petroleumselskap har denne kompetansen. Statoil er et stort selskap som har ressurser og dermed mulighet til å sette inn egne ansatte med Security-bakgrunn. Dette framkommer av avhandlingens funn, ved at de har et godt utarbeidet og gjennomtenkt styringssystem og framgangsmåte for analysering av sikringsrisiko, som både inkorporerer elementer fra Safety og Security. For mindre og nyoppstartede selskap derimot kan dette være utfordrende, da de gjerne ikke har de nødvendige ressursene til å kunne ansette

den type personell, og dermed må ansette folk innad som egentlig ikke har sikring som primæroppgave.

6.4 Mulige årsaker til uenigheten

6.4.1 Ulik risikopersepsjon

Jeg oppfatter at den viktigste årsaken til uenighetene som har kommet fram i mine funn har en bakgrunn i skillet mellom Safety og Security. Albrechtsen (2003) påstår at det er flere ulikheter enn likheter mellom fagfeltene. Dette støtter Securityfagfolkene, da de mener det er to ulike fenomen som må tilnærmes på hver sin måte. Informanten med bakgrunn innenfor Safety mener det ikke nødvendigvis er så stort skille mellom Safety og Security og at samme tilnærming i hovedsak bør benyttes for å sikre en helhetlig tilnærming til risikostyring.

Skillet mellom Safety og Security viser til en ulik risikopersepsjon i fagfeltene. Fenomener som er preget av mye usikkerhet og lite empirisk data, vil ha større grad av subjektivitet å forholde seg til i analyseprosessen, og ifølge Pettersen og Engen (2010) knyttes usikkerhet til risikopersepsjon. Renn (2008) hevder videre at menneskelig atferd blir drevet av persepsjon, ikke fakta. Jeg tolker dette som at hvilket syn på og oppfatning man har av risiko vil påvirke hvordan en velger å tilnærme seg og styre risiko. Innenfor Safety og Security eksisterer det ulike definisjoner av risiko og dermed fører det til ulike meninger om hvordan denne kan tilnærmes. Deres ulike kompetanse, erfaring, informasjonsgrunnlag og personlige overbevisninger vil påvirke deres risikopersepsjon. Dette støttes av Pettersen og Engen (2010) som hevder at ulik erfaring, kunnskap og risikosyn vil føre til at identifisering av Security risiko blir forskjellig. Innenfor Security forholder de seg til andre teorier enn innenfor Safety, blant annet kriminologiteorier, slik som APT-teorien, som beskriver forholdet mellom en verdi, beskytter og trusselaktør (Manunta, 1997 i Stranden, 2013). Denne teorien sammenfaller med NSM og PST sin risikotrekant. På Safetyfeltet blir sannsynlighet et verktøy for å beskrive usikkerhet (Aven og Renn, 2010). Aven (2013) hevder at bruken av sannsynlighet ofte blir unngått innenfor Securityfeltet, noe som også mine funn viser klart og tydelig. Ifølge teorien og risikotrekanten skal det kunne gå an å vurdere risiko knyttet til kriminelle handlinger uten å måtte si noe om sannsynlighet, se vedlegg nr. 3 for eksempel på hvordan dette kan gjennomføres. Dermed er det forståelig at de med Securitykompetanse er opptatt av å beskrive aspektene; verdi, trussel, sårbarhet ved risikoen på en svært omfattende kvalitativ måte, da dette er noe de har kompetanse på.

De med Safety- og risikoanalysebakgrunn derimot kan dette med å gjøre analyser av risiko og bruk av sannsynlighet er en stor del av dette, om det gjelder kvantitativ eller kvalitativ sannsynlighet, det kommer an på hvilken type risiko, enkel eller systemisk.

6.4.2 Ulik begrepsforståelse

Dahl (2000) hevder at det er viktig å ha en en felles forståelse av risiko, for å kunne styre sikkerhet på en helhetlig måte. Aven og Krohn (2013) synes å støtte dette ved å foreslå at man bør ha en grunnleggende teori, prinsipper og metoder for risikovurdering og styring. Funnene viser derimot at det ikke finnes en definisjon av ordene safety, security og risiko, og at fagfolk fra ulike fagområder ikke helt forstår hverandre. Mangel på kunnskap og informasjon kan føre til mangelfull forståelse, slik at misforståelser og uenighet lett kan oppstå.

Sannsynlighetsbegrepet

Jeg opplever at sannsynlighetsbegrepet blir tolket ulikt. Fagfolkene innenfor Safety mener du må tenke sannsynlighet for å vite hvor du skal sette inn ressurser, og mener Security folkene misforstår begrepet. Fagfolkene innenfor Security derimot tar sterk avstand til sannsynlighet, men i den forstand sannsynligheten for hvorvidt et angrep vil inntreffe. Likevel anerkjenner de at det er mulig å si hvor sannsynlig det er at angrepet blir vellykket, gitt at det blir forsøkt, blant annet ved å se på trusselaktørens kapasitet og virksomhetens sårbarheter. De anerkjenner også at man kan si noe om at angrepsmåte A er mer sannsynlig enn angrepsmåte B, om det for eksempel blir utført med eksplosiver eller våpen. Dette kan menes noe om dersom en har sett på kapasitet, vet trusselaktørens kunnskapsnivå, hvilken tilgang de har til ulike våpen, samt historikk som sier noe om deres preferanser. Tilslutt, anerkjennes muligheten for å si noe om at et mål, for eksempel Stortinget, har større sannsynlighet for å bli utsatt for angrep enn et annet mål, for eksempel en matbutikk, blant annet fordi Stortinget vil være et mer attraktivt mål for trusselaktøren. Dette kan menes noe om dersom en kjenner til uttalelser som sier noe om trusselaktørens preferanser, ideologi som støtter opp under strategien deres, om det er mål hvor det er mange mennesker, om det vil føre til store presseoppslag eller om det vil spre massiv frykt. Dette er likevel ikke det samme som å gjøre prediksjoner av når og hvor et angrep vil finne sted. Det vil være umulig å vite, og fastsatte sannsynligheter vil dermed være uegnet som beslutningsstøtte. På den andre siden argumenterer de fra Safetyfeltet at en må bruke sannsynligheter nettopp slik at beslutningstaker kan sammenligne ulike risikoer for så å kunne avgjøre og prioritere hvor og hvilke ressurser som bør settes inn, noe som også støttes av (Aven og Renn, 2010). Det virker

også som om noen tenker på sannsynlighet på en indirekte, ubevisst måte, til tross for at de påstår at dette ikke blir gjort. For å understreke dette poenget, vises det til et sitat fra mine funn:

> *"Det vi ønsker å forholde oss til er det vi kaller rimelige verstefall scenarioer, men vi diskuterer ikke egentlig sannsynlighet for terrorisme for å si det sånn" – Representant fra DSB*

Jeg tolker dette som at de tenker sannsynlighet på en indirekte, kvalitativ og subjektiv måte ved å erstatte sannsynlighetsbegrepet med lignende begreper som rimelig, muligheten for, sjansen for. Dette minner derimot om subjektive sannsynligheter som Aven (2013) beskriver. Dette kan også ses på som en svakhet ved det norske språk, da det i det engelske språk ofte brukes probability i forbindelse med sannsynlighet i en matematisk forstand og likelihood om sannsynlighet som en mer subjektiv vurdering. Det virker som at de ulike fagområdene legger forskjellig mening i sannsynlighetsbegrepet, hvor de innenfor Securityregimet befinner seg litt innenfor det teknisk-naturvitenskapelige perspektivet og forbinder begrepet med matematiske kalkulasjoner og statistikk og en risikoanalyse som ensbetydende med en risikomatrise, sitatet nedenfor illustrerer et eksempel.

> *"Snakker man om lavfrekvente hendelser, vil du jo alltid få et lavt tall. Naturlig nok. Slik at beslutningsgrunnlaget vil bli feil" - Representant fra PST*

Denne tolkningen synes å bli støttet av Aven (2012) ut fra en kronikk i Aftenbladet hvor han hevder at tankene i Gjørv kommisjonen i forhold til overordnet risikotenkning og samfunnssikkerhet bygger på et tenkesett som ble introdusert på 70-tallet. Det virker som om synet på risikostyring og analyse tidligere har vært slik det blir beskrevet i hans sitat nedenfor, men at de som en følge av tragedien som fant sted 22. juli, har innsett at denne tilnærmingen ikke vil fange opp slike uforutsette hendelser, og dermed gått helt bort fra sannsynlighetsbruken.

> *"det er fullstendig ubrukelig for å møte de trusler og farer vi står overfor i dag. (...) kunnskaps- og usikkerhetsdimensjonen gis altfor liten vekt. En tror risiko kan fanges opp gjennom produktet av sannsynlighet og konsekvens/tap (...), men en slik bro bygger på en misforståelse,(...). Beslutningsledere (...) villedes, og feil beslutninger tas" – (Terje Aven, 2012)* [13]

[13] www.aftenbladet.no/meninger/kommentar/Risikotenkningen-er-fullstendig-foreldet-3015836.html#.U5Tvol7Vs48

Sannsynlighet handler som nevnt ovenfor om mer enn det og riskomatrise er ikke ensbetydende med en risikoanalyse, det er en framstilling av risikobildet, slik at det skal være enklere for beslutningstaker å se resultatet. Aven (2008)[14] understreker at fagfolkene må bli bedre til å få frem dette risikobildet. Njå m.fl. (1998) understreker også betydningen av å gjøre eksperter kjent med sannsynlighetsbegrepet, og behovet for å samkjøre sannsynlighetsforståelsen.

Trussel og Risiko

Det virker også som om det er forvirring angående forskjellen på trussel og risiko. Det er svært viktig at disse begrepene ikke blir sett på som en og samme sak. Trussel er en dimensjon av den totale risikoen, sammen med verdi og sårbarhet, akkurat som risiko innenfor risikostyringen på Safetyområdet er bestående av usikkerhet om hvorvidt en hendelse vil oppstå og konsekvenser. Noen blander også sannsynlighetsbegrepet med trusselbegrepet. Et eksempel er for eksempel at et høyt trusselnivå kunne bli sett på som at sannsynligheten var høy, eller motsatt at et lavt trusselnivå kunne ses på som lav sannsynlighet. Dette blir feil fordi hvorvidt en hendelse inntreffer eller ikke vil også ha sammenheng med verdiens attraktivitet og eksisterende sårbarhet. En trusselaktør kan ha tilstrekkelig kapasitet til å angripe en søppeldynge, men målet vil nok ikke være særlig attraktivt, dermed er ikke risikoen høy selv om trusselen er høy.

Kompetanseproblematikk

Funnene viser at det er en forskjell i kompetansen på de ulike fagfeltene. Noen eksempler er representanten fra PST som mener at DSB tror de har et slags eierskapsforhold over risikoanalysefaget, og representanten fra Proactima som tror sannsynlighetsbegrepet er misforstått i Securityfagfeltet. Flere av informantene innenfor Securityfeltet blant annet Mærli og Stranden mener at Safety og Security er svært ulike områder, hvor det kreves egne metoder. Uavhengig av hvilket syn blir det veldig viktig å klargjøre hva som legges til grunn i analyser og vurderinger, hvilken tilnærming som er tatt utgangspunkt i og hva som blir lagt i de ulike begrepene. Ifølge Aven (2007) er det viktig å være bevisst på forskjeller i ulike fagområder. Dersom en ikke er bevisst kan det oppstå dårlig kommunikasjon og dermed misforståelser. Funnene mine viser til en heftig debatt, der begge fagfelt hevder de har rett. Likevel viser sitatene under at begge fagfeltene mangler kompetanse på det motsatte området.

[14] www.sikkerhetsdagene.no/_media/aven.pdf

”kan ikke akkurat si hvordan du skal snakke om sannsynligheter [i forbindelse med Security] slik at du kommer i mål, men at det går det er jeg sikker på” Representant fra Proactima

”Nei vet du hva, dette [Inkorporere Securitymetodikk i den totale virksomhetsstyringen] vrir jeg hjernen min på nesten hver dag. Jeg er nok ikke smart nok til å komme fram til noe” - Representant fra PST

Dersom en skal gjøre noe med kompetanseproblematikken må de ulike fagfeltene samarbeide, Det blir viktig at de parter som kommuniserer i sikkerhetsarbeidet klargjør betydningen av sine definisjoner. På den måten reduseres mulighetene for misforståelser og feil som følge av dette. Samtidig må myndighetene bidra så langt de kan med rådgivning for å øke Security kompetansen i virksomhetene og samfunnet generelt. Tinlund (1997) i Stranden (2011) oppfordret for mange år siden til økt kunnskapsheving innenfor sikkerhetsbransjen. Det er ifølge Njå m.fl. (1998) avgjørende at eksperter snakker noenlunde samme språk for at analyseresultatene skal være mest mulig gyldige. Ved å fremme den faglige utviklingen innen Securitybransjen kan man få en høyere kvalitet på vurderinger og tiltak (Stranden, 2011).

6.5 APT – teorien: Et alternativ?

Sannsynlighet kan være fornuftig å bruke i tilfeller hvor man har god statistikk, og hvor man har aktører og fenomener som ikke bevisst forsøker å omgå innførte sikringstiltak. I forbindelse med trusselvurderinger derimot har fastsettelse av sannsynlighet kanskje vært en årsak til manglende forståelse og kilde til feilvurderinger. Dette synes å bli støttet av Ericson og Doyle (2004) når de påpeker begrensningene til risikovurdering og risikostyring i denne sammenheng. Risiko knyttet til tilsiktede uønskede handlinger skiller seg på mange sentrale områder fra risiko knyttet til det som kan beskrives som ulykker og utilsiktede handlinger. Jeg mener APT-metoden (Stranden, 2013), utviklet av Manunta som er anerkjent innenfor feltet som omhandler tilsiktede handlinger, vil være bedre i stand til å ivareta dette aspektet. En svakhet ved denne måten er dersom metoden ikke ser på forholdet mellom de forskjellige faktorene, da trusselaktøren kan utnytte analyser og vurderinger som er gjort av en virksomhet, dersom de ved hjelp av etterretning får innsyn i slik informasjon. Videre kan sårbarheten til en virksomhet avhenge av i hvilken grad trusselaktøren har evne til og dynamisk endre planer og fortsette angrepet når hindringer er iverksatt. Det blir viktig å se på hvordan faktorene påvirker hverandre, da enhver vurdering av trusselen, som ikke tar hensyn til at trusselaktør kan respondere på forsvarers vurdring og tiltak på vegne av denne vurdringen, vil være upålitelige. Dette gjelder uansett hvilken tilnærming til analysen som blir

brukt (Stranden, 2013). Ledende praksis innen risikoanalysefaget mot kriminelle handlinger og andre uønskede handlinger forsøker å inkorporere dette forholdet ved at de først vurderer de tre faktorene verdi, trussel, sårbarhet individuelt, for at det skal bli enklere å se de relevante faktorene hver for seg, for så å tydeliggjøre hvordan de ulike faktorene påvirker hverandre. Måten det velges å framstille risiko på, bør også gjøres slik at alle faktorene blir ivaretatt likt (Stranden, 2013). En svakhet ved denne metoden er at det kan være vanskelig å framstille risikobildet visuelt ved en tredimensjonal matrise. Det bør dermed vurderes andre metoder å framstille risikobildet på, som for eksempel et boblediagram slik som Statoil benytter seg av.

6.6 Safety og Security – to sider av samme sak?

På den ene siden hvis man ser bort i fra de ulike begrepene, men meningen som ligger bak, kanskje de ulike standardene ikke er så forskjellige, at de dekker litt av det samme. Begge snakker om en identifisering av verdier, en farekilde (trussel i Securityfeltet), sårbarheter, scenarioer/konsekvenser. Det virker som det er ulike begrep, men at de egentlig ikke er så forskjellige. På en annen side kan forskjellen i framgangsmåte føre til at fokuset blir lagt på ulike steder, samt når i prossessen de ulike faktorene blir sett på. Det er derfor ingen fasitsvar for hvordan en virksomhet skal tilnærme seg dette. Et viktig moment man må huske på når vi er opptatt av å skille på begreper er at vi ikke må glemme helheten. Ved å tydeliggjøre skillet mellom tilsiktede handlinger og utilsiktede hendelser er det fort gjort å velge bort noe av utfordringen. Det er nemlig slik at for eieren for verdien som søkes beskyttet, så er det i prinsippet irrelevant om verdien gikk tapt på grunn av en tilsiktet handling eller ulykke. Resultatet er det samme. Eieren står igjen med skade eller tap på sine verdier. I mange tilfeller det viktig å se dem sammen. Det viktigste blir derfor å gjøre en god vurdering og sørge for at om ikke begge aspekter kan bli ivaretatt av analytikeren på en tilstrekkelig måte så må andre få tilgang. Det er ifølge Aven (2013) viktig at eksperter på alle områder er representert i analyseprosessen. Godt samarbeid og god kommunikasjon er nøkkelbegrep (Njå m.fl., 1998).

Jeg vil si at det er forskjell mellom begrepene, men mener at ved litt overlappinger kan de kanskje bli integrert i et helhetlig styringssystem. Hood et al. (1992, p. 135) i Stranden, (2013:26). beskriver en fin måte å se det på; *”istedenfor å argumentere for at risiko bare kan defineres på en måte må fenomenet risiko ses på som en øygruppe. Øyene er individuelle og forskjellige, men de hører likevel sammen. Forskjellen ligger i måten man kommer frem til svaret og hva du velger å gjøre med riskoen som er knyttet til ulike scenarioer.”* Når

risikovurderingen er gjennomført er det hensiktsmessig å samle resultatet i et risikobilde. Formålet med et slikt bilde kan være å lette kommunikajonen med ulike interessenter som ledelsen, ansatte, samarbeidspartnere og styret i en bedrift. Her kan både dagens risikobilde presenteres, men også hvordan risikobildet vil være etter eventuelle tiltak er blitt innført. Slik det er nå, med ulike måter å presentere risikobilde på, vil det lett oppstå misforståelser og kanskje unødvendige uenigheter. Det blir dermed utrolig viktig å klargjøre hva som blir lagt til grunn i de ulike vurderingene, hvilken tilnærming de har brukt til risiko og hva som blir lagt i de forskjellige begrepene. En løsning er først å utføre selve avdekkingen av risikobilde på den måten som analysegruppen måtte finne mest hensiktsmessig, om det er bruk av en tofaktormodell som sannsynlighet og konsekvens eller en trefaktormodell som verdi, trussel og sårbarhet. Deretter presentere risikobildet på en måte hvor analysegruppen nøytraliserer seg fra sitt faglige ståsted og tenker utenfor boksen. Det vil si at en typisk Boston Square modell ikke blir brukt som presentasjonsmiddel. Ved å ha et overordna rammeverk, der alle fagfelt benytter seg av samme kategorisering av risikobilde; lav, moderat, høy eller ekstrem, kan en virksomhet forholde seg til flere typer av risiko og en helhetlig risikostyring kan opprettholdes. Et eksempel er hvis risiko for bevisste anslag blir vurdert som høy, risiko for brann blir vurdert som moderat og risiko for økonomiske tap er lav. Når man så skal gjøre noe med risikoen kan dette igjen deles inn i de ulike fagområdene, som bruker ulike virkemidler for å håndtere risikoen. Den ulike metodikken kan da hentes fram om dette er en tofaktor modell (sannsynlighet x konsekvens) eller en trefaktormodell (verdi, trussel, sårbarhet). Dette kan fungere så lenge risikokategoriseringen er felles, og slik kan prioriteringen innenfor det totale risikobilde blir helhetlig. Likevel er det ikke alle typer av risiko som er direkte sammenlignbare. Hvis risiko knyttet til økonomi vurderes mot risiko knyttet til liv og helse, vil ikke dette ha samme vekting. Det er en normativ vurdering, som må gjøres på tvers, og som avgjøres av risikopersepsjon, menneskelige verdier og holdning til livet.

7 KONKLUSJON

Avhandlingens formål har vært å undersøke hvordan terror blir analysert av norske petroleumsselskaper og av relevante myndigheter, samt i hvilken grad sannsynlighet kan brukes i disse analysene.

Hvordan analyseres risiko for terror i petroleumssektoren og av relevante myndigheter, og i hvilken grad kan sannsynlighet brukes i disse analysene?

Delkonklusjon 1 – Hvordan analyseres risiko for terror i petroleumssektoren og av relevante myndigheter?

Det er to overordnede framgangsmåter for å analysere sikringsrisiko og terror. Safetyfagfeltet har en to-faktortilnærming til risiko i analysesammenheng. Hvor de ser på konsekvens og usikkerhet uttrykket som sannsylighet. Denne framgangsmåten kan finnes i blant annet ISO 31000 og NS 5814. Securityfagfeltet har en tre-faktortilnærming og ser på risiko i sikringssammenheng som en funksjon av verdi, trussel, sårbarhet. Denne framgangsmåten står beskrevet i NS 5830-serien. Det er uenighet om Safety og Security er et hensiktsmessig skille og om det bør være to ulike standarder med forskjellig begrepsbruk og framgangsmåte. Fagfolkene innenfor Safetyområdet mener det fører til en risikostyring som ikke er helhetlig, mens Securityfagfolkene mener det er ulike fagfelt og dermed nødvendiggjør det en ulik tilnærming, men at det kan være et overordnet styringssystem for å sørge for en helhetlig risikostyring.

Delkonklusjon 2 – I hvilken grad kan sannsynlighet benyttes i disse analysene?

Uenigheten og diskusjonen er størst angående bruk av sannsynlighet. Fagfolkene fra Safetyområdet mener man kan si noe om sannsynligheten for om et angrep vil inntreffe. Det understrekes at sannsynligheten ikke er en objektiv sannhet eller basert på statistikk og matematiske kalkulasjoner. Det er basert på en bayesiansk tilnærming, der sannsynligheten kun er en subjektiv vurdering basert på all relevant bakgrunnsinformasjon, slik som verdi, trussel og sårbarhet. Det må også kartlegges hvilken grad av usikkerhet og hvilken kvalitet

som er på den eksisterende informasjonen. Securityfagfolkene mener man kan si noe om sannsynlighet for hvorvidt et angrep blir suksessfullt, gitt at det oppstår, sannsynlighet for at et mål vil være mer attraktivt enn et annet mål eller sannsynligheten for at angrepet blir gjennomført på den måten istedet for en annen. Å si noe om sannsynligheten for om angrepet vil bli forsøkt derimot. Det er umulig. De viktigste årsakene til dette er at trusselaktøren har en intensjon og kapasitet, han er fleksibel og tilpasningsdyktig. Det finnes også lite historisk data og erfaring. Det kan være utfordrende å avgjøre og prioritere hvor ressurser og tiltak skal settes inn uten sannsynlighet og det kan være vanskelig å sammenligne risikobildet for kriminelle handlinger med andre typer risiko. Her kommer de tre faktorene; verdi, trussel og sårbarhet inn. Dersom risikobildet ut fra disse tre faktorene blir plassert innenfor en risikokategori, for eksempel lav, moderat, høy eller ekstrem, og dersom risikobildet på også andre områder blir plassert innenfor samme kategorisering uavhengig om det brukes en tre-faktor eller 2-faktor modell, kan beslutningstaker sammenligne og dermed prioritere mellom dem. Det er opp til hver enkel virksomhet å avgjøre hva de foretrekker, det viktigste er at virksomheten sikrer en helhetlig risikostyring og at analysen blir gjort slik at risikobildet blir kjent og videre brukt slik at sikringstiltak blir iverksatt. Det er likevel selve prosessen som fører til læring.

7.1 Tanker om videre forskning

Det anbefales å gjøre en mer omfattende studie av de ulike tilnærmingene til sikringsrisiko, hvor det gjøres intervjuer med representanter fra flere ulike oljeselskap. Gjerne kan fokus spesielt være på hvordan den store graden av usikkerhet kan reduseres og i hvilken grad iverksatte sikringstiltak fungerer som tiltenkt. Dette kan være vanskelig å studere, da fravær av angrep ikke nødvendigvis betyr at tiltakene ikke har fungert.

Kildehenvisning

Arnesen, S. A., T., Bjørgo og M., B., Mærli. (2005). Hva gjør Norge utsatt for terrorisme? Trusselscenarioer og norsk sårbarhetsforvaltning. Norsk utenrikspolitisk institutt (NUPI).

Aven, T. (2003). *Foundations of risk analysis: a knowledge and decision-oriented perspective.* Chichester: John Wiley & Sons, ltd.

Aven, T. (2007). *Risikostyring: Grunnleggende prinsipper og ideer.* Oslo: Universitetsforlaget.

Aven, T. (2013). Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts. *Reliability Engineering and system safety*. Vol. 119, s. 229-234. Universitetet I Stavanger

Aven, T., & B. S., Krohn. (2013). A new Perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering and system Safety.* Vol. 121, s. 1-10. Universitetet I Stavanger.

Aven, T. & Renn. (2010). *Risk Management and governance: Concepts, guidelines and applications.* Heidelberg: Springer.

Bjørgo, T. (2005). *Root causes of terrorism: myths, reality and ways forward.* London: Routledge.

Dahl, S. (2000). *Organisasjon og ledelse.* Aschehoug forlag.

Dreyfus, H. L. og S. E, Dreyfus (1986). *Mind over Machine: The power of human intuition and expertise in the era of the computer.* New York: Free Press

Engen, m.fl. (2013). Tilsynsstrategi og HMS-regelverk i norsk petroleumsvirksomhet. Rapport utgitt av Arbeidsdepartementet.

Ericson R. V. og A. Doyle (2004). *Economy and Society.* Catastrophe risk, insurance and terrorism. *Vol. 33:2, s. 135-173.*

Flage, R. og Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA). Reliability and Risk Analysis: Theory and Applications. Vol 2:13, s. 9-18.

Golany, B., E. H. Kaplan, A. Marmur og U. G. Rothblum. (2007). Nature plays with dice – terrorist do not: Allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research. Vol.129:1.* Elsevier forlag.

Harel, A. (2012). Preventing Terrorist Attacks on Offshore Platforms: Do States have sufficient legal tools? *Harvard National Security Journal. Vol. 4:1.*

Hellevik, S., G. (1994). *Metoder for vurdering og analyse av godhet av vedlikeholdsstrategier.* Stavanger

Hoffman, B. (2006). *Inside Terrorism.* Revised and expanded edition. New York: Columbia University Press.

Holter, H. og R., Kallevik. (red).(1982). *Kvalitative metoder i samfunnsforskning*. Oslo: Universitetsforlaget.

Jacobsen, D. I. (2005). Hvordan gjennomføre undersøkelser? Innføring i vitenskapelig metode. Høyskoleforlaget, s. 141-163.

Johannessen, A. & P. A., Tufte. (2006). *Introduksjon til samfunnsvitenskapelig metode.* Abstrakt forlag.

Jore, S., H. og O. Njå (2010). Risk of terrorism: A scientifically valid phenomenon or a wild guess? The impact of different approaches to risk assessment: Universitetet i Stavanger

Jore, S., H. (2012). Counterterrorism as Risk Management Strategies. PhD Thesis UIS no. 178 – Faculty of science and technology: Universitetet I Stavanger.

Jore, S., H. og A. Moen (2014). A discussion of the Risk-Management and the Rule-Compliance Regulation Regimes in a Security Context: Universitetet i Stavanger.

Kjøk, Å. & B. Lia (2001). (FFI Rapport). Terrorism and Oil – An explosive Mixture? A Survey of Terrorist and Rebel Attacks on Petroleum Infrastructure 1968 – 1999. Forsvarets forskningsinstitutt

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

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science,* Vol 42:4, 237–270. Publisert av: Elsevier.

Midttun, Ø. (2013). Dialog. Nr. 2: Et tidsskrift fra Petroleumstilsynet. Kan vi planlegge for det utenkelige? Petroleumstilsynet.

Njå, O., Aven, T., og Rettedal, W.K. (1998). Subjective probability assignment in QRAs for offshore construction and cessation projects. Sørco.

Piètre-Cambacédès, L. & C., Chaudet. (2010). The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety". International Journal of Critical Infrastructure Protection, Vol. 3:2. S. 55-66.

Pettersen, K. og O.A., Engen. (2010). *Rethinking risk theory: a critical realist approach to aviation security.* Universitetet i Stavanger

Rausand, M. og I., B. Utne. (2009). *Risikoanalyse – teori og metoder*. Tapir Akademisk forlag

Relf R. & G. Stubblefield (2000). Countering Petroleum Security Risk. Global options. Offshore Technology conference.

Renn, O. (2008). *Risk Governance:* Coping with Uncertainty in a Complex world. Earthscan ltd.

Stranden, R. (2013). *På vakt: Sikkerhet for operativt personell* (utkast 20. Mars). Krokestadelva: Proakt Media.

Stålesen, J. (2011). Security styring i Petroleumssektoren. Hovedoppgave i Samfunnssikkerhet. Universitetet i Stavanger.

Svensson, P., G. & B., Starrin. (red) (1996). *Kvalitative studier i teori och praktikk*. Studentlitteratur

Lovverk

Lov om Etterretningstjenesten (1998).

Lov om forebyggende sikkerhetstjeneste – Sikkerhetsloven (1998, sist endret 2008).

Lov om petroleumsvirksomhet – Petroleumsloven (1996, sist endret 2012).

Lov om Politiet – Politiloven (1995;2013).

Standarder

Norsk Olje og Gass (2003, rev. 2013). 091 – Anbefalte retningslinjer for sikring av forsyninger og materiell i olje- og gassindustrien

Standard Norge, Norsok Z-013 (2001, rev. 2010). Risiko og beredskapsanalyse. Lokalisert på: www.standard.no/pagefiles/954/z-013-n.pdf

Standard Norge, NS 5814 (2008) – Krav til risikovurderinger

Standard Norge, NS 5830 (2012) – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger - Terminologi

Standard Norge, prNS 5831 (2013) Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger - Krav til risikohåndtering

Standard Norge, prNS 5832 (2013) – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger - Krav til risikoanalyse

International Organization for Standardization, ISO 31000 (2009) Risk Management. Principles and Guidelines

NOU 'er og Stortingsmeldinger

NOU (2000:24). Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet. Lokalisert på:
www.regjeringen.no/nb/dep/jd/dok/nouer/2000/nou-2000-24.html?regj_oss=1&id=143248

Stortingsmelding Nr. 12. (2005-2006). Helse, miljø og sikkerhet i petroleumsvirksomheten. 5 storulykkesrisiko. 5.5.2 særlig om terrorberedskap. Lokalisert på:
www.regjeringen.no/nb/dep/asd/dok/regpubl/stmeld/20052006/stmeld-nr-12-2005-2006-.html?regj_oss=1&id=408103

Stortingsmelding Nr. 15. (2011-2012). Hvordan leve med farene. 5.1. Risiko og risikoaksept. Lokalisert på:
www.regjeringen.no/nb/dep/oed/dok/regpubl/stmeld/2011-2012/meld-st-15-20112012/5/1.html?id=676545

Stortingsmelding Nr. 22. (2007-2008). Samfunnssikkerhet. Lokalisert på:
www.regjeringen.no/np/dep/jd/dok/regpubl/stmeld/2007-2008/stmeld/-nr-22-2007-2008-/5.html?id=510696

Stortingsmelding Nr. 29 (2011-2012). Samfunnssikkerhet. 8.2.4. Samarbeid om terrorbekjempelse.
Lokalisert på: http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2011-2012/meld-st-29-20112012/8/2/4.html?id=685688

Internett:

Aven, T. (2008). Risikostyring i et samfunnssikkerhetsperspektiv. Universitetet i Stavanger. Lokalisert på: www.sikkerhetsdagene.no/_media/aven.pdf Nedlastet: 12.06.2014

Aven, T. (20.08.2012). Risikotenkningen er fullstendig foreldet. Lokalisert på: www.aftenbladet.no/meninger/kommentar/Risikotenkningen-er-fullstendig-foreldet-3015836.html#.U5Tvol7Vs48 Nedlastet 01.06.2014

Helgesen, O., K. (2013). Teknisk ukeblad: Petroleum. Lokalisert på: http://www.tu.no/petroleum/2013/09/02/ingen-olje--og-gassinstallasjoner-trenger-ekstra-terrorbeskyttelse Nedlastet 01.06.2014

Homeland security news wire (2013). Modeling terrorism: Game theory helps corporate risk manage analyze terrorism risk. Lokalisert på: http://www.homelandsecuritynewswire.com/dr20131209-game-theory-helps-corporate-risk-manage-analyze-terrorism-risks Nedlastet 05.05.2014

Kashubsky M. (2011). University of Wollongong, Doctor of Philosophy, Faculty of law. Lokalisert på: http://ro.uow.edu.au/thesis /3662/ Nedlastet 20.03.2014

Nasjonal sikkerhetsmyndighet sine hjemmesider. lokalisert på: www.nsm.stat.no/Om-NSM/ Nedlastet 23.05.2014

Norsk Olje og Gass sine hjemmesider. Lokalisert på: http://www.norskoljeoggass.no/ Nedlastet 23.05.2014

Petroleumstilsynet (2013) Sikkert grep om sikring. Lokalisert på: http://www.ptil.no/beredskap/sikkert-grep-om-sikring-article10179-854.html Nedlastet: 23.05.2014

Politiets sikkerhetstjeneste sine hjemmesider. Lokalisert på: http://www.pst.no/trusler/terrorisme/ og www.pst.no/om/ - Nedlastet: 24.05.2014

Regjeringen sine hjemmesider. Direktoratet for samfunnssikkerhet og beredskap. Lokalisert på: http://www.regjeringen.no/nb/dep/jd/dep/underliggende-etater/direktoratet-for-samfunnssikkerhet-og-be.html?id=279674 - Nedlastet 09.06.2014

Sander, K. (2014). Telefonintervju som datainnsamlingsmetode. Lokalisert på: http://kunnskapssenteret.com/telefonintervju/ - Nedlastet 09.06.2014

Seglem, E. Og Myset, O. (25.01.2013). Oljeselskapene trener lite på terror. Lokalisert på: www.aftenbladet.no/energi/--Oljeselskapene-trener-lite-pa-terror-3111252.html#.U51 - Nedlastet 15.06.2014

Taraldsen, L. (2013) Terror mot oljebransjen. Lokalisert på: http://www.tu.no/it/2013/08/20/dette-er-sikkerhetssjefens-skrekkscenario Nedlastet 01.06.2014

Vedlegg 1 Intervjuguide

Del 1 – Introduksjon:

- **Informasjon om meg selv**
- **Informasjon om tema for oppgaven**
- **Gjennomgang av informasjonsskriv og samtykkeskjema**

Eventuelle spørsmål før intervjuet starter

Del 2 – Kartlegge informantens bakgrunn:

- **Stilling/tittel**
- **Funksjon/arbeidsoppgaver**
- **Erfaring fra virksomheten**
- **Annen bakgrunn**

Del 3 – Gjennomgang av begreper

- **Risikobegrepet**
- **Risiko i forbindelse med sikring**
- **Usikkerhetsbegrepet**
- **Terrorisme/Tilsiktede handlinger**
- **Sannsynlighetsbegrep**
- **Risikostyring**

Risikoanalyse

- **Finnes det et dokumentert rammeverk eller interne krav for analysemetodikk i forbindelse med terrorisme eller tilsiktede handlinger, som dere opererer etter?**
- **Gjør dere selvstendige trusselvurderinger? Hvis ja, Hvordan avdekke trusselaktører?**
- **Hvem definerer hvilke verdier som gjelder for dere? Hvordan blir disse identifisert/valgt?**
- **Hvordan modellere scenarioer?**
- **Hvordan gjennomføre en sårbarhetsvurdering?**
- **I hvilken grad kan virksomheten redusere sårbarheten?**
- **Bruker dere sannsynlighet i analysene? Hvordan påvirker bruk eller ikke bruk av sannsynlighet påliteligheten til analysen?**
- **Hvis ja, hvordan er framgangsmåten for å sette sannsynlighet?**
- **Blir det gjort kvantifiseringer? Hvordan påvirker dette framstillingen av risikobildet?**

Bruk av eksperter

- **Hvordan velges eksperter?**
- **Hvem samarbeider dere med?**
- **Hvordan vet dere om dere har den rette kompetansen med i analyseprosessen?**
- **Fordeler og ulemper med ekspertvurderinger?**

Risikoaksept, risikobilde og håndtering

- **Gjøres ulike kategoriseringer av risikonivå?**
- **Hvilke kriterier fører til at at risikoen blir satt inn i de ulike kategoriene?**
- **Hvordan bør prioritering av tiltak og ressurser foregå?**
- **Hvordan framstilles risiko? Brukes eventuelt en risikomatrise?**
- **Hvordan følges risikoen gjennom året? Hvor ofte oppdateres analysene?**
- **Er det noen som evaluerer kvaliteten på risikovurderingen?**
- **Hvordan sørge for at analysen blir brukt?**
-

Vedlegg 2

FEMA 452: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings (2005)

Table 4-7: Total Risk Scale Color Code

	Low Risk	Medium Risk	High Risk
Risk Factors Total	1-60	61-175	≥ 176

Table 4-8: Site Functional Pre-Assessment Screening Matrix

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	280	140	225	90	90
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	7	9	9	9
Engineering	448	128	200	96	96
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	4	5	6	6
Warehousing	168	96	135	54	54
Asset Value	3	3	3	3	3
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	8	9	9	9
Data Center	320	128	120	64	64
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	5	4	3	4	4
Food Service	112	32	50	36	36
Asset Value	2	2	2	2	2
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	4	5	9	9
Security	392	140	350	126	126
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	5	10	9	9
Housekeeping	112	24	30	12	12
Asset Value	2	2	2	2	2
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	3	3	3	3
Day Care	504	324	405	162	162
Asset Value	9	9	9	9	9
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	9	9	9	9

Table 4-9: Site Infrastructure Pre-Assessment Screening Matrix

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	32	128	60	16	16
Asset Value	4	4	4	4	4
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	7	3	4	4
Architectural	40	180	175	20	20
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	9	7	2	2
Structural Systems	64	320	240	32	32
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	10	6	2	1
Envelope Systems	56	252	210	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	9	6	2	1
Utility Systems	112	168	70	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	2	6	2	2	1
Mechanical Systems	56	224	175	126	126
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	8	5	9	9
Plumbing and Gas Systems	40	120	75	60	20
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	6	3	6	2
Electrical Systems	392	224	210	28	14
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	8	6	2	1
Fire Alarm Systems	72	216	320	36	18
Asset Value	9	9	9	9	9
Threat Rating	8	4	5	2	2
Vulnerability Rating	1	6	8	2	1
IT/Communications Systems	512	192	240	32	16
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	8	6	6	2	1