UiT
NORGES ARKTISKE UNIVERSITET

Institutt for ingeniørvitenskap og sikkerhet

Dimensjonering av sikringstiltak mot tilsiktede uønskede handlinger

En kvalitativ studie av sårbarhetsvurderinger som et verktøy for dimensjonering av sikringstiltak i norske ISPS-havneanlegg

Eirik Korneliussen

Masteroppgave samfunnssikkerhet, fordypning i sikkerhet og beredskap i nordområdene

Desember 2017

Antall ord: 20 247

UNIVERSITETET I TROMSØ

Sammendrag

Terror er ikke et nytt fenomen i Europa. Likevel har terrorfokuset økt som et resultat av en rekke alarmerende hendelser de siste tiårene. Etter terrorangrepene mot USA 11. september 2001 fikk den vestlige verden for alvor opp øynene for hvordan terrorangrep kan bli utført på den internasjonale arena. Som følger av terrortrusselen utviklet FNs sjøfartsorganisasjon, IMO, ISPS-koden. Koden stiller krav til at havneanlegg som betjener skip i internasjonal fart skal sikres mot tilsiktede uønskede handlinger. Den enkelte sjøfartsnasjon har selv ansvaret for å følge opp at havneanlegg tilfredsstiller kravene i ISPS-koden. I Norge ligger dette ansvaret hos Kystverket. Hvordan havneanleggene sikres, avgjøres gjennom en «port facility security assessment» og en «port facility security plan». I forskrift om sikring av havneanlegg omtales disse som «sårbarhetsvurdering» og «sikringsplan». Sårbarhetsvurderinger er i praksis en risikoanalyse for havneanlegget. Denne risikoanalysen danner grunnlaget for sikringsplanen, som beskriver sikringstiltakene i havneanlegget. Kystverket har utarbeidet en mal som gir retningslinjer for utarbeidelse av sårbarhetsvurderinger.

Problemstillingen i oppgaven er: «*Hvordan fungerer sårbarhetsvurderinger som et hensiktsmessig verktøy for dimensjonering av sikringstiltak i norske ISPS-havneanlegg?»*. Bakgrunnen for oppgaven er at det kan være utfordrende å gjennomføre risikoanalyser for tilsiktede uønskede handlinger. En har gjerne et for smalt datagrunnlag til å basere analysen på frekvensbasert sannsynlighet. Videre er trusselaktørene i stadig endring, og det kan være vanskelig å vurdere når risikoen er på et akseptabelt nivå. Utfordringene har demonstrert et behov for en standardisert tilnærming til slike risikoanalyser. I perioden 2012-2014 utarbeidet en arbeidsgruppe en standardserie som søker å dekke dette behovet. Norsk Standard 5832:2014, «Krav til sikringsrisikoanalyse», gir et forslag til hvordan en kan gjennomføre risikoanalyser mot tilsiktede uønskede handlinger. Standarden omtaler ikke sannsynlighet, men legger opp til at en virksomhets risikobilde sammenstilles på bakgrunn av trussel-, sårbarhets-, og konsekvensvurderinger. Kystverket har valgt å legge standarden til grunn for malen for gjennomføring av risikoanalyser for havneanlegg.

I oppgaven diskuteres NS 5832:2014, Kystverkets mal, og foreliggende sårbarhetsvurderinger opp mot et teoretisk rammeverk. Studien har vist at både NS 5832:2014 og Kystverkets mal oppfyller de fleste kravene til en god risikoanalyse, og således er hensiktsmessige verktøy for dimensjonering av sikringstiltak i norske ISPS-havneanlegg. En svakhet med metodikken er manglende beskrivelse og vurdering av usikkerhet. I tillegg viser betraktninger fra

foreliggende sårbarhetsvurderinger at trusselvurderinger, sårbarhets- og konsekvensvurderinger og risikovurderinger avgjøres av havneanleggets beliggenhet, operasjoner, og omfanget av operasjonene. Dette er faktorer som kartlegges innledningsvis i sårbarhetsvurderingene, og gjør at en allerede på dette tidspunktet har dannet seg et bilde av hvordan risikobildet blir. En kan dermed ende opp med å gjennomføre en analyse for å støtte en gitt oppfatning, istedenfor å foreta en selvstendig analyse.

Forord

Denne oppgaven markerer ikke bare slutten på mastergradsstudiet i samfunnssikkerhet, men også over 5 år som student ved Universitetet i Tromsø – Norges Arktiske Universitet. Disse årene har gitt meg mange gleder og nye bekjentskaper. Jeg ble ansatt i Kystverket Nordland i januar 2017, hvor studiene har vist seg å komme godt med.

Jeg ønsker først og fremst å takke min veileder, Maria Sydnes. Rådene og innspillene jeg har fått fra deg har vært helt sentrale for å holde meg på riktig kjøl. Videre ønsker jeg å takke familie, venner og medstudenter for en fin studietid med gode diskusjoner og sosialt samvær. En stor takk rettes også til Nora, for støtte og nådeløs korrekturlesing!

Til slutt vil jeg takke Kystverket, som har gitt meg tid og rom til å få dette prosjektet i havn.

Kabelvåg, 15. desember 2017 – Eirik Korneliussen

Innhold

1. Innledning

Terror er ikke et nytt fenomen i Europa. Likevel har terrorfokuset økt som et resultat av en rekke alarmerende hendelser de siste tiårene, særlig fra ekstreme islamister (Nesser, Stenersen og Oftedal, 2016). Etter terrorangrepene mot USA 11. september 2001 fikk den vestlige verden for alvor opp øynene for hvordan terrorangrep kan bli gjennomført på den internasjonale arena. I løpet av de siste årene har flere dødelige angrep vært rettet mot befolkede steder i Europa. Angrep har rammet blant annet England, Frankrike og Belgia og ført til at flere hundre mennesker har mistet livet (Harris, 2017, Nesser m.fl., 2016). Norges første møte med terrorisme i nyere tid skjedde i Oslo og på Utøya 22. juli 2011 (NOU 2012:14). Til tross for at dette angrepet ble gjennomført av en høyreekstrem terrorist, sier PST (2017) at ekstreme islamister representerer den største terrortrusselen mot Norge. Dette illustrerer at terrortrusselen er i konstant endring, noe krever kontinuerlig tilpasning fra en rekke ulike aktører. Dermed er det nødvendig at tilnærmingene til risikoanalyser også utvikles og forbedres.

Både tett befolkede steder og industrien blir rammet av terrorangrep. Havner og havneanlegg er en del av infrastrukturen som benyttes både i næringsvirksomhet og av store deler av befolkningen. En kan dermed anta at terrorisme og kriminalitet også kan utgjøre en trussel mot maritim virksomhet, til tross for at terrorangrep rettet mot maritim sektor bare utgjør litt over 1 % av de registrerte terrorangrepene i verden i perioden 1970-2013 (Jiang, 2017 i LaFree og Freilich, 2017). Som følge av den potensielle trusselen mot maritim sektor ble koden for «International Ship and Port facility Security» (ISPS-koden) utviklet og vedtatt i FNs sjøfartsorganisasjon, International Maritime Organization (IMO), som en utvidelse av SOLAS-konvensjonen (Safety Of Life At Sea). Regelverket ble iverksatt 1. juli 2004. Hensikten med koden er å etablere et internasjonalt rammeverk for samarbeid mellom myndigheter, kommuner, operatører, havner, havneanlegg og skipsindustrien. Samarbeidet skal sørge for at en oppdager og vurderer sikkerhetstrusler for å kunne komme med tiltak som beskytter havner, havneanlegg og skip som opererer i internasjonal trafikk (IMO, 2003). Alle havneanlegg som ønsker å motta skip i internasjonal trafikk må tilfredsstille kravene fra ISPS-koden. For å bli godkjent stilles det krav om at hvert havneanlegg må utarbeide en sårbarhetsvurdering (port facility security assessment) og en sikringsplan (port facility security plan) (IMO, 2003).

Sårbarhetsvurderinger og sikringsplaner er elementer i en risikoanalyseprosess. Det er særlig interessant å studere sårbarhetsvurderinger, ettersom analyser av tilsiktede uønskede handlinger kan være svært utfordrende å gjennomføre (Dillon m.fl., 2009, Jore og Moen, 2015). Det er vanskelig å basere seg på statistikk, da en ofte har lite data. I tillegg består truslene av tenkende aktører som kan tilpasse seg de sikringstiltak som iverksettes. En må også utvikle troverdige trusselscenarioer, som stiller store krav til kunnskaper om trusselaktørenes intensjoner, kapasiteter og handlingsmønster. Det kan også være en utfordring å definere en grense for når sikringen er god nok. I tillegg finnes det lover og regler en må forholde seg til, og som legger føringer for sikringen. Videre har en heller ingen garanti for at en noen gang får se effekten av sikringen, noe som kan gjøre det vanskelig å vite om en har iverksatt de riktige tiltakene. Utfordringene knyttet til risikoanalyser for tilsiktede uønskede handlinger har blitt synliggjort i både nasjonal og internasjonal forskning de senere årene (Busmundrud, Maal, Kiran og Endregard, 2015, Jore og Moen, 2015, Cox Jr, 2008 og 2009, Brown og Cox Jr, 2010). Yang, Ng og Wang (2014) har studert muligheten for en kvantitativ tilnærming til risikovurderinger for havnesikring med fokus på kost-nytte analyser, men det finnes lite forskning på kvalitative risikoanalysemetoder for havnesikringsfeltet. Det synes derfor viktig å studere utfordringen mellom å finne en hensiktsmessig risikoanalysemetodikk, gjennomføringen av risikoanalysen, og i tillegg forholde seg til sikringskrav fra regelverket.

I denne studien relateres havnesikring til risiko for tilsiktede uønskede handlinger. Det er delte meninger om hvorvidt de samme fremgangsmåter for risikoanalyser bør benyttes for tilsiktede uønskede handlinger som for utilsiktede hendelser (Busmundrud m.fl., 2015). Kystverket (2016a) har valgt å legge Norsk Standard 5832:2014 til grunn for gjennomføringer av sårbarhetsvurderinger i norske havneanlegg. Denne standarden er spesifikt rettet mot risikoanalyser mot tilsiktede uønskede handlinger. Standarden har fått kritikk for manglende vitenskapelig forankring (Busmundrud m.fl., 2015). Derfor er målet med denne studien å se nærmere på denne metodens fremgangsmåte i lys av vitenskapelig forankrede teoretiske perspektiver. Videre er det interessant å undersøke hvordan Kystverket lykkes med å operasjonalisere standarden, og hvilken innvirkning fremgangsmåten har på dimensjoneringen av sikringstiltak i ISPS-godkjente havneanlegg.

1.1. Litteraturgjennomgang

Det er gjennomført flere studier som retter seg mot risikoanalyser forbundet med terrorisme og kriminalitet. Dillon m.fl. (2009) mener det er flere utfordringer knyttet til slike

risikovurderinger. Trusselaktører kan ha forskjellig motivasjon og kan raskt endre sine mål. Videre kan den som står overfor risikoen iverksette ulike sikringstiltak som det kan være vanskelig å fastslå effekten av. Forskningen til Kujawski og Miller (2007) fremhever at statistiske metoder er lite anvendelige når det kommer til tilsiktede uønskede handlinger. Dette skyldes blant annet at det stadig dukker opp nye metoder for å ramme et mål. Kujawski og Miller (2007) mener derfor at det er mer hensiktsmessig å vurdere sannsynligheten for at et angrep lykkes dersom det skulle skje, enn sannsynligheten for om det vil bli gjennomført. Dette stiller store krav til valg og utarbeidelse av scenarioer. Brown og Cox Jr (2010) problematiserer også bruken av tradisjonelle sannsynlighetsbaserte risikoanalyser når en skal analysere terror-risiko. En av de store utfordringene forfatterne peker på, er angriperens evne til å tilpasse angrepet etter de innførte sikringstiltakene. Dette synes å gjøre risikoen for tilsiktede uønskede handlinger unike, fordi trusselaktøren aktivt søker informasjon og ut fra denne tilpasser sin fremgangsmåte. Hvis en derimot skal si noe om sannsynlighet, mener også Brown og Cox Jr. (2010) at det er mer interessant å vurdere sannsynligheten for at et angrep lykkes, dersom det skulle inntreffe.

Aven og Renn (2008) mener at også kvantitativ risikoanalyse er viktig når en analyserer risiko for tilsiktede uønskede handlinger. Forfatterne understreker viktigheten av å være klar over at de statistiske dataene kan være mangelfulle, og mener derfor at usikkerhetsbegrepet spiller en sentral rolle. Dette stiller større krav til bakgrunnskunnskapen hos den som gjennomfører risikoanalysen. Busmundrud m.fl. (2015) har tidligere studert ulike tilnærminger til risikovurderinger for tilsiktede uønskede handlinger. Særlig fokus blir rettet mot metodikkene i Norsk Standard 5814:2008 og Norsk Standard 5832:2014. De største forskjellene på de to standard-seriene er at NS 5832:2014 er spesifikt rettet mot tilsiktede handlinger, og omtaler ikke sannsynlighet i sin tilnærming. Forskningen fremhever både styrker og svakheter hos begge standardene. Imidlertid pekes det på at NS 5814:2008 har en mye bredere vitenskapelig forankring. Videre understrekes det blant annet at det ikke finnes en omforent beste fremgangsmåte for risikovurderinger for tilsiktede uønskede handlinger (Haneborg, 2015, i Busmundrud m.fl., 2015). Thomas Haneborg, et av medlemmene i arbeidsgruppen til NS 5832:2014 og seniorrådgiver i PST, fremhever den nye standardens fokus på verdiene som trenger beskyttelse. Haneborg peker på at dette er sentralt for å vite hvor det behøves tiltak (Busmundrud m.fl., 2015). Lederen ved Center for risk management and Societal Safety (SEROS) ved Universitetet i Stavanger, Sissel Haugdal Jore, fremhever at det positive med NS 5832:2014 er at denne standarden får virksomheter til å prioritere hvilke verdier en vil

beskytte, samt anerkjenne verdiens sårbarhet overfor ulike trusselaktører. Hun mener likevel at standarden har en manglende begrepsdybde og at den ikke sier noe om usikkerhet. Jore trekker også frem viktigheten av at virksomheten selv må ha eierskap til prosessen og resultatene i ettertid (Haugdal Jore, 2015, i Busmundrud m.fl., 2015).

Manunta (1997) peker på at enhver sikringskontekst består av forholdet mellom en verdi, en trussel og en beskytter, og dermed at dette er de tre sentrale elementer som må kartlegges. Av disse er beskytteren det eneste elementet en kan påvirke for å redusere konsekvensen av et angrep, og en bør derfor identifisere beskytterens sårbarheter. Bier (2007) vektlegger at en må velge hva som skal beskyttes, og at den som ønsker å beskytte seg er nødt til å prioritere ressurser på ulike områder, på samme måte som en trusselaktør må velge hva og hvor en vil angripe. For å kunne gjøre dette mener Bier (2007) at det er viktig å studere den strategiske adferden til trusselaktøren. Her eksemplifiserer Bier (2007) med å si at skanning av kontainere for farlig gods i store havner kan være et svært godt tiltak, frem til trusselaktøren får kunnskap om tiltaket og dermed flytter aktiviteten til en havn uten dette systemet. Dillon m.fl. (2009) trekker frem at de fleste forskere er enige om at terrorrisiko innebefatter elementene trussel, sårbarhet og konsekvens, men at det finnes ulike teorier rundt hvordan disse skal vurderes.

Cox Jr (2008) viser til at "Department of Homeland Security" (DHS) bruker modellen «risiko = trussel x sårbarhet x konsekvens». DHS bruer denne modellen på en semi-kvantitativ måte og knytter tallverdier til de ulike faktorene. Cox Jr (2008) er kritisk til at modellen tvinger risikoanalytikere til å bruke og tolke tall uten klare konseptuelle definisjoner. Hovedutfordringen blir ofte at en vurderer trusselaktørens handlinger som mer eller mindre tilfeldige, der en egentlig bør vurdere trusselaktører som intelligente opportunister som tilpasser handlingene sine etter de svake leddene i et objekts sikring (Cox Jr, 2008).

Det eksisterer flere utfordringer når en skal gjennomføre risikoanalyser for tilsiktede uønskede hendelser. Jore og Moen (2015) peker på valg av trusselscenarioer som en sentral utfordring i denne typen analyser. En må blant annet finne et tilstrekkelig utvalg relevante scenarioer, og bestemme hvilket sikringsnivå en er tilfreds med. I tillegg er risikoen i stadig endring. Det kan dermed være vanskelig å beregne hvilke tiltak som er effektive, og å kunne beregne kost/nytte for de iverksatte tiltakene.

Cox Jr (2009) har også studert hvordan en går frem for å sikre seg mot tilsiktede uønskede handlinger. Han påpeker at risikoreduserende tiltak må evalueres etter hvor effektivt tiltakene

faktisk reduserer risiko, og at tiltakene kan bli uinteressante hvis andre tiltak åpenbart synes å kunne redusere risikoen mer. Cox Jr. (2009) fortsetter med at det er essensielt å modellere hvordan en angriper vil respondere når aktøren møtes med et tiltak. Dette stiller store krav til utarbeidelse av scenarioer, noe som også understrekes av Jore og Moen (2015).

Basert på utfordringene som presenteres, synes det å foreligge et behov for å se nærmere på sammenhengen mellom metodikk for risikoanalyser mot tilsiktede uønskede handlinger og dimensjoneringen av sikringstiltak. I tillegg synes det å være lite forskning som direkte forholder seg til lovverk på et fagområde, og jeg vil derfor inkludere denne dimensjonen i min studie.

1.2. Formålet med studien

Det internasjonale regelverket er i Norge operasjonalisert gjennom Havne- og farvannsloven, samt forskrift om sikring av havneanlegg. Lovens formål er blant annet å legge til rette for effektiv og sikker havnevirksomhet (Havne- og farvannsloven § 1, 2009). Kystverket er ansvarlig for implementering og oppfølging av regelverket (Forskrift om sikring av havneanlegg § 20, 2013). Regelverket har etablert tre maritime sikringsnivåer, der nivå 1 er det laveste og nivå 3 er det høyeste. Tiltakene som gjennomføres på de ulike nivåene bestemmes gjennom havneanleggets sikringsplan som utarbeides på bakgrunn av en sårbarhetsvurdering. Senest i juli 2014 måtte 600 norske ISPS-godkjente havneanlegg trappe opp beredskapen for en periode, på ordre fra Kystverket (Kystverket, 2014, Aftenposten, 2014). Det maritime sikringsnivået ble hevet til nivå 2 på bakgrunn av at Politiets sikkerhetstjeneste (PST) gikk ut med informasjon om at det forelå en konkret terrortrussel mot Norge, med ukjent mål og tidspunkt for gjennomføring.

Lovverket stiller visse krav til måten en skal sikre seg på, og Kystverket har utgitt flere maler for hvordan en sårbarhetsvurdering og en sikringsplan kan utformes (Kystverket, 2012). Den siste malen ble utgitt i desember 2016. Det er havneanleggene selv som må utforme og iverksette hensiktsmessige tiltak som tilfredsstiller kravene, men regelverket stiller krav til at sårbarhetsvurderinger gjennomføres av sikringsvirksomheter som er godkjent av Kystverket. Slike virksomheter kalles for «Recognized security organizations» (RSO). Disse godkjennes gjennom å oppfylle en rekke kompetansekrav definert i ISPS-koden (IMO, 2003).

Uansett hvilken metode en velger å benytte for å avdekke og beskrive risiko, er hensikten å konkludere med hvilke tiltak som må iverksettes for å få risikoen til et akseptabelt nivå. Planleggingen skal føre til tilpassede tiltak (Perry og Lindell, 2003), og samtidig skal en

risikovurdering aldri være designet slik at en får en analyse som støtter et allerede gitt svar (Yoe, 2012). Et av utgangspunktene for denne studien er at det finnes ulike tilnærminger til risikoanalyser for tilsiktede uønskede handlinger, og at disse skal danne grunnlaget for en risikohåndteringsstrategi og sikringstiltak. Formålet med studien er å studere en foreliggende metode for gjennomføring av risikoanalyser for tilsiktede uønskede handlinger, og undersøke hvorvidt denne metoden er hensiktsmessig i en havnesikringskontekst. Foksuområdet for casen i denne studien er markert med rød ramme i figuren under.

Figur 1: Godkjenningsprosessen for norske havneanlegg som ønsker motta skip i internasjonal fart.

1.3. Problemstilling og forskningsspørsmål

På bakgrunn av nevnte formål er følgende problemstilling formulert:

Hvordan fungerer sårbarhetsvurderinger som et hensiktsmessig verktøy for dimensjonering av sikringstiltak i norske ISPS-havneanlegg?

For å kunne svare på problemstillingen stilles følgende forskningsspørsmål:

1. *Kan Norsk Standards metode anses som et hensiktsmessig verktøy for gjennomføring av risikoanalyser for tilsiktede uønskede handlinger?*

For å si noe om hvorvidt sårbarhetsvurderinger fungerer som et hensiktsmessig verktøy, er det naturlig å starte med hva som kan regnes som hensiktsmessig i denne sammenheng. For å undersøke dette vil Norsk Standard 5830-serien, med hovedvekt på 5832:2014, studeres og vurderes opp mot relevant teori om sårbarhet og risikoanalyser. Det er nødvendig å studere

standarden som et verktøy i seg selv fordi denne gir et forslag til en universell risikoanalysemetodikk for tilsiktede uønskede handlinger.

2. *Hvordan gjennomføres og utformes sårbarhetsvurderinger for norske ISPS-havneanlegg?*

En undersøkelse av hvorvidt sårbarhetsvurderinger fungerer som et hensiktsmessig verktøy, vil bero på en undersøkelse av hvordan norske sårbarhetsvurderinger gjennomføres og utformes. Her vil Kystverkets mal for utarbeidelse av sårbarhetsvurderinger, som er basert på NS 5832:2014, være gjenstand for undersøkelse. Hensikten er å ta risikoanalysemetodikken fra Norsk Standard ned et nivå, for å se hvordan risikoanalyser for tilsiktede uønskede handlinger kan operasjonaliseres i en gitt kontekst som også har et regelverk å ivareta. I tillegg er det hensiktsmessig å se nærmere på noen gjennomførte sårbarhetsvurderinger fra norske ISPS-havneanlegg. Under dette forskningsspørsmålet vil jeg også se nærmere på hvilke føringer regelverket legger for gjennomføringen av sårbarhetsvurderinger.

3. *Hvordan bidrar en analyse av sårbarhet til å fremstille et risikobilde for havneanleggene, og hvordan brukes dette til utforming av tiltak?*

Det tredje forskningsspørsmålet er todelt. Avdekking av sårbarheter i et system er en metode for å avdekke punkter som krever beskyttelse. Dette forskningsspørsmålet tar sikte på å undersøke hvordan avdekking av sårbare punkter bidrar i fremstillingen av et risikobilde. Også her er det naturlig å se på foreliggende sårbarhetsvurderinger og forklaringer fra NS 5830-serien. Ved å stille dette forskningsspørsmålet kan en finne ut hvordan risikobildet brukes ved utformingen av sikringstiltak. For å undersøke dette vil resultater fra sårbarhetsvurderinger vurderes som et grunnlag for utforming av sikringstiltakene i havneanleggenes sikringsplan.

1.4. Avgrensning

Denne studien tar for seg systemet rundt norske havneanlegg som er godkjent for å motta skip i internasjonal fart. Dette innebærer at studien kun omfatter havneanlegg på norsk territorium, som har Kystverkets ISPS-godkjenning.

Oppgaven avgrenses mot å omhandle havneanlegg, ikke havner. Reglene rundt sikring av havneanlegg kommer fra FNs sjøfartsorganisasjon IMO, gjennom EU-forordning 725/2004 og ISPS-koden, og reglene rundt sikring av havner kom gjennom Direktiv 2005/65/EF (EU/EØS-direktiv). Et «havneanlegg» defineres av IMO (2012, s. 11) som en lokasjon fastsatt

av departementene eller Kystverket, der skip-havn-operasjoner forekommer. Dette inkluderer vente- og ankringsområder. En havn defineres som et bestemt land- og sjøområde med grenser fastsatt av den aktuelle staten havnen befinner seg i, som inneholder anlegg og utstyr som benyttes til å betjene kommersiell sjøtransport (Directive 2005/65/EC, 2005, article 3). I praksis innebærer dette at en havn er et bestemt område der det ligger ett eller flere havneanlegg. Både skip og havneanlegg omfattes av det internasjonale regelverket, men i denne studien ligger fokuset kun på havneanlegg. Dette skyldes at sikring av skip gjennomføres gjennom en annen forskrift som Sjøfartsdirektoratet har ansvaret for.

Problemstillingen tar sikte på å undersøke hvorvidt sårbarhetsvurderinger er et hensiktsmessig verktøy for å konkludere med sikringstiltakene som vedtas gjennomført i havneanleggene. Fokus i denne oppgaven er dermed på planleggingsfasen i en beredskapssammenheng. Studien har ikke fokus på havneanleggenes respons i en eventuell beredskapssituasjon.

2. Teori

Dette kapitlet presenterer en oversikt over teorien som ligger til grunn for denne studien. Teorien vil danne et rammeverk for innsamling av data, samt analyse av denne i drøftingskapitlet. Sårbarhetsvurderinger og sikringsplaner er begge viktige i beredskapsplanleggingen for norske ISPS-havner. Derfor vil teorikapitlet innledningsvis presentere en generell beskrivelse av beredskapsplanlegging. Videre tar kapitlet for seg risikoanalyseprosessen, herunder planlegging av analysen, risikovurdering og risikohåndtering. Hensikten er å danne et teoretisk rammeverk for å kunne si noe om hvordan sikringstiltak i norske ISPS-havner blir til, hvorfor de blir som de blir, og om en eventuelt kunne kommet frem til andre sikringstiltak.

2.1. Beredskapsplanlegging

Å planlegge hensiktsmessige sikringstiltak er en del av beredskapsplanleggingen. Planlegging kan defineres som «en form for systematisk og faglig kunnskapsinnhenting og –bearbeidelse som foregår før beslutningstakere fatter beslutninger og iverksetter tiltak» (Aven, Boyesen, Njå, Olsen og Sandve, 2004, s. 46). Noen planlegger fordi de må, andre planlegger fordi det synes fornuftig, og mye planlegging gjøres fordi det er lovpålagt (Aven m.fl., 2004). Det finnes store mengder forskning på planleggingsfeltet i beredskapsøyemed (Quarantelli, 1977, Dynes, 1994). Alexander (2005) fokuserer på retningslinjer for katastrofeplanlegging og har vist behovet for en standard på området på grunn av store variasjoner i beredskapsplaner. Perry og Lindell (2003) presenterer ti retningslinjer for hvordan en kan planlegge for uønskede hendelser og viser ofte til terrorangrepet i New York 11. september. I det følgende presenteres utdrag av noen av retningslinjene som anses mest relevant sett i sammenheng med problemstillingen.

Perry og Lindell (2003) mener utgangspunktet for beredskapsplanlegging vil være tilnærmet likt, for både utilsiktede hendelse og tilsiktede handlinger. Den første retningslinjen for beredskapsplanlegging er at planleggingen skal baseres på kunnskap om truslene en står ovenfor og på den sannsynlige menneskelige responsen. Viktigheten av kunnskapsinnhentingen understøttes av den ovennevnte definisjonen til Aven m.fl. (2004). Kunnskapen om trusler får en gjennom trusselvurderinger og sårbarhetsanalyser (Perry og Lindell, 2003). En skal finne den beste tilgjengelige informasjonen, men samtidig være klar over at den informasjonen som er best tilgjengelig, ikke nødvendigvis er den mest optimale eller fullstendig uttømmende.

Når en i beredskapsplanleggingen har identifisert aktuelle trusler og sårbarheter, blir det lettere å klarlegge hvilken ekspertise som er nødvendig for prosessen videre (Perry og Lindell, 2003). Identifisering av risiko krever som oftest samarbeid mellom virksomheten som driver beredskapsplanleggingen og myndigheter eller andre relevante aktører. Hensikten er å kombinere den lokale kunnskapen til virksomheten med ressursene og ekspertisen til andre aktører (Perry og Lindell, 2003).

Videre skal en effektiv planlegging føre til at en velger tilpassede tiltak. Nøye planlegging fører til hurtigere respons (Perry og Lindell, 2003). Quarantelli (1977) fokuserer derimot mer på at riktig og tilpasset respons er viktigere enn rask respons. Planlegging skal bidra til at en holder igjen impulsive reaksjoner, og heller iverksetter passende handlinger i den gitte situasjonen. Planleggere må også anerkjenne at hendelser er dynamiske og endrer seg hele tiden (Staupe-Delgado og Kruke, 2017). Dette innebærer at det er umulig å forutse og planlegge for alle hendelser som kan oppstå. Derfor er det viktig at en planlegger for en fleksibel respons, slik at de involverte kan justere handlingene sine etter det som kreves av hendelsen (Perry og Lindell, 2003 og Staupe-Delgado og Kruke, 2017). I praksis betyr dette at en bør unngå for mange detaljer i planleggingen av kriseresponsen, og heller ha fokus på viktige prinsipper. En viktig årsak til dette er at detaljfokusert planlegging stadig har behov for ressurs- og tidkrevende oppdateringer og tilpasninger (Dynes m.fl., 1972).

Perry og Lindell (2003) beskriver planlegging som en kontinuerlig prosess, og påpeker at dette er en av de viktigste egenskapene til et godt planverk. Det forventes at planer forbedres etter alle øvelser, treninger og faktiske hendelser. Det er også viktig at en ikke bruker et skrevet planverk som en hvilepute. Dersom en betrakter skrevne planer som et ferdig produkt, risikerer en å leve i god tro om at en er forberedt på situasjoner, der dette ikke er tilfellet (Quarantelli, 1977).

I denne studien omtales planlegging i forbindelse med gjennomføringen av sårbarhetsvurderinger. Aven, Røed og Wiencke (2008) omtaler sårbarhetsanalysen som en del av risikoanalysen. Sårbarhet kan defineres som «…kombinasjonen av mulige konsekvenser og usikkerhet, gitt at et system utsettes for en initierende hendelse» (Aven m.fl., 2008, s. 33). Aven m.fl. (2008) viser også til Sårbarhetsutvalget (NOU 2000:24) som sier at sårbarhet knyttes opp til mulig tap av verdier. Det er altså en forutsetning å definere verdiene en ønsker å beskytte før en kan gjennomføre en sårbarhetsvurdering. På bakgrunn av en slik vurdering kan en konsultere med de riktige fagfolkene for å innhente informasjon om hvordan en kan håndtere de aktuelle truslene en står ovenfor (Perry og Lindell, 2003). En kan dermed

argumentere for at en ved gjennomføringen av en sårbarhetsanalyse må kartlegge sine verdier, identifisere relevante trusler, samt innse sine begrensinger og sårbarheter ovenfor trusselen. Studien vil videre se nærmere på om dette er en praksis som brukes i sårbarhetsvurderinger for norske ISPS-havneanlegg.

2.2. Risikoanalyseprosessen

Risikoanalyseprosessen er en sentral del av beredskapsplanleggingen. Analysen kan brukes til å etablere et risikobilde og gir grunnlag for blant annet å velge mellom ulike tiltak, vurdere tilpasninger som kan gjøre et system mindre sårbart, og konkludere om ulike tiltak møter gitte krav (Aven m.fl., 2008). En risikoanalyse er en prosess for beslutningstaking under usikkerhet (Yoe, 2012). En analyse av risiko skal gjøre oss i stand til å kartlegge problemområder og studere effekten av ulike tiltak (Aven m.fl. 2004). Aven m.fl. (2008) deler risikoanalyseprosessen inn i tre overordnede faser. I det følgende vil disse fasene presenteres. Hovedfokuset vil være på fase 2, risikovurdering og fase 3, risikohåndtering, grunnet disse fasenes sammenhengende betydning for dimensjonering av sikringstiltak.

1. Planlegging av analysen
2. Risikovurdering
3. Risikohåndtering

2.2.1. Planlegging av analysen

I planleggingsfasen er det viktig å si noe om hvorfor en gjennomfører analysen. Aven m.fl. (2008) peker på klare målsettinger som en forutsetning for en god analyse. En må avklare grunnleggende momenter som ressursbruk og organisering. Videre må en innhente nødvendig informasjon og det må klargjøres hvordan en ønsker å analysere denne. Informasjonen en samler inn i planleggingsfasen utgjør grunnlaget for hva en skal vurdere i neste fase, risikovurderingen. Planlegging av analysen er således viktig for den helhetlige risikoanalyseprosessen og skal ifølge Aven m.fl. (2008) vektlegges i like stor grad som de andre to fasene. Det skal i denne studien ses nærmere på en allerede gitt analysemetode, og dermed blir det et større fokus på stegene for risikovurdering og risikohåndtering.

2.2.2. Risikovurdering

Risikovurderingen er den vitenskapsbaserte delen av en risikoanalyse. Den gir informasjon om risiko, og skal skape et grunnlag for beslutningstakingen. Dersom en har oversikt over hvilke verdier en eier, kan en finne ut hvilke potensielle farer som truer. Vurderingen skal også inkludere en beskrivelse av den relevante usikkerheten som kan påvirke beslutningene

(Yoe, 2012). Risiko er dermed ikke noe som kan fastslås som et objektivt faktum, men heller en «…kombinasjon av usikkerhet og konsekvens/utfall av en gitt aktivitet» (Aven m.fl., 2004, s. 64). Denne definisjonen av risiko synes hensiktsmessig både når en snakker om risiko tilknyttet ulykker og tilsiktede hendelser. Jore og Njå (2010) understreker også at risiko er en vurdering, og ikke ren fakta. Aven m.fl. (2008) legger til at muligheten for at en hendelse med gitte konsekvenser vil inntreffe, kan uttrykkes med sannsynlighet med bakgrunn i kunnskap. Busmundrud m.fl. (2015) fremhever at det ikke er noen omforent fremgangsmåte for risikovurderinger for tilsiktede uønskede handlinger, men at kjennetegn som struktur, bred kompetanse, kartlegging av kunnskapsstyrken, klar kommunikasjon av risiko og usikkerhet, og et helhetlig perspektiv er noen av faktorene som går igjen. En risikovurdering bør aldri være designet på en slik måte at en skaper en analyse som skal støtte et allerede gitt svar (Yoe, 2012). Hvis beslutningstakerne allerede vet hvilke sikringstiltak de ønsker vil en risikovurdering være unødvendig. Yoe (2012) fremhever at prosessen ved å gjennomføre en risikovurdering er like viktig som resultatet.

Aven m.fl. (2008) peker særlig på at identifikasjon av initierende hendelser er viktig. Forfatterne mener at en vanskelig kan beskytte seg mot farer og trusler, dersom disse ikke er identifisert. I og med at beredskapsplanlegging, herunder også risikovurdering, er en kontinuerlig prosess, gjør en ofte analyser av liknende systemer flere ganger. Her er det vanlig å kopiere listen over trusler fra tidligere analyser (Aven m.fl., 2008). Dette innebærer at en lett kan overse lokale forhold og endringer i trusselbildet. Dette underbygger viktigheten av at risikovurderingen baseres på relevant og oppdatert kunnskap (Aven m.fl., 2004, Perry og Lindell, 2003).

Sikringsrisiko

I forbindelse med sikring av norske havneanlegg, snakker en om sikring mot tilsiktede uønskede handlinger (International Maritime Organization, 2003), eller sikringsrisiko (NS 5832:2014). I Norsk Standard 5832:2014 defineres sikringsrisiko som et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (Standard Norge, 2014, s. 4). Standarden nevner dermed ikke sannsynlighet i sin definisjon. Aven (2013) mener likevel at en forholder seg til sannsynlighet når en snakker om risiko knyttet til tilsiktede uønskede handlinger. Aven skiller mellom frekvensbasert og kunnskapsbasert sannsynlighet, og mener at den kunnskapsbaserte, som uttrykker usikkerhet eller troverdighet til den som utfører en vurdering, kan bli brukt med hensyn på sikringsrisiko (Busmundrud m.fl., 2015). Jore og Njå (2010) refererer til denne

typen sannsynlighet som en bayesiansk tilnærming. Hensikten med denne metodikken er at den gir større rom for å inkludere ekspertvurderinger når en snakker om sannsynlighet for utilsiktede hendelser, som for eksempel terrorisme (Jore og Njå, 2010). Rausand og Utne (2009) mener at en ved en bayesiansk tilnærming ikke trenger å avgrense seg til forsøk som utføres gjentatte ganger. Dette betyr at en ved hjelp av kunnskap om det aktuelle temaet kan si noe om sannsynlighet, uten store datamengder. Ettersom det foreligger begrenset med data og statistikk på terrorangrep, og en stor usikkerhetsfaktor knyttet til trusler (Dillon m.fl., 2009), er det viktig å kjenne til den kunnskapsbaserte tilnærmingen til sannsynlighet når en skal gjennomføre en risikovurdering for havneanlegg.

Et av medlemmene i arbeidsgruppen til NS 5832:2014 trekker frem at den gamle standarden, NS 5814:2008, omtaler sannsynlighet som et frekvensbasert fenomen, og dermed er uegnet for sikringsrisiko (Barane, J. i Busmundrud m.fl., 2015). Terje Aven, professor ved Universitetet i Stavanger, mener det er svært uheldig, og en stor svakhet å gå vekk fra sannsynlighetsbegrepet. Aven viser blant annet til at PST, ved omtalen av sannsynlighet for at et angrep skal skje i Norge, snakker om kunnskapsbasert sannsynlighet (Aven, T. i Busmundrud m.fl., 2015). Lederen for arbeidsgruppen som har laget NS 5832:2014, viser derimot til at mange virksomheter har lite kompetanse på securityfeltet og dermed har vanskelig for å forstå de ulike tolkningene av sannsynlighetsbegrepet: «Virkeligheten der ute er at man forstår sannsynlighet som frekvensbasert. I NS 5814 og i Sikringshåndboken står det at de tolker sannsynlighet som frekvensbasert. Det er dette folk leser, ikke artikler i vitenskapelige tidsskrifter» (Stranden, R. i Busmundrud m.fl., 2015, s. 130).

En ønsker å redusere risiko for å oppnå god sikkerhet. Sikkerhetsbegrepet brukes ofte ved omtalen av tiltak som skal redusere risiko, og i hvilken grad et system evner å unngå skader og tap (Aven m.fl., 2004). Sikkerhet omtales også som en «…tilstand som innebærer fravær av uønskede hendelser, frykt eller fare» (NS 5830:2012, s. 2). På engelsk skiller en ofte mellom «safety» og «security». Begge begrepene relateres til uønskede hendelser, men Idsø og Jacobsen (2000) og NOU 2000:24 sine definisjoner forklarer skillet med at safety relateres til uønskede hendelser som oppstår mer eller mindre tilfeldig, og security omhandler tilsiktede uønskede handlinger. Dette skillet er sentralt, da risiko i en havnesikringskontekst relateres til security. Williams (2013) peker også på at en må definere hvem sin sikkerhet en snakker om. Han sier at uten et referanseobjekt som ønskes beskyttet, står en heller ikke overfor trusler.

Manunta (1997) sin teori bygger på de samme prinsippene. Han mener at basiselementene av en security-kontekst består av en verdi, en beskytter og en trussel. Han argumenterer for at en

verdi bare eksisterer dersom det er noen som ønsker å beskytte denne, og at dersom en ikke står overfor en trussel, befinner en seg heller ikke i en sikringskontekst. En verdi kan dermed være alt en ønsker å beskytte, for eksempel menneskeliv, helse, omdømme og fysiske objekter (Manunta, 1997). Ifølge Manunta (1997) er beskytteren noen som ved eierskap eller ansvar for verdien har en interesse av å beskytte denne. Trusselen er i denne sammenheng en aktør som ved villede handlinger kan ramme verdien. Trusselen kan være vanskelig å definere, men han understreker at det vesentlige er at beskytteren oppfatter at det finnes en trussel med en intensjon og kapasitet til å påføre skade på verdien. Det er dermed behov for beskrivelse og vurdering av disse tre elementene for å vurdere hvilke tiltak en bør iverksette. De samme elementene finner en igjen i Cohen og Felson (1979) sin rutineaktivitetsteori som omhandler kriminalitet. Deres teori fokuserer på de tre faktorene «mulig gjerningsperson», «passende mål» og «fraværet av beskyttelse». Tar en bort én av faktorene har en ikke lengre en sikringskontekst.

Årsaksanalyse, konsekvensanalyse og risikobilde

Når en har kartlagt sine verdier og avdekket hvilke trusler en står ovenfor, gjennomføres en årsaks og –konsekvensanalyse (Aven m.fl., 2008). Det synes nødvendig med kunnskaper om årsaks- og konsekvensanalyser for å kunne vurdere hvorvidt norske ISPS-havneanlegg lykkes i en helhetlig analyse av sine sårbarheter. I årsaksanalysen skal en studere hva som må til for at en initierende hendelse oppstår. Her er det viktig å involvere eksperter med kunnskap om truslene en har identifisert (Aven m.fl. 2008). Dette synes spesielt viktig når en virksomhet skal sikre seg mot tilsiktede uønskede handlinger, fordi trusselbildet er usikkert og uforutsigbart. I konsekvensanalysen gjennomføres en vurdering av konsekvensene av hendelsene som kan oppstå. På bakgrunn av årsaks- og konsekvensanalysen etableres virksomhetens risikobilde, som kan sies å være en presentasjon av risikoresultater (Aven m.fl., 2008). Jore og Njå (2010) peker på at det er et stort behov for å studere risikobildene en kommer frem til. I forhold til tradisjonelle risikomodeller, bør en når en snakker om terrorisme, legge ekstra vekt på blant annet potensielle trusler, barrierer, sårbarhet i kritiske systemer, påvirkende faktorer for terrorister og sannsynligheter. Sannsynligheten må baseres på terroristenes intensjoner, kapasitet og effektene fra eventuelle barrierer og mottiltak (Jore og Njå, 2010).

En bør også uttale seg om usikkerheten som er knyttet til resultatene. Eksempelvis fastsettes det ofte kun én verdi av konsekvens, selv om en hendelse kan ha mange ulike utfall. Verdien en velger å fastsette på bakgrunn av konsekvensanalysen, omtales som forventningsverdien til

den gitte hendelsen (Aven m.fl., 2008). Dersom en bruker analysemetoder som konkluderer med én konsekvensverdi, må en også være klar over at hendelsen kan ha andre utfall enn det som presenteres i risikobildet.

Teorien rundt risikovurdering, årsaks- og konsekvensanalyse og risikobilder vil også benyttes for å kunne si noe om hva en risikoanalyse mot tilsiktede uønskede hendelser bør inneholde. En kan argumentere for at en god risikoanalyse må bygge på teori og forskning som sier noe om hvordan risikoanalysen bør gjennomføres. Videre vil teorien også være grunnleggende for forskningsspørsmål 2, der jeg vil undersøke hvordan sårbarhetsvurderinger i norske ISPS-havneanlegg gjennomføres, og hvorvidt denne metoden sammenfaller med teori om hvordan en risikoanalyse bør se ut.

2.2.3. Risikohåndtering

Aven m.fl. (2008, s. 69-70) definerer risikohåndtering som «…prosessen og implementeringen av virkemidler for å modifisere risiko, herunder virkemidler for å unngå, redusere, optimalisere og overføre risiko». Denne prosessen dekker dermed både identifisering og vurdering av tiltak, samt ledelsens vurdering og beslutning (Aven m.fl., 2008). En kan argumentere for at risikohåndteringen er selve målet med en hvilken som helst analyse av risiko. Det synes derfor helt essensielt å inkludere teori rundt selve håndteringen av risiko. Det er i dette steget en fatter beslutninger om hvilke strategier eller tiltak en velger for å håndtere risiko.

Tiltak som kan redusere risikoen kan enten være sannsynlighets- eller konsekvensreduserende (Aven m.fl., 2008, Reason, 1997, Rausand og Utne, 2009). Rausand og Utne (2009) mener det generelt er hensiktsmessig å prioritere sannsynlighetsreduserende tiltak foran konsekvensreduserende tiltak, dersom dette er mulig. Når en skal identifisere tiltak er det naturlig å ta utgangspunkt i hendelsene som påfører virksomheten størst risiko. Basert på sikringsmålene en ønsker å nå, må en søke alternative løsninger for å oppnå målet, og vurdere konsekvensene av løsningene som presenteres (Aven m.fl., 2004).

Et vanlig prinsipp for risikohåndtering er å gjennomføre en «As Low As Reasonable Practicable»-vurdering (ALARP). ALARP innebærer at risikoen skal reduseres så langt som praktisk mulig. Nytten ved å implementere et tiltak skal vurderes mot ulempen ved å implementere tiltaket (Aven m.fl., 2008). Denne balansen mellom kost-nytte er ofte avgjørende for hvorvidt en velger å implementere risikoreduserende tiltak (Aven og Renn, 2008). I mange tilfeller må en også ta hensyn til andre evalueringer, herunder gjeldende lover

og forskrifter (Yoe, 2012). Videre blir slike avgjørelser enda mer kompliserte når risikoen gjelder sikring i en security-kontekst, på grunn av den høye graden av usikkerhet (Jore og Moen, 2015). En kost-nytte vurdering gir dermed ikke et fasitsvar på hva som er det beste sikringsalternativet.

Aven m.fl. (2008, s. 72) presenterer tre steg som utgjør vurderingsprosessen for tiltak:

1. Grovvurdering av praktisk gjennomførbarhet og kostnader.
2. Konkludering vedrørende implementering der gevinst er åpenbart større enn ulempe.
3. Resterende tiltak skal inngå i en liste over tiltak med behov for en mer detaljert analyse- og vurderingsprosess.

Gjennom prosessens steg 1 og 2 kan en raskt avgjøre å implementere tiltak som synes å være åpenbare. Dette kan typisk være tiltak som koster lite, men som gir en relativt stor effekt på risikoen. En må likevel være oppmerksom på at risiko- og kostnadsberegninger ikke fanger opp alle aspekter som er viktige for beslutningen (Aven m.fl., 2008). Det finnes også flere aktuelle strategier for håndtering av risiko, herunder virkemidler for å unngå, overføre, optimalisere og akseptere risiko (Aven m.fl., 2008). Teorien om risikohåndtering vil sammen med teorien om sårbarhet gi en forståelse for forskningsspørsmål 3. Hensikten er å kunne si noe om hvordan en analyse av en virksomhets sårbarhet bidrar til fremstillingen av et risikobilde, og hvordan dette brukes for å dimensjonere sikringstiltak.

2.3. Analytiske implikasjoner

Gjennom kapitlet er det lagt fram et teoretisk rammeverk som er sentralt for å kunne undersøke problemstillingen. Problemstillingen består av flere deler og krever bidrag fra ulike teoretiske perspektiver. Dette har igjen ført til formuleringen av de tre forskningsspørsmålene. Ved å sette sammen ulike teoretiske bidrag ønsker jeg å kunne si noe om faktorer i en risikoanalyse som ulike teorier fremhever som nødvendige. På den måten kan jeg si noe om hva som kan anses som et hensiktsmessig verktøy for å dimensjonere sikringstiltak. Videre vil jeg analysere risikoanalysemetoden som i dag brukes i norske ISPS-havneanlegg, og si noe om hvorvidt denne metoden kan anses som hensiktsmessig. Til slutt vil teorien rundt sårbarhet og risikohåndtering kunne si noe om hvordan analyse av disse faktorene brukes til utforming av tiltak. Her er det sentrale å si noe om hvordan analysen av den avdekte sårbarheten tas med i vurderingen av et risikobilde og eventuelle sikringstiltak. Det vil også drøftes hvorvidt regelverket legger føringer for valg av tiltak.

3. Metode

I dette kapitlet vil oppgavens metodiske tilnærming presenteres og begrunnes. Oppgavens hovedmål er å undersøke hvorvidt sårbarhetsvurderinger er et hensiktsmessig verktøy for dimensjonering av sikringstiltak i norske ISPS-havneanlegg. Metodekapitlet tar sikte på å beskrive hvordan jeg har gått frem for å svare på problemstillingen.

3.1. Forskningsdesign

Et forskningsdesign beskriver et forskningsprosjekts fokusområde. Designet sier noe om hva og hvem som er gjenstand for undersøkelsen (Thagaard, 2009). Jeg har valgt å definere dette prosjektet som en case-studie, fordi jeg i stor grad undersøker samspillet mellom en spesiell gruppe og en spesiell kontekst (Jacobsen, 2005). I case-studier fokuseres det på én spesiell undersøkelsesenhet, men en enhet kan også bestå av en gruppe. En kan dele enheter inn i flere nivåer. En tenker ofte på en enhet som et enkeltindivid. Dette definerer Jacobsen (2005) som enheter på laveste nivå, eller en absolutt enhet. En case kan også være på et høyere nivå, og en snakker da gjerne om en kollektiv enhet. Jacobsen (2005) beskriver en kollektiv enhet som flere absolutte enheter, som da utgjør en gruppe, en organisasjon eller flere grupper. I dette prosjektet undersøkes et system, bestående av en gruppe aktører som befinner seg i en spesiell situasjon. Alle havneanlegg som ønsker en ISPS-godkjenning må gjennom den samme prosessen for å bli godkjent, og kan derfor betegnes som en kollektiv enhet.

Målet med studien er ikke å undersøke utbredelsen av, men å gå i dybden på et fenomen. Oppgavens tilnærming er derfor kvalitativ (Andersen, 1997). Dey (1993) viser til at kvantitative data uttrykkes med tall, og kvalitative data med meninger som i hovedsak formidles gjennom språk og handlinger (I Jacobsen, 2005, s. 126). Studien er tidsmessig avgrenset til å omhandle godkjenningsprosessen til havneanleggene, og studerer verktøyet som benyttes, fremfor brukerne.

3.2. Valg av tema og case

Jeg ble ansatt av Kystverket som rådgiver i havnesikring i januar 2017. Mine oppgaver går i hovedsak ut på å gjennomgå planverk, utstede ISPS-godkjenninger og føre tilsyn med at havneanleggene overholder bestemmelsene i regelverket. Jeg ble på et tidlig stadium introdusert for FFI-rapporten til Busmundrud m.fl. (2015) om tilnærminger til risikovurderinger for tilsiktede uønskede handlinger. Rapporten tar for seg en viktig debatt rundt ulike tilnærminger og ulike synspunkter mellom personer som arbeider med sikkerhet til daglig, og forskere. Gjennom mitt arbeid med gjennomgang av planverk, har jeg lest flere

titalls sårbarhetsvurderinger og sikringsplaner. Disse dokumentene er unndratt offentlighet fordi de inneholder skjermingsverdig informasjon om sikringen i havneanleggene. Planverkene har vist at selv om det gjennomføres egne sårbarhetsvurderinger for hvert enkelt havneanlegg, er tiltakene ofte svært like.

Yin (2014) påpeker at en må velge casen som mest hensiktsmessig belyser problemstillingen en ønsker å besvare. Stor grad av likhet mellom sikringstiltak, og en pågående debatt om tilnærminger til risikoanalyser mot tilsiktede uønskede handlinger, er årsaken til den valgte casen. Jeg ønsker å undersøke metodikken som brukes i det norske systemet for havnesikring, og hvordan denne bidrar til å dimensjonere sikringstiltakene som velges.

3.3. Datainnsamling

Datamaterialet i denne oppgaven består i all hovedsak av innsamlede dokumenter. Dokumenter er sekundærdata, som innebærer at dataen er samlet inn av andre (Jacobsen, 2005). Yin (2003) omtaler dokumenter som relevante for de fleste studier. Dokumenter har ofte samme styrke som intervjuer, ved at en får vite hva personer mener (Jacobsen, 2005). Styrken til dokumenter er at de ofte viser en mer gjennomtenkt og bearbeidet informasjon enn uttalelser fra intervjuer. Dette kan også være en svakhet, fordi en går glipp av spontane reaksjoner (Jacobsen, 2005). Et intervju er også kjent for å gi undersøkeren et unikt innblikk i menneskelige opplevelser fra deres ståsted, og en får muligheten til å gå dypt inn i hvordan enkeltpersoner oppfatter enkelte begivenheter og situasjoner i sitt eget liv (Brinkmann og Tanggaard, 2012). En kan likevel innhente kunnskap på mange måter gjennom tekst, og ved å tolke og filtrere informasjon kan en få grep om det som er bortenfor de nærmeste omgivelsene og vår egen oppfattelse (Bratberg, 2014).

I denne studien har jeg sett nærmere på følgende dokumenter:

- Norsk Standard: NS 5830:2012, Samfunnssikkerhet, Beskyttelse mot tilsiktede uønskede handlinger, Terminologi
- Norsk Standard: NS 5831:2014, Samfunnssikkerhet, Beskyttelse mot tilsiktede uønskede handlinger, Krav til sikringsrisikostyring
- Norsk Standard: NS 5832:2014, Samfunnssikkerhet, Beskyttelse mot tilsiktede uønskede handlinger, Krav til sikringsrisikoanalyse
- Norsk Standard: NS 5814:2008, Krav til risikovurderinger
- Kystverkets mal for utarbeidelse av sårbarhetsvurderinger (PFSA) for havneanlegg, 2016

- Kystverkets veileder for utarbeidelse av sårbarhetsvurderinger (PFSA) for havneanlegg, 2016
- Forskrift om sikring av havneanlegg, 2013
- ISPS-koden, IMO, 2003
- Interne dokumenter om antall sikringsplaner utarbeidet av RSO kontra sikringsleder, Kystverket, ikke offentlig tilgjengelig
- Sårbarhetsvurderinger for havneanlegg, utarbeidet etter mal av 2016 (Unntatt offentlighet)
- Sikringsplaner for havneanlegg, basert på sårbarhetsvurderinger som er utarbeidet etter mal av 2016 (Unntatt offentlighet)

Dokumentanalyse har etter mitt syn vært den mest hensiktsmessige metoden for å studere sårbarhetsvurderinger som dimensjonerende for sikringstiltak i ISPS-havneanlegg. Regelverket legger føringer for analyser, planverk og tiltak, og er derfor sentralt å inkludere i studien. Standardene beskriver hvordan noen mener sikringsrisikoanalyser bør gjennomføres. Sett opp mot teori på fagfeltet har jeg kunnet ta stilling til hvorvidt standarden er et hensiktsmessig verktøy for gjennomføring av risikoanalyser. Videre viser malen for gjennomføring av sårbarhetsvurderinger for havneanlegg hvordan Kystverket har valgt å operasjonalisere standarden.

I denne studien har jeg ikke gjennomført egne intervjuer. Jacobsen (2005) skriver at intervjuer blant annet egner seg når vi er interessert i hva det enkelte individ sier, eller hvordan en fortolker og legger mening i et spesielt fenomen. En kan naturligvis tenke seg at det ville vært gunstig å gjennomføre intervjuer med sikringsledere i havneanlegg, eller med representanter fra en RSO. Disse har førstehåndsinformasjon om hvordan sårbarhetsvurderinger utarbeides, og i hvor stor grad de vektlegges når sikringstiltak utformes. Intervjuer med disse parter ble sterkt vurdert, og informasjonen hadde utvilsomt vært nyttig.

Det er likevel to ting som har ført til fraværet av slike intervjuer i denne studien. For det første dreier studien seg i hovedsak om sammenhengen mellom et risikoanalytisk verktøy og gjennomføringen av sikringstiltak. Dette er et teoretisk fagfelt som dekkes godt av eksisterende faglitteratur, og foreliggende sårbarhetsvurderinger og sikringsplaner. For det andre, og kanskje den viktigst, vil min stilling som representant fra myndighetene ved Kystverket kunne påvirke respondentene. Jacobsen (2005) fremhever at en prøver å studere en objektiv virkelighet, som ikke må forstyrres av forskeren. En skal så langt det er mulig forsøke å unngå at resultatene blir styrt av hvem som gjennomfører forskningen. Det bør altså

være et skille mellom den som undersøker og den som undersøkes. En må huske at en aldri kan bli helt kvitt «forskningseffekter», og mange har hevdet at det vil være usant å hevde at forskningen er helt nøytral (Jacobsen, 2005). Likevel har jeg vurdert det dithen at min posisjon ha kunne påvirket respondentene i for stor grad til at intervjuer ville vært hensiktsmessige.

Det kan tenkes at eventuelle intervjuer kunne tilført empirisk materiale som hadde påvirket resultatene. RSOene kunne for eksempel ha bidratt med førstehåndsinformasjon om utfordringer knyttet til utarbeidelsen av trusselvurderinger og –scenarioer, som igjen kunne hatt innvirkning på hvilken metode som synes hensiktsmessig. Videre kunne sikringsledere fra havneanlegg gitt en oversikt over hvor mye disse involveres i risikoanalyseprosessen, og en kunne således fått en pekepinn på i hvilken grad RSOene anbefaler mer eller mindre standardiserte sikringstiltak.

Det synes også sentralt å nevne at min stilling i Kystverket har gitt meg tilgang på datamateriale som ellers ville vært vanskelig å få tak i. Dette har således også vært en utfordring, da deler av dokumentene er unntatt offentlighet og inneholder sikkerhetsgradert informasjon. Derfor har jeg ikke utarbeidet en liste over havneanleggene som sårbarhetsvurderingene og sikringsplanene som omtales i denne studien er hentet fra. De nødvendige kjennetegnene er heller omtalt i eksempler i empirikapitlet.

3.4. Deltakende observasjon

Observasjon handler om å registrere atferd i en kontekst, eller undersøke hva mennesker gjør, fremfor hva en sier at en gjør (Jacobsen, 2005). Et skille i observasjonsstudier dreier seg om hvorvidt undersøkeren deltar i en aktivitet eller ikke. Jeg har vært inne på tanken om hvorvidt min rolle som ansatt i Kystverket kan regnes som en deltakende observatør. Jeg arbeider daglig med gjennomgang og godkjenning av sårbarhetsvurderinger og sikringsplaner, og fører tilsyn med at havneanleggene gjennomfører de beskrevne sikringstiltakene. Dette har gjort at jeg har måttet vie mye oppmerksomhet til forskningseffekter, og ta hensyn til min egen forutinntatthet. Jeg vil påstå at det er umulig å ikke la seg påvirke av egne erfaringer, på godt og vondt. Tilsynene jeg har deltatt på har også gitt meg et unikt innblikk i hvordan tiltakene blir utformet i praksis. Samtidig har jeg ikke bevisst gjennomført observasjoner med hensyn på denne studien. Jacobsen (2005) påpeker at observasjoner som regel foregår på det fysiske stedet som er av interesse for problemstillingen. Med bakgrunn i dette kan en argumentere for at en form for observasjon har blitt gjennomført. Disse observasjonene går mest ut på at jeg

har fått et inntrykk av hvilke sikringstiltak som benyttes hyppig, og hvordan disse utformes i havneanleggene. Min rolle på tilsynene har ført til at jeg personlig også har sett behov for en studie som denne. Jeg har forsøkt å være så nøytral som mulig, og ikke legge mine observasjoner til grunn for det empiriske materialet som studeres.

3.5. Validitet

Krumsvik (2014) skriver at validitet handler om hvorvidt undersøkeren har studert det han hadde som formål å undersøke. Validitet sier noe om gyldigheten av en studie, og kan deles inn i intern og ekstern gyldighet (Jacobsen, 2005). Intern gyldighet beror på om resultatene en kommer frem til oppfattes som riktige. Jacobsen (2005) påpeker også at en i samfunnsvitenskapen egentlig snakker om riktighet i den forstand at noe er det nærmeste vi kommer sannheten. For at noe skal kunne omtales som riktig betyr dette i praksis at flere må være enige om at noe er riktig beskrevet.

Gjennom validering retter en et kritisk blikk på studien. En kan være kritisk til utvalget av, og innholdet i, datamaterialet. En må reflektere over om en har brukt de riktige enhetene, og om disse inneholder riktig informasjon. En bør også være kritisk til analysefasen for å undersøke om de sammenhengene en finner faktisk er reelle, eller konstruert av undersøkeren. (Jacobsen, 2005). Etter mitt syn har dokumentanalyser den styrken at en enkelt kan gjennomgå dokumenter i ettertid og få bekreftet den informasjonen som er gitt. I denne studien er majoriteten av dokumentene offentlig tilgjengelig. Til sammenligning vil det være vanskeligere å etterprøve intervjuer. Selv om en intervjuer med helt lik bakgrunn og i en helt lik kontekst bør kunne få ut de samme hovedpoengene, kan det være vanskelig å få tilgang til respondentene igjen, og svarene vil trolig variere noe (Batalden, 2015).

Det synes også relevant å nevne at Kystverkets mal for utarbeidelse av sårbarhetsvurderinger ble utarbeidet mot slutten av 2016, men for alvor tatt i bruk vår/sommer 2017. Dette innebærer at det hittil finnes få sårbarhetsvurderinger utarbeidet etter nevnte mal, noe som har begrenset utvalget av enheter. Således har det også stilt enda større krav til anonymitet. Skulle en tilsvarende studie blitt gjort på et senere tidspunkt kan det være at en vil sitte på flere erfaringer for hvordan malen fungerer som et verktøy for dimensjonering av sikringstiltak.

Ekstern gyldighet omtales ofte som overførbarhet eller generalisering (Jacobsen, 2005). I praksis stiller en spørsmål om hvorvidt resultatene fra studien kan overføres til andre sammenhenger. Jacobsen (2005) fremhever at kvalitative studier i liten grad har som mål å kunne generaliseres, og er heller ikke egnet til dette. Hensikten er heller å skape en dypere

forståelse av et fenomen. Det en imidlertid kan oppnå er en teoretisk generalisering fra empiri til teori (Dey, 1993). Yang m.fl. (2014) påpeker at det til tross for mye forskning på både havnesikring og risikoanalyser, er få studier som ser på risikoanalysemetodikk opp mot havnesikring. Denne studien søker dermed å gi et bidrag til forståelse for hvordan en risikoanalysemetodikk for tilsiktede uønskede handlinger bidrar til de tiltakene som iverksettes, og hvilken rolle nåde nasjonalt og internasjonalt regelverk spiller inn.

3.6. Reliabilitet

Reliabilitet handler om hvorvidt vi kan stole på det innsamlede datamaterialet, altså resultatets pålitelighet (Jacobsen, 2005). Krumsvik (2014) skriver at reliabiliteten sier noe om hvordan en har kommet frem til de resultatene en presenterer. Jacobsen (2005) fremhever dette som viktig fordi selve undersøkelsen kan medføre at den eller de som undersøkes opptrer annerledes. I denne studien er den klare majoriteten av data innhentet fra eksisterende dokumenter. Dette gjør at jeg som undersøker ikke har hatt noen effekt på materialet som sådan. Likevel kan en argumentere for at jeg med mine forutsetninger har innvirkning på hvordan materialet fremstilles, benyttes og tolkes. Jacobsen (2005) mener at en trussel mot en studies troverdighet også kan komme fra uoppmerksomhet og slurv fra undersøkeren ved nedtegning av data. Jeg har derfor lagt vekt på i hovedsak å benytte åpne kilder og dokumenter som kan etterprøves. En kan også argumentere for at den store bruken av dokumenter, og mindre vekt på andre datakilder gir et svakere datagrunnlag. Dette har likevel fremstått som den mest hensiktsmessige metoden, av årsakene beskrevet i delkapitlet om datainnsamling. Selv om studien inneholder liten grad av triangulering (Jacobsen, 2005), har jeg forsøkt å legge stor vekt på åpenhet i metodebruken. Det kan også anses som en styrke at dokumenter kan gjennomgås i ettertid for å bekrefte empirien.

Hva gjelder deltakende observasjon kan en utvilsomt argumentere for at min tilstedeværelse har påvirket personell i havneanlegg. Det har derfor vært naturlig at observasjonene i denne sammenhengen vektlegges i mindre grad. Observasjonene som har blitt gjennomført under tilsyn jeg har deltatt på, har først og fremst gitt meg en oversikt over hvordan sikringstiltak gjennomføres i praksis. Tilsynene er ikke gjennomført for formålet med denne studien, men mine observasjoner har gitt meg et bilde av realiteten i havneanleggene.

3.7. Etikk

De etiske problemstillingene i denne studiens sammenheng dreier seg i hovedsak om to ting: For det første, at jeg som undersøker arbeider for en virksomhet som er en del av studien.

Dette er en utfordring som Jacobsen (2005) belyser når han skriver om etiske dilemma i forholdet mellom forsker og arbeidsgiver – såkalt oppdragsforskning. Her er det viktig for meg å understreke at min studie på ingen måte er et bestillingsverk fra, eller i regi av, Kystverket. Det er heller ikke Kystverket som har foreslått å studere temaet. Temaet i oppgaven kommer utelukkende av at jeg ser behovet, gjennom litteraturgjennomgangen for studier som omhandler sammenhengen mellom en risikoanalysemetodikk, tiltak og regelverk, og at jeg nå er i posisjon til å kunne gjennomføre nevnte studie.

For det andre er sårbarhetsvurderingene og sikringsplanene i havneanleggene unndratt offentlighet etter offentleglova § 24 tredje ledd, forskrift om sikring av havneanlegg § 13, og sikkerhetsloven. Dette har gjort det vanskelig å kommentere innhold i planverk og sikringstiltak. Studien inneholder derfor i få konkrete eksempler fra havneanleggene, men omtaler heller metoder og fellestrekk som ikke går på bekostning av skjermingsverdig informasjon. Data som innhentes fra foreliggende sårbarhetsvurderinger omtales derfor som betraktninger, og inneholder få karakteristikker fra havneanleggene. Ettersom at det ikke er gjennomført intervjuer eller observasjoner av enkeltmennesker i denne studien, tar jeg ikke stilling til de etiske aspektene ved denne typen undersøkelser.

4. Empiri

Innledningsvis vil det i kapitlet gis en oversikt over det gjeldende regelverket for havnesikring, internasjonalt og i Norge. Deretter gis en innføring i Norsk Standard (NS) 5830-serien med hovedvekt på NS 5832:2014 – Krav til sikringsrisikoanalyse. Dette er en serie utgitt av Standard Norge, om samfunnssikkerhet og beskyttelse mot tilsiktede uønskede handlinger. Videre vil Kystverkets mal for utarbeidelse av sårbarhetsvurderinger presenteres. Denne malen er utarbeidet for å gi en felles plattform for gjennomføring av sårbarhetsvurderinger for havneanlegg. Underveis vil også betraktninger fra foreliggende sårbarhetsvurderinger og sikringsplaner gi eksempler på hvordan malen blir operasjonalisert.

4.1. Regelverk for havnesikring

Selv om det i utgangspunktet er sårbarhetsvurderingen som skal være dimensjonerende for tiltakene en beslutter i sikringsplanen, har havnesikringsfeltet et regelverk som legger føringer for hvordan havneanleggene skal sikre seg. I det følgende gis en oversikt over gjeldende regelverk. Videre presenteres utdrag fra regelverket som omhandler sårbarhetsvurderinger og sikringsplaner. Regelverket som har direkte innvirkning på dimensjonering av sikringstiltak vil stå i hovedfokus. Kystverket har, fra Samferdselsdepartementet, fått ansvaret for gjennomføring av havnesikringsregelverket i alle norske havneanlegg som mottar skip i internasjonal fart.

Regelverket som norske havneanlegg må forholde seg til bygger på internasjonale regelverk fra FN og EU. EU-forordning 725/2004, som stiller krav til styrking av sikkerhet på skip og havneanlegg, er grunndokumentet i havnesikringsregelverket. Forordningen fremhever at maritim sektor i det europeiske fellesskap til enhver tid må sikres mot forsettlig ulovlige handlinger, som terrorangrep eller piratvirksomhet (Regulation (EC) No 725/2004). SOLAS-konvensjonen kapittel XI-2 og ISPS-koden er FN-regelverk og vedlegg til EU-forordningen. SOLAS XI-2 presenterer definisjoner, retningslinjer og krav for myndigheter, havneanlegg og skip, for å styrke maritim sikkerhet (IMO, 2017). I Norge gjennomføres EU-forordningen gjennom forskrift om sikring av havneanlegg (forskrift om sikring av havneanlegg, 2013). Forskriften stiller blant annet krav til at havneanleggene gjennomfører en sårbarhetsvurdering, en sikringsplan og at det utpekes en sikringsleder (Kystverket, 2016c). Det fremkommer også av forskriften hvilke deler av ISPS-koden som gjøres obligatorisk. ISPS-koden består av del A - obligatoriske krav, og del B - veiledning (IMO, 2003). I Norge er del A og deler av del B

gjort obligatorisk. Forskriftens §§ 9 og 10 omhandler henholdsvis sårbarhetsvurdering og sikringsplan for havneanlegg (forskrift om sikring av havneanlegg, 2013).

Forskrift om sikring av havneanlegg § 9. Sårbarhetsvurdering av havneanlegg

Paragraf 9 i forskriften er delt i fire ledd: «Med sårbarhetsvurdering menes en prosess for å identifisere og vurdere sårbarhet for infrastruktur og eiendeler som er viktig å beskytte, for deretter å fastsette de riktige sikringstiltak» (forskrift om sikring av havneanlegg, § 9 første ledd). Det første leddet tar sikte på å gi en kort forklaring på hva som menes med en sårbarhetsvurdering. «Det skal gjennomføres en sårbarhetsvurdering for hvert havneanlegg» (forskrift om sikring av havneanlegg, § 9 andre ledd). Ulike havneanlegg driver med ulike operasjoner. I tillegg kan lokale forhold ha innvirkning på risikoen. Derfor følger det av regelverket at hvert enkelt havneanlegg skal ha en egen sårbarhetsvurdering. «Sårbarhetsvurderingen kan gjennomføres av Kystverket eller godkjent sikringsvirksomhet. En sårbarhetsvurdering som er gjennomført av en godkjent sikringsvirksomhet skal godkjennes av Kystverket» (forskrift om sikring av havneanlegg, § 9 tredje ledd). I Norge er systemet lagt opp slik at godkjente sikringsvirksomheter (RSO) fungerer som konsulenter for havneanleggene, og gjennomfører sårbarhetsvurderinger på vegne av disse. Sårbarhetsvurderingene må godkjennes av Kystverket. «Sårbarhetsvurderingen skal minst tilfredsstille de krav som fremgår av ISPS-koden del A kapittel 15 og del B 15.3» (forskrift om sikring av havneanlegg, § 9 fjerde ledd).

ISPS-kodens del A kapittel 15 omhandler en del generell informasjon om sårbarhetsvurderinger. Del A 15.5 sier at en sårbarhetsvurdering som et minimum skal:

- Identifisere og evaluere viktige verdier og infrastruktur som er viktig å beskytte;
- Identifisere aktuelle trusler mot verdiene og infrastrukturen og muligheten for at disse inntreffer, for å kunne etablere og prioritere tiltak;
- Identifisere, velge og prioritere mottiltak og prosedyrer og deres effektivitet for å redusere sårbarhet; og
- Identifisere svakheter, inkludert menneskelige faktorer, i infrastruktur, retningslinjer og prosedyrer.

(IMO, 2003, s. 20).

Videre følger det av del B 15.3 at en sårbarhetsvurdering skal ta for seg fysisk sikkerhet, strukturell integritet, beskyttelse av personell, prosedyrer, radio og kommunikasjonssystemer, transportrelatert infrastruktur, verktøy, andre områder som kan utgjøre en risiko mot personer,

eiendeler eller operasjoner i havneanlegget, havnefartøy (los, slepebåter o.l.), sikrings- og overvåkningsutstyr samt tilgrensende sjøområder (IMO, 2003, s. 76). Det internasjonale regelverket legger altså føringer for hvilke momenter som skal inkluderes og vurderes i sårbarhetsvurderingen, men myndighetene i hvert enkelt land står fritt til å utforme sårbarhetsvurderingene innenfor de gitte rammene. En godkjent sårbarhetsvurdering er gyldig i 5 år (forskrift om sikring av havneanlegg, 2013).

Forskrift om sikring av havneanlegg § 10. Sikringsplan for havneanlegg

Forskriftens § 10 er delt inn i fem ledd: «Med sikringsplan menes en plan for gjennomføring av tiltak som skal beskytte havneanlegget og skip, personer, last, transportenheter og skipsforsyninger i havneanlegget mot risikoene ved en sikringshendelse.» (forskrift om sikring av havneanlegg, § 10 første ledd). Sikringsplanen er med dette det operative dokumentet som beskriver havneanleggets konkrete gjennomføring av sikringen. «På bakgrunn av en sårbarhetsvurdering skal det utarbeides en sikringsplan for hvert havneanlegg. Sikringsplanen skal utarbeides av havneanleggets sikringsleder eller godkjent sikringsvirksomhet, og skal godkjennes av Kystverket.» (forskrift om sikring av havneanlegg, § 10 andre ledd). Gjennomføringen av sikringsplanen skiller seg fra gjennomføringen av sårbarhetsvurderingen ved at det ikke er krav om bruk av godkjent sikringsvirksomhet (RSO). Sikringsplanen kan altså utarbeides av havneanleggets egen sikringsleder, men den skal baseres på den foreliggende sårbarhetsvurderingen.

Det følger av § 10 tredje ledd at «Sikringsplanen skal oppfylle de krav til innhold som fremgår av ISPS-koden del A 16.3 og del B 16.3 og 16.8. Relevante deler av ISPS-koden del B kapittel 16 skal følges i valg av sikringstiltak på de ulike sikringsnivå.» (forskrift om sikring av havneanlegg, § 10 tredje ledd). ISPS-koden stiller altså en del krav til sikringsplanen, og legger på den måten føringer for hvordan sikringen av havneanleggene skal ivaretas. Til sammen består del A 16.3, del B 16.3 og 16.8 av 35 punktvise krav til innholdet i sikringsplanen. Eksempler fra regelverket sier at sikringsplanen blant annet skal beskrive prosedyrer for; hvordan en hindrer innføring av våpen og farlig gods, hvordan en hindrer uautorisert adgang, evakuering, ansattes sikringsoppgaver, rapportering av sikringshendelser, informasjonssikkerhet og kommunikasjonssystemer, system for kontroll med gods, sikringsorganisasjonen, og opplæring i sikringsoppgaver.

Eksemplene over er et utdrag av kravene som stilles til innholdet i en sikringsplan. Selv om sårbarhetsvurderingen skal fungere som et grunnlag for sikringsplanen, står en altså ikke helt

fritt til å utforme sikringsplanen som en ønsker. Videre følger det av fjerde ledd at «Havneanleggets sikringsleder skal sørge for at sikringsplanen oppdateres kontinuerlig, og at oppdatert sikringsplan sendes til Kystverket.» (forskrift om sikring av havneanlegg, § 10 fjerde ledd). Dette understreker at sikringsplanen er et levende dokument som krever kontinuerlig oppdatering. Til slutt følger det av femte ledd at «Endringer i sikringsplanen skal godkjennes av Kystverket før de kan iverksettes dersom disse følger av endringer i sårbarhetsvurderingen, eller påvirker omfanget av sikringstiltakene.» (forskrift om sikring av havneanlegg, § 10 femte ledd). Kystverket skal dermed alltid være i besittelse av havneanleggets siste versjon av sikringsplanen.

4.2. Norsk Standard – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger

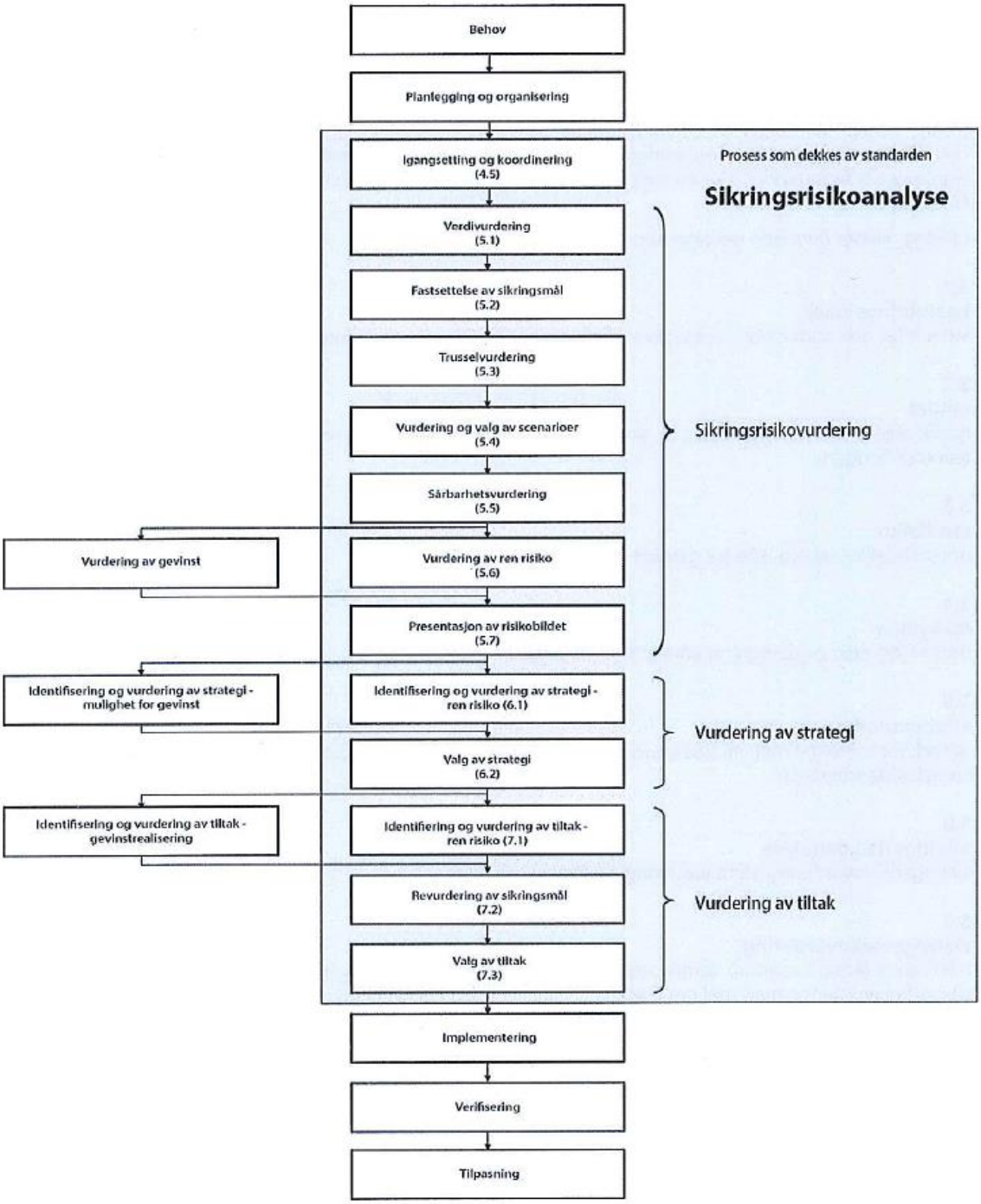
Standard Norge er Norges medlem i den internasjonale standardiseringsorganisasjonen International Organization for Standardization og europeiske European Committee for Standardization (Standard Norge, 2017a). Standard Norge utvikler standarder innenfor de fleste områder i samfunnet, blant annet for næringsliv, interesseorganisasjoner, forskningsinstitusjoner og myndigheter. Standard Norge er en privat og uavhengig medlemsorganisasjon som utvikler det de betegner som en felles «oppskrift» på hvordan noe skal gjennomføres (Standard Norge, 2017b). På nettsidene til Standard Norge (2017b) presiseres det at en standard er et forslag til valg av løsning. Standarder utvikles gjennom at en ser et behov for en standardisering, og at en har tilstrekkelig med ressurser. Videre må prosjektforslaget sendes til nasjonal vurdering og godkjenning før arbeidet med standarden begynner. Arbeidet gjøres av personer Standard Norge (2017b) definerer som eksperter på fagområdet.

I juli 2008 kom Norsk Standard (NS) 5814:2008 «Krav til risikovurderinger». Denne standarden orienteres mot «[...]å hindre eller forebygge uønskede hendelser og beskriver hvordan risikovurderinger passer inn i en bredere sammenheng som beslutningsstøtte for tiltak eller valg av løsninger.» (Standard Norge, 2008, s. 2). I standardens kapittel for risikoanalyse beskrives det at det skal gjøres en analyse av årsak og sannsynlighet. Dette innebærer at årsaker til uønskede hendelser først skal identifiseres, før en kommer frem til sannsynligheten eller frekvensen for uønskede hendelser.

I juni 2012 kom en ny standard, NS 5830, som omhandler beskyttelse mot tilsiktede uønskede handlinger. Standarden er utviklet av en komité hos Standard Norge som kalles «SN/K 296

Samfunnssikkerhet i BAE-sektoren». Standard Norge opplyser ikke hvem som sitter i komitéen, og det finnes heller ingen kildehenvisninger i standarden. Standarden rettes mot fagområdet «sikring» som standarden selv definerer som «Bruk av sikringstiltak ved håndtering av risiko forbundet med tilsiktede uønskede handlinger» (Standard Norge, 2012, s. 2). Standard Norge (2012) begrunner utgivelsen med at fagområdet ikke har hatt en gjennomarbeidet og samordnet terminologi, og at denne terminologien ikke har vært tilstrekkelig systematisert. NS 5830:2012 omtaler kun terminologi på fagfeltet. Videre kom det to nye standarder i november 2014, som bygger videre på NS 5830:2012. Disse heter NS 5831:2014 – Krav til sikringsrisikostyring og NS 5832:2014 – Krav til sikringsrisikoanalyse. Standard Norge har dermed nå tre utgivelser som omhandler samfunnssikkerhet og beskyttelse mot tilsiktede uønskede handlinger. Hovedforskjellen mellom NS 5814:2008 og den nyere NS 5830-serien er at sistnevnte utelukkende retter seg mot beskyttelse mot tilsiktede uønskede handlinger. I denne studien er det særlig NS 5832:2014 – Krav til sikringsrisikoanalyse som er interessant å undersøke nærmere.

Standarden NS 5814:2008 (s. 5) definerte risiko som et «Uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse». Den nye standarden bruker til sammenligning begrepet «sikringsrisiko», som de har valgt å definere som et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (Standard Norge, 2014, s. 4). Her kommer det frem at den nye standarden vurderer (sikrings-)risiko som en kontekst bestående av de tre elementene; trussel, verdi og sårbarhet. Disse tre elementene finnes også i standardens flytdiagram som illustrerer prosessen i en sikringsrisikoanalyse (figur 2). NS 5831:2014 beskriver at sikringsrisikoanalysen skal danne et beslutningsgrunnlag som gir et situasjonsbilde av risiko, og at analysen skal identifisere, bryte ned og vurdere alle relevante faktorer. Til slutt skal analysen vurdere strategier og tiltak for å håndtere den identifiserte risikoen. Nedenfor følger flytdiagrammet til Standard Norge (2014) som viser sammenhengen mellom de ulike trinnene i en sikringsrisikoanalyse.



Figur 2: Prosessen for sikringsrisikoanalyse og sikringsrisikostyring (Standard Norge, 2014, NS 5832, *s. 3).*

Før de ulike trinnene forklares, presiseres det at analysen må forankres hos beslutningstaker, at bakgrunnen for analyseresultatene skal dokumenteres, at usikkerhet knyttet til vurderinger skal beskrives, og at en må bruke kildehenvisninger. Det fremkommer også at målet med analysen skal beskrives. Dette innebærer at en må ha et klart mål med hvorfor en velger å gjennomføre en sikringsrisikoanalyse før en setter i gang med selve gjennomføringen.

Eierskap, ressurser og organisering må også defineres før selve analysen iverksettes. Standarden deler videre prosessen for sikringsrisikoanalyse i tre overordnede steg; sikringsrisikovurdering, vurdering av strategi og vurdering av tiltak. Fokuset i oppgaven vil være på stegene som dekkes av sikringsrisikoanalysen.

Sikringsrisikovurdering

Sikringsrisikovurderingen er det trinnet som er viet mest oppmerksomhet i standarden. Trinnet deles inn i 7 steg:

Verdivurdering (1) er steget der virksomheten, eller havneanlegget, skal kartlegge verdiene sine. Videre skal disse vurderes og rangeres. Verdivurderingen beskrives som det viktigste vurderingsgrunnlaget for analysen, og skal brukes for prioritering av ressurser i en sikringssammenheng. Dette innebærer at det er de verdiene som defineres i dette steget, og vurderingen av disse, som danner grunnlaget for hvilke trusler en vurderer og dermed hvilken beskyttelse verdiene krever. En kan også si at det er her en definerer hva en ønsker å oppnå med tiltakene sine. Verdier kan for eksempel være utstyr og infrastruktur som er viktige for havneanleggets operative evne. Det kan også være liv og helse, omdømme eller miljø.

I steget for *fastsettelse av sikringsmål (2)* skal det uttales et mål for hva som er ønsket eller akseptabel tilstand for virksomhetens verdier som følge av en uønsket hendelse. Her skal en definere mål for hva verdiene skal kunne tåle å utsettes for. Det understrekes at disse målene skal forankres hos eieren eller forvalteren av verdiene.

I neste steg skal virksomheten gjennomføre en *trusselvurdering (3).* Hensikten med denne vurderingen er ifølge standarden å identifisere og beskrive trusselaktører, deres intensjon, kapasitet og andre relevante faktorer. Mange antar nok at gjennomføring av trusselvurderinger er et ansvar som bare tillegges myndigheter. Både Nasjonal Sikkerhetsmyndighet (NSM), Politidirektoratet (POD) og Politiets Sikkerhetstjeneste (PST) oppfordrer likevel virksomheter til å gjennomføre egne trusselvurderinger, og fastslår at en kan finne mange tilgjengelige åpne kilder som kan bidra med relevant informasjon (NSM, POD og PST, 2015). I følge standarden kan en trusselvurdering ha to formål. Det ene knyttes til å identifisere aktørene og fremgangsmåten deres for å kunne dimensjonere beredskapstiltakene. Det andre formålet er at en skal varsle(s) tidlig slik at tiltak kan iverksettes før et angrep skjer. En kan altså dimensjonere sikringstiltakene sine ut fra hvilken trusselaktør en står ovenfor, og en kan iverksette disse og eventuelt ytterligere tiltak, dersom noe tyder på et forestående angrep.

Etter trusselvurderingen skal virksomheten gjennomføre en *vurdering og valg av scenarioer (4)*. Hensikten med dette steget er å utforske hvordan de identifiserte trusselaktørene kan gå frem for å ramme de identifiserte verdiene. Steget synes utfordrende fordi en kan se for seg et nesten ubegrenset antall scenarioer. Standarden bemerker at det bør utvikles et tilstrekkelig antall scenarioer for å belyse utfordringer, men også at et for stort antall kan føre til at analysen blir uoversiktlig og uhåndterlig. Standarden gir ingen føringer eller hjelpemidler for selve utarbeidelsen av scenarioene. Det er nærliggende å tro at en bør se til historikk for andre lignende aktører som har blitt utsatt for tilsiktede uønskede handlinger, og hvordan trusselaktører har gått fram i slike tilfeller. Det vil også være naturlig å vurdere hvor attraktiv verdiene til virksomheten er for trusselaktøren, for å kunne si noe om hvor langt trusselaktøren er villig til å gå for å ramme disse.

Videre skal virksomheten gjennomføre en *sårbarhetsvurdering (5)*. På bakgrunn av det en avdekker i verdi- og trusselvurderingen skal en vurdere i hvilken grad virksomhetens verdier er sårbare overfor de valgte scenarioer. I dette steget må det vurderes i hvilken grad det eksisterer tiltak som vil være i stand til å beskytte verdiene mot et angrep. På bakgrunn av vurderingen skal en kunne si noe om hvor sårbare verdiene er.

Neste steg i sikringsrisikovurderingen er *vurdering av ren risiko (6)*. Standarden definerer ren risiko som «potensialet for tap og ikke for gevinst» (Standard Norge, 2014, s. 4). Basert på informasjon om verdi, trussel og sårbarhet skal en her vurdere ren risiko for de ulike scenarioene. I dette trinnet skal også usikkerheten rundt de ulike delvurderingene og konklusjonen beskrives.

Sikringsrisikovurderingen avslutter med en *presentasjon av sikringsrisikobildet (7)*. Terminologistandarden NS 5830:2012 beskriver et risikobilde som en tidsavgrenset beskrivelse av risiko. Sikringsrisikobildet blir ikke definert i standarden, men en kan anta at hensikten er en tidsavgrenset beskrivelse av sikringsrisiko. Sikringsrisikobildet skal fungere som et beslutningsgrunnlag for videre sikringsrisikostyring hos virksomheten. NS 5832:2014 påpeker at en ved en helhetlig tilnærming også skal vurdere potensialet for gevinst.

Vurdering av strategi

På bakgrunn av sikringsrisikovurderingen, skal virksomheten gjennomføre en strategivurdering for håndteringen av den identifiserte sikringsrisikoen. Standarden trekker frem fire ulike strategier: Unngå risiko, overføre risiko, akseptere risiko og reduksjon/fjerning av risiko. Strategivurderingen skal beskrive de ulike alternativene og hvilke konsekvenser en

kan forvente ved valg av de ulike strategiene. Valg av strategi er et ansvar som tillegges beslutningstaker, for eksempel daglig leder, et styre eller en direktør. Strategivalget anses som en overordnet tilnærming til sikringsrisikohåndteringen.

Vurdering av tiltak

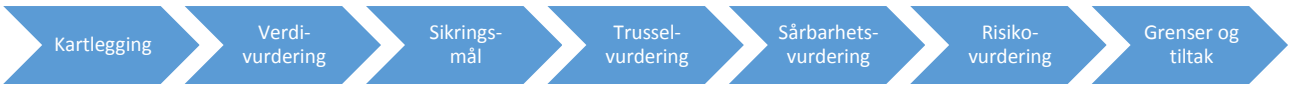
Den siste prosessen som gjennomføres i sikringsrisikoanalysen er prosessen for vurdering av tiltak. Først skal en identifisere og vurdere tiltak for håndtering av ren risiko. Vurderingen skal tilpasses virksomheten og forholdene som er avdekket tidligere i analysen. Vurderingen skal også ta for seg ulike muligheter ved valg eller utelukkelse av de ulike tiltakene. Kombinasjonen av flere tiltak skal også vurderes. Standarden bemerker at dersom en ønsker å redusere eller fjerne risikoen, bør tiltakene kombinere teknologiske, organisatoriske og menneskelige tiltak. Terminologistandarden omtaler teknologiske sikringstiltak som fysiske, elektroniske eller logiske siktingstiltak. Dette kan for eksempel være alarmsystemer på området som skal beskyttes, eller kryptering av viktige filer. Organisatoriske sikringstiltak omtales som tiltak som regulerer ledelse, organisering, prosesser, rutiner m.m. For eksempel kan en ha regelmessige møter i sikringsledelsen for å øke bevisstheten. Menneskelige tiltak omtales som tiltak som påvirker persepsjon, vurderingsevne, kunnskap og adferd til å kunne bruke andre tiltak. Her kan en for eksempel stille krav til opplæring hos vaktpersonell. En skal vurdere disse kategoriene av tiltak både mot forebyggende og skadereduserende effekter. Tiltaksvurderingen skal også inneholde en kostnadsvurdering som ser på hvor effektive sikringstiltakene er for oppnåelsen av sikringsmålene. Videre skal sikringsmålene for virksomheten revurderes. Også her skal en ta hensyn til gevinst og kostnader. På bakgrunn av disse vurderingene skal beslutningstaker fatte en avgjørelse om valg av tiltak.

Dersom en følger stegene som vist i figuren, skal en ende opp med et tilstrekkelig beslutningsgrunnlag for å velge strategi for risikohåndtering, og for å kunne iverksette tiltak. For at analysen skal fungere, stilles det likevel store krav til innsamling og vurdering av datamateriale. Særlig trusselvurderingen og valg av scenarioer synes utfordrende. Det finnes ingen fasit på hva som er riktig i disse stegene, men en synes å måtte inneha mye kunnskap om aktuelle aktører og deres karakteristikker for å kunne gjennomføre stegene på en adekvat måte.

4.3. Kystverkets mal for utarbeidelse av sårbarhetsvurderinger for havneanlegg

Kystverket er en nasjonal, statlig etat for kystforvaltning, sjøsikkerhet, og beredskap mot akutt forurensning, som ligger under Samferdselsdepartementet (Kystverket, 2017a). Etaten er delt

inn i fem regioner som utfører oppgaver på vegne av Kystdirektøren. En av oppgavene Kystverket har er å gjennomføre ISPS-koden og havnesikringsregelverket i norske havneanlegg som omfattes av regelverket. For at et havneanlegg skal godkjennes for å motta skip i internasjonal fart settes det blant annet krav gjennomføring av en sårbarhetsvurdering og en sikringsplan (forskrift om sikring av havneanlegg, 2013). Sårbarhetsvurderingen er det grunnleggende dokumentet for kartlegging av sikringsrisiko i havneanleggene, og det er denne som skal gi tilstrekkelig informasjon for dimensjonering av sikringstiltak. For å kunne gjennomføre sårbarhetsvurderinger på en hensiktsmessig måte, som tilfredsstiller kravene i regelverket, har Kystverket utarbeidet maler for utarbeidelse av disse. Den siste malen ble gitt ut i 2016. Malen baserer seg på stegene som vist i figuren under. I tillegg til malen ble det gitt ut en veileder kalt «Kystverkets veileder for utarbeidelse av sårbarhetsvurderinger for havneanlegg». Veilederen skal benyttes sammen med malen og gir ytterligere forklaringer. Hovedfokuset vil her være på selve malen.



Figur 3: Stegene i Kystverkets mal for utarbeidelse av sårbarhetsvurderinger (PFSA) for havneanlegg (Kystverket, 2016, s. 2).

På Kystverkets hjemmesider omtales sårbarhetsvurderingen som en sikringsrisikoanalyse. Likevel velger Kystverket å kalle dokumentet for en mal for utarbeidelse av sårbarhetsvurderinger. Kystverket sier selv at malen forsøker å inkludere analysetrinnene i NS 5832:2014, samtidig som den tar hensyn til regelverkets krav. Dette gjør den for eksempel gjennom å legge opp til vurderinger som er spesifikke for havneanlegg, som vurdering av farled, innseiling og kartlegging av skip-havn operasjoner. Det er krav om at sårbarhetsvurderingene gjennomføres av en godkjent sikringsvirksomhet (RSO) eller av Kystverket selv. Praksisen er likevel at sårbarhetsvurderinger gjennomføres av RSOer (Veiledning til forskrift om sikring av havneanlegg, Kystverket, 2013). RSOer må godkjennes av Kystverket, og gjennomfører sårbarhetsvurderinger på vegne av havneanlegget. Innledningsvis i sårbarhetsvurderingen skal RSOen gi en kort presentasjon av sentrale detaljer

som navn på havneanlegget, adresse, arbeidsgruppen for analysen og en presentasjon av virksomheten. Videre deles sårbarhetsvurderingen, som figuren illustrerer, inn i 7 steg.

I Norge er det pr. d.d. 9 godkjente RSOer (Kystverket, 2017b). Det er kun disse og Kystverket selv som har anledning til å gjennomføre en sårbarhetsvurdering for et havneanlegg. I skrivende stund foreligger det relativt få sårbarhetsvurderinger som er utarbeidet etter den nye malen. I det følgende gjøres det, av hensyn til anonymitet, i liten grad rede for karakteristikker ved havneanleggene betraktningene hentes fra. Planverket tilhører alt fra havneanlegg som skiper ut grus, ligger i grisgrendte strøk og har få årlige anløp, til havneanlegg i mer urbane strøk, som mottar cruiseskip og har mange anløp.

Trinn 1: Kartlegging

I kartleggingen skal analyseområdet defineres, og en skal sette inn tilstrekkelig antall kart over området. En skal kartlegge infrastruktur og beskrive nærliggende områder med tilhørende aktiviteter og bebyggelse. Videre skal skipsanløp og skipstyper kartlegges. En skal også beskrive organisasjonsmessige forhold, hvilke aktører som befinner seg i analyseområdet, antall personer og om det håndteres farlig last. Den største oppgaven i dette steget er imidlertid å kartlegge hvilke operasjoner som gjennomføres og hvilke verdier som finnes i havneanlegget. Her skal det gis en detaljert beskrivelse av hva som gjøres når et skip anløper, laster, losser og legger fra kai. Typiske verdier er lasthåndteringsutsyr, kjøretøy, kaier, oppstillingsplasser og nøkkelpersonell. Kystverket bruker terminologistandardens definisjon på en verdi som sier at en verdi er en «ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen» (Standard Norge, 2012, s. 4). En skal også si noe om havneanleggets eventuelle strategiske og samfunnsøkonomiske betydning.

Alle foreliggende sårbarhetsvurderinger starter med en generell kartlegging av havneanlegget. Her vurderes beliggenhet i forhold til tettbygde strøk, andre havneanlegg, industri og andre relevante forhold. Videre beskrives aktiviteten i havneanlegget, herunder antall anløp og hvor disse kommer fra og går videre til, type skip/last og operasjoner, eventuelle farlige stoffer og hvor mange personer som potensielt befinner seg i havneanlegget. Videre kartlegges alle verdier i havneanlegget. Virksomhetens strategiske betydning kommenteres også.

Trinn 2: Verdivurdering

Kystverket deler verdivurderingen i to deler. Først skal en vurdere havneanleggets strategiske verdier, herunder liv og helse, operativ evne og miljø. Videre skal havneanleggets taktiske og operasjonelle verdier vurderes. Veilederen til malen omtaler de strategiske verdiene som konsekvensområdene som de taktiske og operasjonelle verdiene skal vurderes opp mot. Taktiske verdier knyttes til organisering og ledelse, eksempelvis styringssystemer og informasjonssystemer. Operasjonelle verdier omtales som den enkelte bestanddel i et system, for eksempel konkrete eiendeler, infrastruktur og nøkkelpersoner. Det er konsekvensene knyttet til negativ påvirkning av verdiene som skal vurderes, og disse rangeres som ubetydelig, lav, moderat, høy eller svært høy. Konsekvensnivået skal begrunnes. Eksempelvis skal den operasjonelle verdien «kai» vurderes opp mot de strategiske verdiene liv og helse, operativ evne og miljø. Basert på disse vurderingene settes et samlet konsekvensnivå. Til slutt skal alle de vurderte verdiene oppsummeres i et verdibilde, som visualiserer den potensielle konsekvensen knyttet til den enkelte verdi.

Verdivurderingene fremstår ofte som veldig like hos havneanlegg med like operasjoner. Verdiene vurderes mot parameterne liv og helse, miljø og operativ evne. Hos havneanlegg som mottar cruiseskip vektlegges særlig verdier relatert til store folkemengder som viktig, og hos mindre havneanlegg som laster og losser grus vurderes selve kaiens operative betydning som viktig. Et fellestrekk hos de fleste havneanleggene er at utstyr som lett kan erstattes vurderes til mindre viktige. Eksempler på dette er trucker, lasteutstyr og datautstyr.

Trinn 3: Sikringsmål

Kystverkets mal bygger opp trinnet for sikringsmål i en tabell. Tabellen tar for seg funksjonsområde, krav til sikring etter ISPS-koden og virksomhetens sikringsmål (ytelseskrav). Eksempler på funksjonsområder er adgang, lasthåndtering og overvåkning. Videre stiller ISPS-koden konkrete krav til sikring, og under virksomhetens sikringsmål beskrives det hvordan virksomheten planlegger å oppfylle kravet. Et eksempel på et krav fra ISPS-koden er at havneanlegget skal hindre ulovlig adgang. Virksomheten kan da si at de ønsker å oppnå dette med blant annet en perimetersikring rundt området. Sikringsmålene i de ulike havneanleggene ser svært like ut. ISPS-koden stiller klare krav til sikring, og sårbarhetsvurderingene beskriver hvordan kravene oppfylles i havneanlegget. For eksempel

innfris kravet om å hindre ulovlig adgang svært ofte med et sikringsmål om perimetersikring og at uautorisert adgang skal oppdages innen få minutter.

Trinn 4: Trusselvurdering

I trusselvurderingen skal først relevante og potensielle trusselaktører listes opp. Kystverkets veileder til gjennomføring av sårbarhetsvurderinger viser til Forsvarsbygg (2016) sin Sikringshåndbok for hjelp til identifisering av trusselaktører. Forsvarsbygg deler trusselaktørene inn i kategoriene terrorisme, etterretning, sabotasje og kriminalitet. Videre deles hver trusselaktør inn i nivåene alfa, beta, charlie og delta, ut fra trusselaktørenes kapasiteter og alvorlighetsgrad. Alfa representerer de minst alvorlige, og delta representerer svært alvorlige og farlige trusselaktører. Neste steg i trusselvurderingen er å vurdere hvorvidt hver enkelt trusselaktør kan ramme havneanlegget. Aktørene vurderes på indikatorene tilstedeværelse, kapasitet, intensjon, historie og målvalg. I analysen skal det eksempelvis krysses av for om trusselaktøren har kapasitet til å ramme havneanleggets verdier. Alle vurderingene skal begrunnes. På bakgrunn av vurderingene settes et trusselnivå. Trusselnivået måles på skalaen ubetydelig, lav, moderat, høy og svært høy. Bakerst i malen finnes tabellbeskrivelser som sier hvilke indikatorer som skal til for å havne på de ulike nivåene. Det finnes også tabeller som sier noe om hva trusselnivået innebærer. Til slutt oppsummeres trusselaktørene i et trusselbilde for havneanlegget.

Trusselvurderingene i de foreliggende sårbarhetsvurderingene gjøres stort sett ved å henvise til åpne kilder, som for eksempel PSTs årlige trusselvurdering. I tillegg vises det nesten alltid til samtaler med lokalt politi. Ettersom konklusjonene som trekkes fra de nasjonale trusselbildene nesten alltid blir de samme, med unntak av små variasjoner ut fra havneanleggets operasjoner, faller det meste på de lokale trusselvurderingene. Også her er konklusjonene svært like: En kjenner ikke til at grupper eller enkeltpersoner har planer om å gjennomføre et angrep, men det kan heller ikke utelukkes. Den faktoren som oftest spiller inn på lokale trusselvurderinger er havneanleggets beliggenhet eller omfanget av virksomheten (antall anløp, antall passasjerer, størrelse mm.). Det synes dermed som at disse to faktorene, kombinert med hvilke operasjoner som gjennomføres, er de to mest avgjørende faktorene for konklusjonen i trusselvurderingene.

Trinn 5: Konsekvens og sårbarhetsvurdering

Innledningsvis i trinnet for konsekvens og sårbarhetsvurdering skal en utvikle trusselscenarioer. Her skal en beskrive ett eller flere tenkte scenarioer for hver trusselaktør. I

følge veilederen bør scenarioene ta utgangspunkt i motivasjonen hos trusselaktøren, attraktiviteten til havneanlegget og aktuell handlemåte (modus operandi) for trusselaktøren. Veilederen peker også på viktigheten av å ta hensyn til verdiene med høyest konsekvensnivå som ble kartlagt og vurdert i trinn 1 og 2. Det trekkes også frem at en bør inkludere andre forhold utenfor havneanlegget som kan påvirke sikringen, for eksempel dersom havneanlegget grenser mot et område hvor det lagres farlige stoffer. Malen sier ingenting om vurdering av usikkerhet knyttet til dette steget.

Like trusselvurderinger fra trinn 4 fører videre til at havneanlegg med like operasjoner, lik karakteristikk i beliggenhet og tilnærmet likt omfang, står med et svært likt utgangspunkt når en skal utvikle trusselscenarioer. Også disse ligner mye på hverandre. Trusselscenarioene beskrives som oftest med 1-3 setninger. Uavhengig av hvilken RSO som har gjennomført analysen, synes det som de samme trusselaktørene vurderes opp mot de samme scenarioene. Kriminelle personer og organisasjoner vurderes opp mot vinningskriminalitet, terrorister vurderes opp mot angrep som har til hensyn å ta mange liv, og psykisk ustabile personer vurderes ofte opp mot scenarioer med et ønske om å skade personer eller ramme virksomheten. Dette er i stor grad i henhold til Sikringshåndboka (Forsvarsbygg, 2016), men det synes nok en gang at vurderingene er tilnærmet like – nesten kun avhengig av operasjoner, omfang og beliggenhet. Hvis en ser til samtalene som gjennomføres med lokalt politi, kommer det sjeldent frem trusler her. Om dette skyldes at det ikke er spesielle, lokale forhold en må ta høyde for, eller at politiet holder kortene tett til brystet, er vanskelig å si noe om på bakgrunn av datagrunnlaget i denne studien.

Når trusselscenarioene er utarbeidet skal det gjøres en vurdering av konsekvens og sårbarhet. En skal vurdere hvordan trusselaktøren, gjennom det aktuelle trusselscenarioet, rammer de aktuelle verdiene. Her skal det vurderes konsekvens for operativ evne, liv og helse og miljø. På bakgrunn av konsekvensvurderingen settes et konsekvensnivå. Kystverkets mal sier ingenting om beskrivelse av usikkerhet knyttet til trusselscenarioene eller konsekvensnivået. Vurderingene som blir gjort i de foregående trinnene, legger premissene for konsekvensvurderingen. Konsekvensen skal vurderes for hvert scenario og fastsettes for liv og helse, operativ evne og miljø, og til slutt i en samlet konsekvens. Resultatet her avhenger av en kvalitativ vurdering, og hvorvidt den som gjennomfører analysen har vektlagt mulige konsekvenser eller foretatt en «worst case»-vurdering. Også her blir fellestrekkene mellom ulike sårbarhetsvurderinger like, avhengig av scenarioet. Konsekvenser for liv og helse ved

anløp av passasjerskip vurderes til høy/svært høy, og vurderes til lav ved anløp av grusbåter eller mindre fraktskip.

Videre skal virksomheten vurdere verdienes sårbarhet ovenfor scenarioene. Dette gjennomføres ved en kartlegging av eksisterende sikringstiltak. En må vurdere hvilke barrierer som eksisterer, og i hvilken grad disse er i stand til å forebygge eller forhindre negative konsekvenser. Kartleggingen skal resultere i et sårbarhetsnivå. Her brukes samme skala som tidligere, fra ubetydelig til svært høy. Sårbarheten avgjøres dermed av hvorvidt de eksisterende tiltak er i stand til å avverge eller begrense et trusselscenario. På bakgrunn av at havneanlegg med like operasjoner, omfang og beliggenhet ofte har relativt like sikringstiltak og vurderes opp mot like scenarioer, vurderes sårbarheten tilsvarende likt. Noen variasjoner forekommer naturlig på bakgrunn av lokale forhold og noe ulikhet i eksisterende sikringstiltak. Ofte ender sårbarhetsvurderingen opp med å si at den generelle sårbarheten er lav, men at den kan reduseres ytterligere ved å øke sikringsbevisstheten og gi mer opplæring til personell med sikringsoppgaver. Til slutt oppsummeres konsekvens og sårbarhet for de ulike scenarioene i en enkel tabell.

Trinn 6: Risikovurdering

Forankret i analysen av verdier, trusler og sårbarheter, skal dette trinnet si noe om ren risiko for hvert trusselscenario. Risikoen fastsettes etter en kvalitativ vurdering av de tre faktorene trussel, konsekvens og sårbarhet, på skalaen fra ubetydelig til svært høy. I malen spesifiseres det at en skal belyse usikkerheten knyttet til vurderingene, og hvordan dette kan påvirke risikoen. I vedlegget til malen finnes en tabell som utdyper hva de forskjellige nivåene på skalaen innebærer. Når risikoen er fastslått, skal det oppgis en strategi for håndteringen av risiko. Her skal det beskrives om risikoen kan unngås, aksepteres, overføres eller reduseres. Videre skal en vurdere eventuelle nye sikringstiltak og effekten av disse, før en til slutt anslår en ny risiko som følger av endret sårbarhet. Resultatene fremstilles i et nytt risikobilde gjennom opplisting av trusselscenarioene, identifisert risiko og ny risiko som følger av eventuelle tiltak. En skal også si noe om vurderingen av behov for visitasjon og gjennomsøking av personer, håndbagasje, bagasje, skipsforsyninger og gods. Dette gjøres gjennom en tabell der en skal angi frekvens for gjennomsøking på de tre ulike maritime sikringsnivåene.

Som et eksempel, ble det i en sårbarhetsvurdering utarbeidet et trusselscenario som beskrev et angrep mot et passasjerskip. I dette tilfellet ble trusselen satt til lav, konsekvens til svært høy,

og sårbarheten til lav. Samlet risiko ble i dette tilfellet vurdert til lav. Som et resultat ble risikohåndteringsstrategien satt til å videreføre gjeldende sikringstiltak, i tillegg til å øke sikringsbevisstheten, som igjen førte til uendret risiko for dette scenarioet. Noen havneanlegg ender opp med en lavere risiko som følge av nye tiltak, og andre ender opp med den samme risikoen. I eksemplet ovenfor endte havneanlegget opp med en uendret risiko, til tross for at nye tiltak ble vurdert som nødvendig. I en annen sårbarhetsvurdering kommer det frem at store folkeansamlinger i forbindelse med cruiseanløp er sårbare overfor potensielle angrep med kjøretøy. Under vurderingen av nye tiltak kommer det frem at det bør innføres fysiske barrierer som kan hindre slike angrep. Selv med dette tiltaket forble risikovurderingen uendret. Dette førte til at havneanlegget besluttet å iverksette en enklere form for mobile kjøretøysperrer, slik at de, til tross for uendret risiko, kunne redusere sårbarheten.

Det er oppsiktsvekkende få sårbarhetsvurderinger som omtaler eller vurderer usikkerhet. Gjennomgangen av foreliggende sårbarhetsvurderinger som er utarbeidet etter Kystverkets gjeldende mal, viser at under halvparten benytter seg av usikkerhetsbegrepet, til tross for at både standarden og malen sier at en må vurdere usikkerhet. Det synes å være en klar sammenheng mellom vurdering av usikkerhet, og hvilken RSO som har utarbeidet sårbarhetsvurderingen. Dette steget er likevel det første steget hvor Kystverket legger opp til vurdering av usikkerhet, noe som kan forklare hvorfor RSOene ikke gjør en kontinuerlig vurdering av denne faktoren.

Trinn 7: Grenser og tiltak

I det siste trinnet i Kystverkets mal for utarbeidelse av sårbarhetsvurderinger skal en fastsette de fysiske grensene og adgangsbegrensede områder i havneanlegget. Videre skal det gjøres en vurdering av om havneanlegget faller inn under forskrift om sikring av havner. Til slutt skal det utformes en tiltaksplan. Denne skal baseres på de nye tiltakene som ble identifisert i trinn 6. Det skal komme tydelig frem hvor tiltakene skal etableres, og om det er teknologiske, organisatoriske eller menneskelige tiltak.

Tiltakene som fastsettes gjennom en sikringsplan skal godkjennes av Kystverket før de iverksettes. I praksis er det dermed Kystverket som avgjør hvilke tiltak som kan regnes som tilstrekkelige i de ulike havneanleggene. Det er naturlig å anta at et havneanlegg med en avsides beliggenhet som bare anløpes av noen få grusbåter i året, kan ha mildere sikringstiltak enn havneanlegg i tettbygde strøk med flere titalls cruiseanløp. Dette kommer også frem i de faktiske sikringsplanene. Likevel synes det som de tre ovennevnte faktorene operasjoner,

omfang og beliggenhet er de avgjørende faktorene. To havneanlegg med likt operasjonsmønster, tilnærmet lik størrelse og like karakteristikker i beliggenhet ender ofte opp med å gjennomføre de samme sikringstiltakene.

Selv om sårbarhetsvurderingene må gjennomføres av en RSO, står sikringslederen i havneanlegget fritt til å lage sin egen sikringsplan. Sikringsplanen må uansett tilfredsstille kravene som stilles i ISPS-koden og forskrift om sikring av havneanlegg. Likevel viser interne data fra Kystverket at minst 90 % av havneanleggene velger å benytte seg av en RSO for gjennomføringen av sikringsplanen.

Oppsummering

Kapitlet har vist at § 9 i forskrift om sikring av havneanlegg stiller krav til hvem som skal gjennomføre sårbarhetsvurderinger, og hva denne skal inneholde. Det følger videre av forskriftens § 10 at det skal utarbeides en sikringsplan på bakgrunn av sårbarhetsvurderingen. Det følger også av denne bestemmelsen at sikringsplanen må oppfylle en rekke funksjonskrav som fremgår av ISPS-koden. Videre har gjennomgangen av NS 5832:2014 sin prosess for sikringsrisikoanalyse vist at metodikken fremstiller risiko på bakgrunn av verdiers sårbarhet overfor ulike trusselscenarioer. Til forskjell fra tradisjonelle risikoanalysemetoder, omtaler ikke standarden sannsynlighet i sin prosess. Standarden har heller ikke et eget steg for vurdering av usikkerhet, men påpeker innledningsvis, og i steget for risikovurdering, at usikkerhet må beskrives gjennom analysen. Usikkerhetsmomentet har blitt mindre vektlagt i Kystverkets (2016b) mal for gjennomføring av sårbarhetsvurderinger. Malen følger stegene i standarden, men legger kun opp til at usikkerhet skal vurderes i trinn 6, risikovurdering. I tillegg har det vist seg at mange RSOer avstår fra å beskrive og vurdere usikkerhet, selv i dette trinnet. Det har også vist seg at et havneanleggs beliggenhet, operasjoner, og omfanget av operasjonene er avgjørende for den samlede risikoen.

5. Drøfting

I det følgende vil de empiriske funnene drøftes opp mot studiens teoretiske rammeverk. Kapitlet struktureres etter forskningsspørsmålene, som vil bli drøftet underveis. Til slutt vil jeg sette sammen delkonklusjonene fra de tre forskningsspørsmålene for å svare på problemstillingen «*Hvordan fungerer sårbarhetsvurderinger som et hensiktsmessig verktøy for dimensjonering av sikringstiltak i norske ISPS-havneanlegg?*».

5.1. Norsk Standards risikoanalysemetodikk

Kan Norsk Standards metode anses som et hensiktsmessig verktøy for gjennomføring av risikoanalyser for tilsiktede uønskede handlinger?

Aven m.fl. (2004) sin definisjon har vist at planlegging krever en systematisk og faglig kunnskapsinnhenting og bearbeidelse av denne, før en kan fatte beslutninger og iverksette tiltak. Sett i lys av risikoanalyseprosessen (Aven m.fl., 2008), kreves det at en risikoanalyse planlegges og at en innhenter relevant informasjon, før denne vurderes og en beslutter tiltak for å håndtere risikoen. Det første forskningsspørsmålet rettes mot risikoanalyseprosessen, og tar sikte på å si noe om hva en risikoanalyse mot tilsiktede uønskede handlinger bør inneholde, og om Norsk Standards metode er vitenskapelig forankret. I det følgende vil jeg drøfte om NS 5832:2014 «Beskyttelse mot tilsiktede uønskede handlinger – krav til sikringsrisikoanalyse» kan anses som et hensiktsmessig verktøy for dimensjonering av sikringstiltak mot tilsiktede uønskede handlinger. Drøftingen til dette forskningsspørsmålet struktureres etter sikringsrisikoanalysens tre steg; sikringsrisikovurdering, vurdering av strategi og vurdering av tiltak.

Sikringsrisikovurdering

Perry og Lindell (2003) peker på at utgangspunktet for beredskapsplanleggingen er tilnærmet likt, uavhengig av om den uønskede hendelsen er uintendert eller intendert. Dette synes å stemme dersom en ser på de overordnede stegene i risikoanalyseprosessen til Aven m.fl. (2008) og NS 5832:2014. Både prosessen som beskrives av Aven m.fl. (2008) og NS 5832 har en egen fase for planlegging. I NS 5832 er dette trinnet ikke et steg i selve sikringsrisikoanalysen, men inngår likevel i det helhetlige arbeidet som må gjøres. Aven m.fl. (2008) trekker frem at en i planleggingsfasen må innhente relevant informasjon og velge hvordan en skal analysere informasjonen. Standardens tilnærming er noe annerledes på dette punktet. Den peker på at det skal utarbeides en plan for innhenting av informasjon, men prosessen videre bestemmer i stor grad hvilken informasjon som skal samles inn. Det kan

således synes som om informasjonsinnhentingen må gjøres på ulike måter, avhengig av om en ser på uintenderte hendelser, eller intenderte handlinger. For uintenderte hendelser kan det synes som det meste av informasjonen kan samles inn før risikovurderingen iverksettes, der en for intenderte handlinger i større grad må innhente ny informasjon til hvert steg, avhengig av hva en fant i det forrige.

Det første steget i standardens sikringsrisikoanalyse er å igangsette og koordinere arbeidet. Dette kan en finne igjen i planleggingsfasen til Aven m.fl. (2008). Selve analysearbeidet i standarden starter med den overordnede fasen, sikringsrisikovurdering. Det første som gjøres her er at virksomheten må identifisere verdiene sine. Verdier er noe vi finner igjen i Manuntas (1997) security-kontekst. Dette innebærer at en verdi bare eksisterer dersom det er noen som ønsker å beskytte denne. Også Williams (2013) har trukket frem at en må ha et referanseobjekt som en ønsker å beskytte. Standarden sier også at verdiene skal vurderes og rangeres. Dette innebærer at en må prioritere hvilke verdier en verdsetter høyest, for å finne ut hva som er viktigst å beskytte. Videre fastsettes sikringsmål etter hva som er ønsket eller akseptabel tilstand for verdiene. Standarden sier svært lite om dette steget, men det er nærliggende å anta en her må operasjonalisere ytelseskrav til verdiene, for å si noe om hvor stor påkjenning disse skal kunne utsettes for. Eksempelvis kan en si at den operasjonelle virksomheten til et havneanlegg skal kunne gjennomføres uten store forsinkelser, ved en økning til maritimt sikringsnivå 2. Hensikten synes å være at en setter et mål, slik at en senere kan identifisere og iverksette tiltak som gjør at en når målet.

Steget for trusselvurdering er også noe vi finner igjen i Manuntas (1997) security-kontekst. Standarden sier at en må identifisere og beskrive relevante trusselaktører før en kan gå videre i analysen. Dette kommer også frem fra Aven m.fl., (2008), som trekker frem at en vanskelig kan beskytte seg mot farer og trusler som en ikke har identifisert. I dette trinnet kommer det tydelig frem at en må basere seg på relevant og oppdatert kunnskap (Aven m.fl., 2004 og Perry og Lindell, 2003). Jore og Njå (2010) peker på at en må ta høyde for trusselaktørers intensjoner, kapasitet og effektene av eventuelle mottiltak. Dette har standarden klart å implementere i sine trinn for trusselvurdering og sårbarhetsvurdering. Ettersom trusselaktører og trusselbildet er i stadig endring, krever det at en gjennomfører en kontinuerlig informasjonsinnhenting. NSM, POD og PST (2015) viser til at en kan finne mye informasjon gjennom åpne kilder. Dette synes likevel å stille en del krav til den som gjennomfører analysen. Aven m.fl., (2008) har vist at det er vanlig å kopiere listen over trusselaktører fra tidligere analyser. Ulempen er at en da ikke baserer trusselvurderingen på de særegne

karakteristikkene til det enkelte havneanlegget. Etter mitt syn er dette en felle mange kan ha lett for å falle i. Trusselvurderingen fremstår som det mest krevende steget. En kan stille spørsmål ved hvor detaljerte en må være i identifiseringen, og når en har identifisert et tilstrekkelig antall trusselaktører. Holder det for eksempel å identfisere trusselaktøren «terrorist», eller bør en spesifisere om terroristen er høyre- eller venstreekstrem? Kanskje en til og med bør uttale konkret hvilken terrororganisasjon den potensielle aktøren stammer fra. Standarden fremmer likevel gode forslag til vurderingsparametere. Samtidig kan det være utfordrende for den som gjennomfører analysen å uttale seg om ulike aktørers intensjon og kapasitet til å ramme de identifiserte verdiene.

Basert på verdiene en ønsker å beskytte, og de potensielle trusselaktørene mot de nevnte verdiene, skal analysen utarbeide trusselscenarioer (Standard Norge, 2014). Scenarioer kan relateres til initierende hendelser, som Aven m.fl. (2008) har trukket frem som noe av det viktigste i en risikoanalyse. Standarden sier at scenarioene skal beskrive hvordan trusselaktørene kan gå frem for å ramme verdiene, og forutsetter således at en har kunnskap om aktørenes forventede handlingsmåter. Utarbeiding av scenarioer er noe en finner både i teorien og i standarden, men en får lite veiledning på hvordan dette bør gjøres. Det synes vanskelig å vite hvor detaljert en skal være når en konstruerer et tenkt angrep på verdiene sine. Videre, når en skal avdekke sårbarheter, kan det bli vanskelig å identifisere disse dersom scenarioene er uklare. På den andre siden kan for detaljerte scenarioer føre til en stor og uoversiktlig analyse. I tillegg er det ikke sikkert et reelt scenario vil utvikle seg på samme måte som risikoanalytikeren har tenkt. Sistnevnte forhold synes å avdekke et behov for også å beskrive usikkerhet knyttet til et scenarios utfall. Utformingen av selve scenarioet må ta høyde for trusselaktøren som forbindes med scenarioet. Dette innebærer at en trenger kunnskap om aktørens normale og potensielle handlingsmønster, som igjen kan være en vanskelig vurdering dersom en ikke har spesifisert dette grundig i det foregående trinnet.

Perry og Lindell (2003) påpeker at en må planlegge for en fleksibel respons. Dette er med å underbygge at scenarioer som er for detaljerte kan bli for mye rettet mot en bestemt respons, og dermed bør unngås. Det presiseres som en merknad i standarden at det er sentralt å beskrive denne typen usikkerhet gjennom analysen. Steget for vurdering og valg av scenarioer har klare fellestrekk med en årsaks- og konsekvensanalyse (Aven m.fl., 2008). Årsaksanalysen skal vise hva som skal til for at en hendelse inntreffer, og konsekvensanalysen sier noe om utfallet. Aven m.fl. (2008) sier at muligheten for at en hendelse inntreffer kan uttrykkes med sannsynlighet med basis i kunnskap. Standarden på sin

side bruker ikke sannsynlighet som et eget parameter når den snakker om hvorvidt det er trolig at scenarioene kan inntreffe. Det den derimot gjør er å oppfordre til å bruke kunnskap om trusselaktørene til å utarbeide scenarioene. På denne måten kan en argumentere for at en bruker en form for kunnskapsbasert sannsynlighet eller bayesiansk metode (Jore og Njå, 2010), selv om standarden ikke benytter seg av disse begrepene.

Trinnet for selve sårbarhetsvurderingen skal avdekke om verdiene er sårbare ovenfor trusselscenarioene som ble utarbeidet i forrige steg. Sårbarhet kan også relateres til det Manunta (1997) omtaler som «beskytter». I denne sammenheng kan verdien være forbundet med en sårbarhet som følge av en manglende beskytter. Dette kan føre til at verdien kan rammes av en trusselaktør. Hvis en ikke klarer å definere verdier, relevante trusler eller sårbarheter, har en heller ikke en sikringskontekst (Cohen og Felson, 1979 og Manunta, 1997). NOU 2000:24 sin definisjon sier at sårbarhet knyttes opp mot mulig tap av verdier. Dette er med på å underbygge rekkefølgen til stegene i standarden, ved at en må kartlegge verdier før en kan vurdere og uttale seg om sårbarhet. En styrke med standardens tilnærming er at det også påpekes at en må rangere verdiene sine. Dette gjør det lettere for den som skal fatte beslutninger, å prioritere hvor en må sette inn ressurser.

I det neste steget følger det av standarden at virksomheten skal vurdere «ren risiko» for hvert scenario. Ut fra standardens definisjon skal en dermed vurdere potensialet for tap, og ikke for gevinst. På dette steget presiseres det i standarden at også usikkerheten skal beskrives. Aven m.fl. (2004) sin definisjon av risiko omhandler også kombinasjonen av usikkerhet og konsekvensen av en aktivitet. Definisjonene innebefatter således de samme faktorene, men standarden presiserer at det som undersøkes her er potensialet for tap, og ikke mulige gevinster ved risikoen. Selv om det fortsatt dreier seg om risiko med hensyn på verdier, trusler og sårbarhet, bruker ikke standarden begrepet sikringsrisiko, som kanskje hadde vært mer naturlig i og med at den innfører dette begrepet innledningsvis. Steget for vurdering av ren risiko synes å være en logisk måte å sammenfatte vurderingene som er gjort i de tidligere stegene, og fraviker heller ikke nevneverdig fra det foreliggende teoretiske rammeverket. Konklusjonene fra stegene i risikovurderingen skal presenteres i et risikobilde (NS 5832:2014). Dette kommer også frem fra både Aven m.fl. (2008) og Jore og Moen (2010). I standarden vises det til at dersom risikobildet skal visualiseres, må en ivareta både verdi, trussel og sårbarhet, men det gis ingen føringer for hvordan en kan presentere dette visuelt. Etter mitt syn kunne standarden med fordel ha illustrert et eksempel på hvordan dette kan

visualiseres. Et godt visualisert risikobilde kunne forenklet kommunikasjonen av virksomhetens risiko.

Vurdering av strategi

Innholdet i dette steget samsvarer med Aven m.fl. (2008) sin definisjon av risikohåndtering. En skal her velge den overordnede tilnærmingen til hvordan en ønsker å håndtere risikoen. Risiko er en vurdering, og ikke fakta (Jore og Njå, 2010). Derfor må virksomheter selv kunne vurdere hvilken risiko som kan aksepteres. Dersom en ønsker å redusere risiko, tar en risikoen videre til neste steg, vurdering av tiltak. Til tross for at forskjellige vurderinger ligger til grunn, er det ikke noe som tilsier at dette steget bør gjennomføres ulikt for uintenderte og intenderte hendelser. Det kan likevel, på bakgrunn av risikoens natur, være slik at en ender opp med ulike strategier.

Vurdering av tiltak

I dette steget skal det ifølge standarden velges tilpassede tiltak. I vurderingen skal det tas hensyn til muligheter og konsekvenser ved å velge eller utelukke de ulike tiltakene. Perry og Lindell (2003) har også pekt på at det er viktig å tilpasse tiltakene sine til virksomheten. Både Reason (1997), Aven m.fl. (2008) og Rausand og Utne (2009) viser til at tiltak enten kan være sannsynlighetsreduserende, eller konsekvensreduserende. Standarden bruker begrepene forebyggende og skadereduserende, som i praksis betyr det samme. Likevel synes standardens begreper å være vel så hensiktsmessige i en sikringssammenheng, da en kan argumentere for at det er vanskelig å redusere sannsynligheten for at en aktør ønsker å ramme en virksomhet. Sett fra en annen vinkel kan en med synlige tiltak gjøre seg til et mindre attraktivt mål. En kan dermed si at tiltaket både er sannsynlighetsreduserende og forebyggende. Standarden gir ikke noe fasitsvar på hvordan en beslutter hvilke tiltak en skal innføre, men påpeker at det er viktig at en ivaretar hensynet på kostnader, effekt og sikringsmålene. Dette er også faktorer en kan finne igjen i vurderingsprosessen for tiltak (Aven m.fl., 2008).

Delkonklusjon forskningsspørsmål 1

Framgangsmåten for å finne svaret på forskningsspørsmål 1 har vært å gjennomføre en systematisk gjennomgang av analyseprosessen i NS 5832:2014, og vurdere stegene opp mot foreliggende teori. Perry og Lindell (2003) har vist til at utgangspunktet for beredskapsplanleggingen vil være tilnærmet lik for både tilsiktede og utilsiktede hendelser. Etter mitt syn er utgangspunktet svært likt, men er nødt til å gjøre noen ulike vurderinger

underveis i prosessen. Den største forskjellen mellom standarden og tradisjonelle tilnærminger til risikoanalyser, er at standarden unnlater å buke sannsynlighetsbegrepet. Fordelen med dette er at frekvensbasert sannsynlighet er vanskelig å vurdere for tilsiktede uønskede handlinger (Kujawski og Miller, 2007, Brown og Cox Jr., 2010). Ulempen synes derimot å være at personer uten omfattende kompetanse på risikofaget kan ha lett for å avvise scenarioer som urealistiske dersom en ikke uttaler seg om sannsynlighet. En løsning kunne vært å benyttet seg av en kunnskapsbasert eller bayesiansk tilnærming (Aven, 2013 og Jore og Njå, 2010), på samme måte som PST (2017). Til tross for at sannsynlighetsbegrepet er unnlatt fra analysen, gir stegene for trusselvurdering og vurdering og valg av scenarioer, etter mitt syn, tilstrekkelig med informasjon til at standarden fremstår som et logisk og hensiktsmessig verktøy for gjennomføring av risikoanalyser for tilsiktede uønskede handlinger. En forutsetning er likevel at den eller de som gjennomfører analysen har tilstrekkelig med kompetanse til å gjennomføre krevende vurderinger.

5.2. Kystverkets tilnærming

Hvordan gjennomføres og utformes sårbarhetsvurderinger for norske ISPS-havneanlegg?

I Kystverkets veileder til malen for utarbeidelse av sårbarhetsvurderinger (PFSA) for havneanlegg, beskrives det at malen er basert på analysetrinnene i NS 5232:2014. I forrige delkapittel ble det konkludert med at denne metodikken fremstår som hensiktsmessig for tilsiktede uønskede handlinger, men at den stiller store krav til analytikeren. I det følgende vil jeg diskutere hvorvidt Kystverkets mal lykkes med å implementere analysetrinnene, og hvordan malens steg kan relateres til det teoretiske rammeverket. I tillegg vil jeg se nærmere på om denne fremgangsmåten synes hensiktsmessig for havnesikring, med hensyn til kravene som stilles fra ISPS-koden og forskrift om sikring av havneanlegg.

Kystverkets mal for gjennomføring av sårbarhetsvurderinger for havneanlegg er bygget opp etter de 7 stegene kartlegging, verdivurdering, sikringsmål, trusselvurdering, sårbarhetsvurdering, risikovurdering, og grenser og tiltak. De fleste av disse stegene finner vi igjen i standardens fremgangsmåte. Før de 7 stegene presenteres i malen, legges det opp til at det skal beskrives hvem som har deltatt i arbeidet, og hvilke sentrale møter som er avholdt. Dette finner en igjen i standardens trinn for planlegging og organisering, som gjennomføres før selve analysen iverksettes. Steget «grenser og tiltak» kan delvis spores direkte til standarden, men er også spesifikt tilpasset havnesikring. Slike tilpasninger er forøvrig også gjort i de andre stegene, og synes nødvendig for å tilfredsstille kravene i regelverket.

Regelverket stiller blant annet krav til at sårbarhetsvurderinger oppdateres ved endringer i havneanleggene, og minimum hvert femte år (forskrift om sikring av havneanlegg, 2013). Således kan en argumentere for at planleggingen ivaretas som en kontinuerlig prosess (Quarantelli, 1977 og Perry og Lindell, 2003).

Verken standarden eller Kystverkets mal har et eget steg rettet mot usikkerhet. Begge påpeker likevel under steget for «vurdering av ren risiko» (standarden) og «risikovurdering» (Kystverkets mal) at usikkerheten skal beskrives. En kan argumentere for at usikkerhetsmomentet kunne vært tyngre vektlagt i begge tilnærmingene, som følge av den store usikkerheten som knyttes til risikovurderinger (Aven m.fl., 2008, Dillon m.fl., 2009 og Yoe, 2012). Grunnet den kvalitative tilnærmingen i analysen, vil det uansett dreie seg om en beskrivelse og vurdering av risiko. En kan således argumentere for at belysningen av usikkerhet likevel er tilstrekkelig, gitt at analytikeren vektlegger en grundig beskrivelse av denne faktoren. Det har imidlertid vist seg at flere RSOer unnlater å beskrive og vurdere usikkerhet i analysen. Når flere RSOer velger å unnlate slike vurderinger, kan en stille spørsmål om Kystverket har vært tydelig nok på at slike vurderinger skal gjennomføres. Kystverkets mal sier for eksempel ingenting om vurdering og beskrivelse av usikkerhet i innledningen, noe standarden gjør. Samtidig finnes det også RSOer som vurderer usikkerhet, og dette viser at noen har klart å fange opp at vurdering av usikkerhet er viktig. En kunnskapsbasert sannsynlighetstilnærming kunne vært en del av løsningen, da denne ivaretar usikkerhetsmomentet knyttet til vurderingene (Busmundrud m.fl., 2015).

Den mest synlige forskjellen på Kystverkets mal og standarden, synes å være navnet på prosessen. Standarden er nøye med å kalle prosessen for en sikringsrisikoanalyse. Kystverket har derimot valgt å kalle prosessen for en sårbarhetsvurdering. Sårbarhetsvurderingen er i standarden beskrevet som en del av den helhetlige analysen, og en kan dermed argumentere for at Kystverket også burde kalt sin prosess for en sikringsrisikoanalyse. Også Aven m.fl., (2008) legger frem sårbarhetsvurderinger som en del av den helhetlige risikoanalyseprosessen. Årsaken til Kystverkets navnevalg på prosessen, synes å stamme fra forskrift om sikring av havneanlegg (2013), som stiller krav til at havneanleggene gjennomfører en «sårbarhetsvurdering». ISPS-koden kaller dokumentet for en «Port facility security assessment», og samsvarer således bedre med standarden, enn det den norske forskriften gjør. Det er lite trolig at dette har noen innvirkning på utfallet av analysen, men etter mitt syn ville det vært mer hensiktsmessig for Kystverket å kalle prosessen for en sikringsrisikoanalyse.

Det følger av forskrift om sikring av havneanlegg at sårbarhetsvurderingen skal gjennomføres av Kystverket eller en godkjent sikringsvirksomhet (Forskrift om sikring av havneanlegg, 2013). I Norge er likevel hovedregelen at RSOer gjennomfører sårbarhetsvurderingene (Kystverket, 2013, Veiledning til forskrift om sikring av havneanlegg). Veilederen til Kystverkets mal presiserer at utarbeidelsen av sårbarhetsvurderingen skal gjennomføres i tett samarbeid med havneanlegget. Dette fremheves også av førsteamanuensis ved UiS, Sissel Jore (Busmundrud m.fl., 2015). Jore mener at det er viktig at en virksomhet selv skal ha eierskap til både risikoanalyseprosessen og resultatene i ettertid. Basert på datagrunnlaget i denne studien er det er vanskelig å uttale seg om i hvilken grad havneanleggene blir inkludert i prosessen med utarbeidelsen av sårbarhetsvurderingene, men dette er noe en bør være oppmerksom på. Dersom havneanleggene ikke involveres, kan en risikere å gå glipp av sentral informasjon om havneanlegget og det nærliggende området. Det er likevel ting som kan tyde på at havneanleggene ikke er så involverte i prosessen som de skulle vært. Det tydeligste signalet på dette er at både resultatene fra ulike analyser, og utformingen av sikringstiltak ofte blir svært like for forskjellige havneanlegg. Dersom havneanleggene hadde vært ytterligere involvert i prosessen med gjennomføringen av sårbarhetsvurderinger og sikringsplaner, kunne en forventet en større variasjon av sikringstiltak i havneanleggene.

Empirien har vist at regelverket legger føringer for hva som må inkluderes i analysen. Disse føringene fremstår som et godt hjelpemiddel, og en påminnelse for hva som må vurderes. Betraktningene fra foreliggende sårbarhetsvurderinger har vist at mange sårbarhetsvurderinger fremstår som like. Særlig dersom havneanleggene har tilnærmet like operasjoner, omfang og beliggenhet. Dersom det er flere havneanlegg som driver utskipning av grus, med en beliggenhet langt fra folk, synes det også naturlig at disse setter seg relativt like sikringsmål, og at de dermed ender opp med en tilnærmet lik trusselvurdering. Det samme gjelder for havneanlegg som driver med cruisevirksomhet. En har ofte de samme verdiene en ønsker å beskytte, som igjen fører til like sikringsmål og en lik trusselvurdering. Aven m.fl. (2008) har trukket frem viktigheten av å involvere eksperter med kunnskap om truslene en har identifisert. Mange RSOer involverer således lokalt politi, men med tilsynelatende varierende resultat. Det kan derfor til tider virke som en vet resultatet av analysen allerede etter verdiene er kartlagt i trinn 1. Yoe (2012) viser til at en risikovurdering aldri bør være designet slik at den støtter et allerede gitt resultat. Således synes det sentralt å stille krav til at RSOene må klare å skille mellom lokale forskjeller, i tillegg til å planlegge for en fleksibel respons som tar høyde for ulike scenarioer (Staupe-Delgado og Kruke, 2017).

Samtidig er det ikke slik at analysene nødvendigvis er feil selv om de er like, men dersom dette er tilfellet bør Kystverket vurdere å se etter løsninger som sikrer at RSOer ikke bare kopierer inn resultater fra analyser med tilnærmet like operasjonsmønster, omfang og beliggenhet – samtidig som en eventuell løsning må ivareta kravene fra regelverket.

Etter forskrift om sikring av havneanlegg § 9, stilles det konkrete krav til hva som skal vurderes i sårbarhetsvurderingen. Disse kravene fungerer etter mitt syn som gode retningslinjer til hva en må huske å vurdere. Kravene synes heller ikke å være utslagsgivende for hvilke tiltak en ender opp med. I forskriftens § 10 stilles derimot konkrete krav til hvordan et havneanlegg skal sikres. For eksempel skal havneanlegg hindre innføring av ulovlig last og uautorisert adgang, og en skal beskrive hvordan sikringshendelser skal rapporteres. Dette er krav som synes fornuftige, men som overlater heller lite til analysen for øvrig. En kan argumentere for at det er begrenset med tiltak som gjør at et havneanlegg tilfredsstiller disse kravene i regelverket. Dette fører igjen til at det er legitimt å stille spørsmål rundt formålet med en omfattende analyse. Formålet til analysen synes med bakgrunn i dette å være at en må finne ut hvilket nivå en skal dimensjonere sikringen etter. Dette kan for eksempel innebære å avdekke om det er tilstrekkelig med et skilt som opplyser om at et område er adgangsbegrenset, eller om en fysisk må sikre området med høye gjerder. Således kommer analysen til sin rett der en er i tvil om hvordan en skal dimensjonere sikringen. I mange tilfeller, basert på de tidligere diskuterte parameterne operasjoner, omfang og beliggenhet, synes det likevel noe innlysende hvordan en skal dimensjonere tiltakene. Derfor er det igjen viktig at havneanleggene selv deltar i prosessen, slik at de får fremmet sine synspunkter på hvilke tiltak som er nødvendige (Yoe, 2012).

Delkonklusjon forskningsspørsmål 2

Kystverkets mal lykkes godt med å operasjonalisere NS 5832:2014. Den største forskjellen har vist seg å være at Kystverket omtaler analysen for havneanlegg som en sårbarhetsvurdering. Det ville etter mitt syn vært bedre å omtale prosessen som en sikringsrisikoanalyse, på samme måte som i standarden. Også Aven m.fl. (2008) omtaler analysen av sårbarhet som en del av risikoanalysen. Videre har det har vist seg å være utfordrende å gjennomføre gode trusselvurderinger, og således også å utarbeide relevante scenarioer. Kombineres denne utfordringen med at det allerede foreligger klare krav til sikring i regelverket, blir det tydelig at den som gjennomfører sårbarhetsvurderingen må ha høy kompetanse på området for å klare å få frem nyansene som skiller ulike havneanlegg. På bakgrunn av hvordan sårbarhetsvurderinger gjennomføres i dag, kan det synes som

Kystverket og RSOene har et forbedringspotensiale når det gjelder å unngå at resultater er gitt, før sårbarhetsvurderingen er gjennomført. Kystverket kan også med fordel tydeliggjøre viktigheten av å beskrive og vurdere usikkerhet, både med hensyn på trusselaktører, scenarioer, konsekvensvurderinger og risikovurderinger.

5.3. Sårbarhet, risikobilde og tiltak

Hvordan bidrar en analyse av sårbarhet til å fremstille et risikobilde for havneanleggene, og hvordan brukes dette til utforming av tiltak?

Ettersom forskrift om sikring av havneanlegg og Kystverket omtaler analysen som en sårbarhetsvurdering, synes det naturlig å undersøke hvordan en avdekking og vurdering av sårbarhet virker på risikobildet. Videre er det også interessant å diskutere hvorvidt tiltak som besluttes, kan spores tilbake til analysen. Som tidligere påpekt er det ikke noe poeng i å gjennomføre en risikoanalyse dersom målet er å støtte et allerede gitt svar (Yoe, 2012). Dette forskningsspørsmålet tar sikte på å undersøke hvordan sårbarhetsanalysen er med på å utforme et risikobilde for havneanleggene. Risikobildet presenterer risikoresultatene for et havneanlegg, og danner beslutningsgrunnlaget for hvilke(n) risikohåndteringsstrategi(er) og -tiltak som kommer frem av havneanleggets sikringsplan (Aven m.fl., 2008).

Risikoen for hvert trusselscenario utgjør summen av nivået som tidligere har blitt satt for trussel, konsekvens og sårbarhet. Risikonivået skal begrunnes, og det skal fastsettes en risikohåndteringsstrategi. Videre skal det gjennomføres en vurdering av nye sikringstiltak for å håndtere risikoen. Risikobildet utgjør avslutningen på *trinn 6 – risikovurdering*, i Kystverkets mal for utarbeidelse av sårbarhetsvurderinger (PFSA) for havneanlegg. Malen legger opp til at risikobildet skal illustrere identifisert risiko for hvert trusselscenario, og ny risiko som følger av risikohåndteringsstrategien og vurderingen av nye sikringstiltak. Sårbarhetsvurderingen er én av tre faktorer som vurderes når risikoen fastsettes. Malen sier ingenting om hvordan disse tre faktorene skal vektlegges, men presiserer at fastsettingen av risiko er en egen vurdering. Jore og Njå (2010) presiserer også at risiko ikke er ren fakta, men en vurdering som gjøres. Dette gir rom for at den som gjennomfører analysen selv kan fastsette et fornuftig risikonivå. Skalaen er her den samme som tidligere; ubetydelig, lav, moderat, høy og svært høy. Selv om to av faktorene eksempelvis gis verdien ubetydelig, og den tredje moderat, er det altså ikke gitt hva det samlede risikonivået blir. Det viktigste er at risikonivået begrunnes, slik at brukeren av analysen finner nivået fornuftig.

Aven m.fl. (2008) sier at risikobildet dannes på bakgrunn av årsaks- og konsekvensanalyser. Kystverket gjennomfører ikke årsaksanalyser som sådan, men oppnår likevel mye av det samme gjennom kartlegging, prioritering og vurdering av verdier, gjennomføring av trusselvurderinger og utforming av trusselscenarioer. I disse stegene beskrives verdiene en vil beskytte, hvem som potensielt kan ramme disse verdiene og hvordan dette kan forekomme. En legger således opp til å beskrive hva som må ligge til rette for at trusselscenarioene kan inntreffe. Dessuten synes det utfordrende å gjennomføre en mer konkret årsaksanalyse når trusselen består av tenkende aktører i stadig tilpasning (Brown og Cox Jr., 2010). Kystverket legger også opp til at en skal vurdere hvordan verdiene blir rammet ved å gjennomføre konsekvensvurderinger for hvert scenario. Videre skal analysen si noe om hvorvidt havneanleggets verdier er sårbare ovenfor trusselscenarioene. Aven m.fl. (2008) sin definisjon av sårbarhet peker på kombinasjonen av mulige konsekvenser og usikkerhet knyttet mot trusselscenarioer. Dette innebærer ifølge Aven m.fl. (2008) at en må ha informasjon om både konsekvenser og usikkerhet før en kan fastsette et nivå for sårbarhet. Verken malen eller veilederen fra Kystverket omtaler usikkerhet i analysen, før trinn 6 – risikovurdering. Dette støtter funnene som er gjort tidligere i denne studien om at vurderinger av usikkerhet burde komme tydeligere frem. Det presiseres under steget for risikovurdering at en skal belyse usikkerheten i vurderingene for trussel, konsekvens og sårbarhet, men etter mitt syn burde dette kommet frem tidligere. Likevel skal en i henhold til malen ha vurdert både trussel, konsekvens, sårbarhet og usikkerhet før en presenterer havneanleggets helhetlige risikobilde. Således kan en argumentere for at Kystverket har fått med seg de viktigste momentene som utgjør et tilstrekkelig risikobilde.

Videre er det interessant å diskutere hvordan risikobildet spiller inn når det skal besluttes hvordan en ønsker å håndtere risikoen. Aven m.fl. (2008) sin definisjon av risikohåndtering tar for seg både strategier for å unngå, redusere, optimalisere og overføre risiko, i tillegg til virkemidler for å modifisere risiko. En kan argumentere for at all virksomhet knyttes til en form for risiko, og på et tidspunkt må en kunne akseptere restrisikoen. Havneanlegg som skal godkjennes under ISPS-koden må som et minimum oppfylle blant annet de kravene som fremkommer av forskrift om sikring av havneanlegg § 10. Denne bestemmelsen synes å legge klare føringer for hva havneanlegget skal oppnå med sikringen. Likevel synes det sentralt å utarbeide en sikringsplan som tar hensyn til havneanleggets karakteristikker, og som dimensjonerer sikringen på et fornuftig nivå basert på risikobildet. For at sikringen på en hensiktsmessig måte skal tilpasses havneanlegget, er det sentralt at personer med kjennskap til

havneanlegget deltar i utformingen av sikringsplanen. Dette kommer også frem av Yoe (2012), som fremhever at selve risikovurderingsprosessen er like viktig som resultatet. Dersom en deltar i prosessen vil en tilegne seg en bedre forståelse for havneanleggets risiko og sikringstiltakene som gjennomføres. Derfor synes det noe overraskende at omkring 90 % av havneanleggene velger å benytte seg av en RSO ved utarbeidelse av sikringsplanen. Dette i seg selv betyr ikke nødvendigvis at personell fra havneanleggene ikke deltar i prosessen, men tatt i betraktning at tiltakene tidvis synes standardiserte, kan det være en pekepinn på at havneanleggene bør involveres ytterligere.

Betraktningene som er gjort fra foreliggende sårbarhetsvurderinger og sikringsplaner, stammer både fra havneanlegg som ligger langt fra befolkning og som opererer med utskipning av grus, og havneanlegg plassert midt i større byer som betjener store cruiseskip. Noen ender opp med et risikobilde som klarer å redusere risiko ved hjelp av nye tiltak, og andre ender opp med den samme risikoen. I de sistnevnte tilfeller synes resultatet å henge sammen med at risikoen var vurdert til lav eller ubetydelig i utgangspunktet. I ett tilfelle konkluderes det med at store folkemengder kan samles på et åpent område, og således er sårbare for eventuelle angrep. Sårbarhetsvurderingen anbefaler i dette tilfellet at det settes opp fysiske sperrer for å hindre at kjøretøy kan brukes som våpen mot store ansamlinger av passasjerer. Likevel forblir risikoen uendret i risikobildet. I dette tilfellet valgte havneanlegget å innføre en rimeligere variant av fysiske barrierer, som i stor grad likevel kan oppfylle formålet. Dette er et tydelig eksempel på at sårbarhetsvurderingen kan være dimensjonerende for tiltak som implementeres. På den andre siden er tiltak mot denne typen hendelser noe en bør kunne forvente å finne i de fleste nyere planverk for havneanlegg som betjener store mengder av passasjerer.

I og med at alle må sikre seg i henhold til regelverket, også de som konkluderer med lav risiko i sårbarhetsvurderinger, kan det synes som former for ALARP og kost-nytte vurderinger blir mye brukt (Aven m.fl., 2008). Begrepet nevnes ikke i noen av de gjennomgåtte sårbarhetsvurderingene eller sikringsplanene, men det er nærliggende å anta at prinsippet om å redusere risikoen til et så lavt nivå som praktisk mulig, særlig med hensyn på kostnader, benyttes. Dette blir særlig tydelig hos anlegg som gjennomfører lav-risiko operasjoner og som ligger langt fra folk. Slike anlegg synes å ville dimensjonere sikringen på et lavest mulig nivå, for å unngå kostnader som følger med større tiltak. En kan anta at dette har en sammenheng med at havneanlegget selv ikke forbinder virksomheten sin med noen risiko.

Hvorvidt havneanleggene eller RSOene gjennomfører de tre stegene som Aven m.fl. (2008) trekker frem som vurderingsprosessen for tiltak, kommer ikke frem av planverkene. Det synes helt klart fornuftig at havneanlegg med lavrisiko-operasjoner dimensjonerer sikringen på et lavere nivå enn for eksempel cruiseterminaler, og på denne måten kommer sårbarhetsvurderingene til sin rett. Samtidig synes det å være nettopp operasjoner, omfang og beliggenhet som er avgjørende for dimensjoneringen av sikringen av hvert enkelt havneanlegg. Etter mitt syn er hovedårsaken til at havneanlegg med like forutsetninger på disse parameterne sikrer seg likt, at trusselvurderingene og tilhørende scenarioer også er like.

Delkonklusjon forskningsspørsmål 3

Basert på resonnementet ovenfor synes det som om selve vurderingen av sårbarhet er den faktoren som i praksis spiller størst rolle for risikoen som presenteres i risikobildet. Det synes også å være denne faktoren som varierer mest fra havneanlegg til havneanlegg. Havneanlegg med tilnærmet like operasjoner, omfang og beliggenhet tar ofte høyde for like verdier, og vurderes til å måtte forholde seg til like trusselaktører og –scenarioer. Det som dermed er avgjørende for risikoen, er hvilken sårbarhet en kan identifisere hos havneanlegget. Samtidig synes det som Kystverket legger opp til at sårbarheten skal vektlegges på lik linje med trussel og konsekvens. Således synes det noe misvisende å kalle den helhetlige analysen for en sårbarhetsvurdering. Likevel spiller sårbarheten en sentral rolle når havneanleggets tiltak skal besluttes – særlig hos havneanlegg som knyttes til høy risiko. Det er også tydelig at regelverket spiller en rolle når det kommer til valg av sikringstiltak. En kan si at regelverket beskriver hva som skal oppnås, at sårbarhetsvurderingen sier hvilket nivå en skal legge seg på, og at sikringsplanen beskriver de faktiske tiltakene som må gjennomføres.

6. Konklusjon

Hvordan fungerer sårbarhetsvurderinger som et hensiktsmessig verktøy for dimensjonering av sikringstiltak i norske ISPS-havneanlegg?

I det følgende vil de tre forskningsspørsmålene knyttes sammen til en konklusjon, og gi et svar på studiens problemstilling. Gjennom å studere regelverk, Norsk Standard 5832:2014, Kystverkets mal, og foreliggende sårbarhetsvurderinger og sikringsplaner, har jeg fått et innblikk i en metode for gjennomføring av risikoanalyser for tilsiktede uønskede handlinger i en havnesikringskontekst. Studien er ikke generaliserbar som sådan, men det er gjort funn som kan være av betydning for andre virksomheters tilnærminger til risikoanalyser mot tilsiktede uønskede handlinger.

Kystverkets mal for gjennomføring av sårbarhetsvurderinger for havneanlegg har tatt utgangspunkt i NS 5832:2014. Standarden baserer sin fremstilling av risiko på vurderinger av verdier, trusler og sårbarhet. Disse faktorene er ikke nytt for fagfeltet, men standarden har likevel møtt motstand fra noen akademiske miljøer (Busmundrud m.fl., 2015). Kritikken går i hovedsak ut på at standarden ikke omtaler sannsynlighet, og da særlig kunnskapsbasert sannsynlighet. Ved å omtale kunnskapsbasert sannsynlighet, tar en også høyde for usikkerheten knyttet til vurderingene som gjennomføres. For øvrig har det kommet frem at dersom en følger standardens steg, og gjør gode datainnsamlinger og –vurderinger, får en mye av det samme grunnlaget som trolig ville utgjort den kunnskapsbaserte sannsynligheten. Dette forutsetter likevel at en fortløpende og gjennomgående beskriver usikkerheten knyttet til de ulike vurderingene. Standarden påpeker i en merknad innledningsvis, og under «vurdering av ren risiko», at usikkerheten skal beskrives. Likevel kunne dette kommet tydeligere frem under alle stegene der dette er relevant.

Da Kystverket skulle operasjonalisere standarden, måtte de også ta høyde for kravene som stilles i regelverket. Dette har de etter mitt syn gjort på en god måte. Det er likevel to sentrale forbedringspunkter i Kystverkets mal. Det første punktet dreier seg om beskrivelse av usikkerhet. På samme måte som i standarden, er selve risikovurderingen det eneste trinnet i analysen som omtaler usikkerhet. Det presiseres i dette trinnet at en skal vurdere usikkerhet knyttet til trusler, sårbarhet og konsekvens, men etter stegene å dømme er disse vurderingene allerede gjennomført når en kommer til risikovurderingen. Etter mitt syn burde en form for usikkerhetsvurdering vært bedre implementert i den helhetlige analysen. Gevinsten ville kommet i form av mer åpenhet rundt resultatene som legges frem. En ville da også lettere

kunne ta høyde for ulike variasjoner og utfall av et trusselscenario. Det andre punktet går på at Kystverket omtaler analysen som en sårbarhetsvurdering. Det er ingen tvil om at vurdering av sårbarhet er et sentralt element i analysen, men denne vurderingen er bare én av tre faktorer som utgjør et havneanleggs risiko. Kystverkets navngivelse av prosessen synes å ha sin naturlige forklaring med bakgrunn i begrepet som brukes i forskrift om sikring av havneanlegg § 9, men en ville vært mer tro mot både standarden og ISPS-koden ved å kalle analysen for en risikoanalyse eller sikringsrisikoanalyse. Disse begrepene favner bredere enn sårbarhetsvurdering. I tillegg er felles begrepsbruk sentralt for å skape felles forståelse som kan drive fagfeltet fremover.

Når det kommer til dimensjonering av tiltak, legger regelverket noen føringer for hva sikringen skal oppnå. Sårbarhetsvurderingen spiller videre en sentral rolle for hvilket nivå en skal dimensjonere sikringen på, før sikringsplanen spesifikt uttaler hvilke tiltak som skal gjennomføres. Det har likevel vist seg at de faktorene som ser ut til å bety mest for dimensjoneringen av tiltakene er havneanleggets operasjoner, omfanget av operasjonene, og havneanleggets beliggenhet. Alle disse er faktorer som gjøres rede for før stegene i analysen iverksettes. Samtidig er stegene som gjennomføres i analysen sentrale for å avdekke karakteristiske og særegne forhold ved de enkelte havneanleggene. For at analysen skal ha en nytteverdi forutsettes det likevel at vurderingene som gjøres er tilfredsstillende, basert på oppdatert kunnskap, og at risikoeier tar del i prosessen. Det synes særlig viktig at den som gjennomfører analysen har tilstrekkelig kompetanse til å gjennomføre gode trusselvurderinger, og utarbeide scenarioer tilpasset havneanlegget.

6.1. Videre forskning

Risikoanalyser for tilsiktede uønskede hendelser er noe jeg tror vi kan forvente å se mer av i tiden fremover. Den enkelte virksomhet har et ansvar for å sikre seg selv og sitt personell (NSM m.fl., 2015). Dette betyr at stadig flere virksomheter allerede har, eller må ta i bruk verktøy for slike (sikrings-)risikoanalyser. Med dette melder behovet seg for en ensartet forståelse av begreper og metode for gjennomføring av slike analyser. Det synes et behov for forskning på kommunikasjon rundt usikkerhet i slike analyser. Dette gjelder både gjennom hele analysen og presentasjonen av risiko i et risikobilde. Det kunne helt klart vært interessant å sett hvordan andre sivile virksomheter velger å løse dette. Både hvordan en velger å operasjonalisere NS 5832, men også hvilke andre metoder som benyttes. Særlig interessant ville det vært å studere hvordan andre virksomheter tar høyde for usikkerhet i sine vurderinger. Til slutt vil jeg fremheve behovet for studier som ser nærmere på hvordan en bør

gå frem ved utarbeidelse av trusselscenarioer, og hvor detaljerte en bør være når en lager scenarioene. Trusselscenarioer knyter sammen verdier og trusselaktøren(e), og synliggjør dermed virksomhetens sårbarheter. Trinnet spiller således en sentral rolle i en (sikrings-)risikoanalyse.

7. Kilder

Alexander, D. (2005). Towards the development of a standard in emergency planning. *Disaster Prevention and Management: An International Journal, 14*(2), 158 – 175. DOI: 10.1108/09653560510595164

Andersen, S. S. (1997). *Case-studier og generalisering - forskningsstrategi og design*. Bergen: Fagbokforlaget.

Aven, T. & Renn, O. (2008). The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism risk. *Risk analysis, 29*(4), 587 – 600. DOI: 10.1111/j.1539-6924.2008.01175.x

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

Aven, T. (2013). Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts. *Reliability Engineering and system safety, 119*, 229-234. DOI: 10.1016/j.ress.2013.06.044

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget

Aven, T., Røed, W., & Wiencke, H. S. (2008). *Risikoanalyse*. Oslo: Universitetsforlaget

Batalden, B-M. (2015). *Safety Management in Shipping*. (Doktoravhandling). Universitetet i Stavanger

Bier, V. M. (2007). Choosing What to Protect. *Risk Analysis, 27*(3), 607 – 620. DOI: 10.1111/j.1539-6924.2007.00906.x

Bratberg, Ø. (2014). *Tekstanalyse for samfunnsvitere*. Oslo: Cappelen Damm

Brinkmann, S. & Tanggaard, L. (2012). *Kvalitative metoder: empiri og teoriutvikling.* Oslo: Gyldendal akademisk forlag

Brown, G. G., & Cox Jr, L. A. (2010). How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts. *Risk analysis, 31*(2), 196 – 204. DOI: 10.1111/j.1539-6924.2010.01492.x

Busmundrud, O., Maal, M., Kiran J. H., og Endregard, M. (2015). *Tilnærminger til risikovurderingen for tilsiktede uønskede hendelser.* FFI-rapport 2015/00923, Forsvarets forskningsinstitutt. Hentet 12. november 2017 fra https://www.ffi.no/no/Rapporter/15-00923.pdf

Cohen, L., E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588 – 608. DOI: 10.2307/2094589

Cox Jr, L. A. (2008). Some Limitations of «Risk = Threat x Vulnerability x Consequence» for Risk Analysis of Terrorist Attacks. *Risk Analysis, 28*(6), 1749 – 1761. DOI: 10.1111/j.1539-6924.2008.01142.x

Cox Jr, L. A. (2009). Improving risk-based decision making for terrorism applications. *Risk analysis, 29*(3), 336 – 341. DOI: 10.1111/j.1539-6924.2009.01206.x

Dey, I. (1993). *Qualitative Data Analysis*. London: Routledge

Dillon, R.L., Liebe, R.M. & Bestafka, T. (2009). Risk-based decision making for terrorism applications. *Risk Analysis 29*(3), 321 – 335. DOI: 10.1111/j.1539-6924.2008.01196.x

Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security

Dynes, R. (1994). Community Emergency Planning. *International Journal of Mass Emergencies and Disasters, 12*(2), 141-158. Hentet 01. september fra http://www.ijmed.org/articles/430/download/

Dynes, R. R., Quarantelli, E. L., & Kreps, G. A. (1972) A Perspective on Disaster Planning. Ohio State: University Columbus Disaster Research Center. Hentet 12. november 2017 fra: http://www.dtic.mil/get-tr-doc/pdf?AD=AD0750293

Forskrift om sikring av havneanlegg. (2013). *Forskrift 29. mai 2013 nr. 538 om sikring av havneanlegg.*

Forsvarsbygg. (2016). *Sikringshåndboka*: *Håndbok i sikring av eiendom, bygg og anlegg mot terror, sabotasje, spionasje og kriminalitet.* Oslo: Forsvarsbygg

Gedde-Dahl, S. (2014, 24. juli). Økt beredskap på 600 havner. *Aftenposten.* Hentet 20. august fra https://www.aftenposten.no/norge/i/OgmA/Okt-beredskap-pa-600-norske-havner

Harris, L. T. (2017). London and anti-terrorism in Europe. *European View.* DOI https://doi.org/10.1007/s12290-017-0454-6

Havne- og farvannsloven. (2009). *Lov 17. april 2009 nr. 19 om havner og farvann*

International Maritime Organization. (2003). *International Ship and Port Facilities Security (ISPS) Code*. London: International Maritime Organization

International Maritime Organization. (2012). *Guide to Maritime Security and the ISPS Code.* London: International Maritime Organization

International Maritime Organization. (2017). *International Convention for the Safety of Life at Sea (SOLAS), 1974.* Hentet fra http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode* (2. utg.). Kristiansand: Høyskoleforlaget

Jiang, B. (2017). *An Empirical Analysis of Maritime Terrorism Using the Global Terrorism Database*. I LaFree, G., og Freilich, J.D. (2017). *The Handbook of the Criminology of Terrorism.* First edition, John Wiley & Sons, Inc.

Jore S. H. & Njå, O. (2010). Risk of terrorism: A scientifically Valid Phenomenon or a Wild Guess? The Impact of Different Approaches to Risk Assessment, *Critical Approaches to Discourse Analysis across Disciplines (4)*2, 197 – 216. Hentet 12. november fra https://www.scribd.com/document/76412550/Risk-of-Terrorism-a-Scientifically-Valid-Phenomenon-or-a-Wild-Guess

Jore, S. H. & Moen, A. (2015). A discussion of the risk-management and the rule-compliance regulation regimes in a security context. *Safety and Reliability: Methodology and Applications, Nowakowski m.fl.* (Eds). London: Tayler & Francis Group, London

Krumsvik, R. J. (2014). *Forskningsdesign og kvalitativ metode.* Bergen: Fagbokforlaget

Kujawski, E. & Miller, G. A. (2007). Quantitative Risk-Based Analysis for Military Counterterrorism Systems. *Systems Engineering, 10*(4), 273 – 289. DOI: 10.1002/sys.20075

Kystverket. (2011). *Fakta om havnesikring.* Hentet 12. november 2017 fra http://www.kystverket.no/Maritim-infrastruktur/Havnesikring/Fakta/#

Kystverket. (2012). *Veiledning knyttet til havnesikring.* Hentet fra http://kystverket.no/Maritim-infrastruktur/Havnesikring/Veiledning-/

Kystverket. (2013). *Veiledning til forskrift om sikring av havneanlegg.* Hentet fra http://www.kystverket.no/globalassets/havner/havnesikring/veiledning---sikring-av-havneanlegg-rev1.pdf

Kystverket. (2014, 24. juli). Hever sikringsnivået i norske havner. *Kystverket.* Hentet fra http://www.kystverket.no/Nyheter/2014/Juli/Hever-sikringsnivaet-i-norske-havner/

Kystverket. (2016a). *Kystverkets veileder for utarbeidelse av sårbarhetsvurderinger (PFSA) for havneanlegg*.

Kystverket. (2016b). *Kystverkets mal for utarbeidelse av sårbarhetsvurderinger (PFSA) for havneanlegg*.

Kystverket. (2016c). *Regelverk for havnesikring.* Hentet 12. november 2017 fra http://www.kystverket.no/Maritim-infrastruktur/Havnesikring/Regelverk/

Kystverket. (2017a). *Kva er Kystverket?* Hentet 12. november 2017 fra http://www.kystverket.no/Om-Kystverket/Kva-er-Kystverket/

Kystverket. (2017b). *Godkjente sikringsvirksomheter (RSO).* Hentet fra http://www.kystverket.no/Maritim-infrastruktur/Havnesikring/Godkjente-RSO/

Manunta, G. (1997). *Towards a Security Science through a Specific Theory and Methodology*. (Doktoravhandling). University of Leicester. Hentet 20. august fra https://lra.le.ac.uk/bitstream/2381/27756/1/1997ManuntaGPhD.pdf

Nasjonal Sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste. (2015). *Terrorsikring: En veileder i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger*. Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder_terrorsikring_2015_enkelts_final.pdf

Nesset, P., Stenersen, A., Oftedal, E. (2016) Jihadi Terrorism in Europe: The IS-Effect. *Perspectives on terrorism*, Vol 10 No 6 (2016).

NOU 2000:24. *Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*

NOU 2012:14, *Rapport fra 22. Juli-kommisjonen*

Perry, R.W. og Lindell, M. K. (2003). Preparedness for Emergency Response: Guidelines for the Emergency Planning Process. *Disasters*, 27(4), 336-350. DOI: 10.1111/j.0361-3666.2003.00237.x

Politiets Sikkerhetstjeneste, PST (2017). *Trusselvurdering 2017*. Hentet 28. november 2017 fra: http://www.pst.no/media/82648/pst_trusselvurd_2017_no_web.pdf

Quarantelli, E. L. (1977). Social Aspects of Disasters and Their Relevance to Pre-disaster Planning. *Disasters 1*(1), 98–107.

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

Reason, J. (1997), *Managing the Risks of Organizational Accidents*. Farnham: Ashgate Publishing Limited.

Regulation (EC) No 725/2004 of The European Parliament and the Council of 31 march 2004, on enhancing ship and port facility security.

Skavland, E. I. & Jakobsen, Ø. M. (2000). *Objekt- og informasjonssikkerhet. Metode for risiko og sårbarhetsanalyse.* Trondheim: Norges teknisk-naturvitenskapelige universitet, Institutt for produksjons- og kvalitetsteknikk

Standard Norge. (2008). *Krav til risikovurderinger* (NS 5814). Lysaker: Standard Norge.

Standard Norge. (2012). *Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger – Terminologi* (NS 5830). Lysaker: Standard Norge

Standard Norge. (2014). *Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikostyring* (NS 5831). Lysaker: Standard Norge

Standard Norge. (2014). *Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse* (NS 5832). Lysaker: Standard Norge

Standard Norge. (2017a). *Standard Norge.* Hentet 12. november 2017 fra http://www.standard.no/toppvalg/om-oss/standard-norge/

Standard Norge. (2017b). *Standardisering.* Hentet 12. november 2017 fra http://www.standard.no/standardisering/

Staupe-Delgado, R., Kruke, BI. (2017). Preparedness: Unpacking and clarifying the concept. *J Contingencies and Crisis Management.* 2017;00:1-13. https://doi.org/10.1111/1468-5973.12175

Thagaard, T. (2009). *Systematikk og innlevelse: en innføring i kvalitativ metode* (3. utg.). Bergen: Fagbokforlaget.

Williams, Paul D. (2013). *Security Studies an introduction* (2. utg.). London: Routledge

Yang, Z., Ng, A. K. Y. & Wang, J. (2014). A new risk quantification approach in port facility security assessment. *Transportation Research Part A, 59,* 72-90. DOI: 10.1016/j.tra.2013.10.025

Yin, R. K. (2014). *Case study research - design and methods* (5. utg.). London: SAGE Publications Ltd.

Yin, R.K. (2003). *Case Study Research: Design and Methods* (3. utg). Thousand Oaks, CA: Sage

Yoe, C. (2012). *Primer on risk analysis – Decision making under uncertainty.* Boca Raton, FL: CRC Press/Taylor & Francis